American University International Law Review

Volume 35 | Issue 4 Article 8

2020

The Cost of Ensuring Privacy: How the General Data Protection Regulation Acts as a Barrier to Trade in Violation of Articles XVI and XVII of the General Agreement on Trade in Services

Elisabeth Meddin

THE COST OF ENSURING PRIVACY: HOW THE GENERAL DATA PROTECTION REGULATION ACTS AS A BARRIER TO TRADE IN VIOLATION OF ARTICLES XVI AND XVII OF THE GENERAL AGREEMENT ON TRADE IN SERVICES

ELISABETH MEDDIN*

* J.D. Candidate, May 2021, American University Washington College of Law; M.A. in Art Business, 2015, Sotheby's Institute of Art, London; B.A. in French Literature, 2012, The George Washington University. I want to extend my sincerest gratitude to Professor Ben Leff whose guidance and feedback throughout the comment writing process was invaluable. I would also like to thank Professor Fernanda Nicola for her vital insights into EU constitutional law and Professor Padideh Ala'i whose infectious love for trade law helped inspire this comment. This comment is dedicated to the village who has always given me their unwavering support, Nancy Feinrider, Linda Dale Hoffa, Fran and Rosemary Gambardella, and to my family, Alexandre Meddin, Joan Rosoff, and Russell Meddin.

I. INTRODUCTION

The rights of privacy are an integral part of European Union (EU) law and are considered to be one of the fundamental human rights.[1] They are enshrined in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union, which provide rights to a private life, communications, and protections of personal information.[2] As

1. Charter of Fundamental Rights of the European Union, arts. 7–8, 2000 O.J. (C 364) 1.

2. *Id.* ("Everyone has the right to respect for his or her private and family life,

technology advances, these rights are being threatened as more of everyday life occurs online, requiring the input of personal information across a variety of digital transactions. In 2012, the General Data Protection Regulation (GDPR)[3] was proposed in the EU Parliament in the hopes that new legislation could resolve many of these burgeoning issues.[4] Intended to protect the personal information of European citizens within the EU, the GDPR was designed to apply to non-EU companies operating within the EU.[5]

This Comment argues that the compliance requirements under the GDPR for non-EU companies to operate within the EU—even considering the inclusion of adequacy decision provisions—have the effect of either excluding these companies altogether or of pushing them to localize any data-related activities within the EU.[6] As a result, the GDPR prevents the cross-national free flow of services in violation of the General Agreement on Trade in Services (GATS)[7] Articles XVI and XVII.[8]

Part II of this Comment will provide a history of the GDPR as well as clarify the obligations of entities partaking in data protection and collection within the EU.[9] Part II will also examine the GATS' purpose in protecting trade in services and will assess the importance of

---

home and communications [and] . . . [e]veryone has the right to the protection of personal data concerning him or her.").

3. 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), 2016 O.J. (L 119) 1 [hereinafter GDPR].

4. *See The History of the General Data Protection Regulation*, EUR. DATA PROTECTION SUPERVISOR, https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en (last visited Oct. 4, 2019) [hereinafter *History of GDPR*] (noting that on January 25, 2012, the European Commission proposed a comprehensive reform of the European Union's data protection rules).

5. GDPR, *supra* note 3, art. 3.

6. *See infra* Part III.

7. 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].

8. GATS arts. XVI, XVII.

9. *See infra* Part II.A.

Articles XVI and XVII.[10] Part II will also look at the exceptions to GATS which are often used as a defense by World Trade Organization (WTO) Members in complaints brought against them.[11] Finally, Part II will clarify how a piece of national legislation can be viewed as a barrier to trade through illustrating past instances when national legislation has been the basis of a complaint brought before the WTO Dispute Settlement Body (DSB) and where it was argued that such legislation was a non-tariff barrier (NTB) to trade.[12]

In Part III, this Comment will analyze how, through its implementation, the GDPR is acting as a barrier to trade.[13] Part III will further examine how in acting as a barrier to trade, the GDPR is in violation of the GATS, specifically the articles dealing with market access and national treatment.[14] Finally, Part III will present possible defenses the EU could raise should a case be brought against it in front of the DSB.[15]

Part IV will provide recommendations to the EU for ways in which to ameliorate the negative effects on trade caused by the GDPR by eliminating data localization and expanding the number of adequacy decisions.[16] Secondly, it will propose a pathway to bring a case against the EU outside of the DSB.[17]

Finally, Part V will conclude that unless the EU addresses the barriers that the compliance requirements of the GDPR are causing for non-EU companies, it risks remaining in violation of the GATS and leaving itself open to legal action.[18]

II. BACKGROUND

This section provides the background necessary to understand the ways in which the GDPR is in violation of the GATS. Firstly, it delves into the history of the GDPR and the purpose behind the legislation

10. *See infra* Part II.B.
11. *See infra* Part II.B.
12. *See infra* Part II.C.
13. *See infra* Part III.A.
14. *See infra* Part III.B.
15. *See infra* Part III.C.
16. *See infra* Part IV.A.
17. *See infra* Part IV.B.
18. *See infra* Part V.

while also exploring the various obligations owed by entities that fall under the purview of the GDPR.[19] Secondly, it looks at the purpose of the GATS and its history before examining more in depth the articles that are being violated, as well as the article pertaining to exceptions.[20] Thirdly, this section defines a NTB to trade by providing past examples that have come before the WTO.[21]

A. A PRIVACY LAW BY ANY OTHER NAME: EXAMINING HOW THE GDPR WORKS

1. From Directive to Regulation: The Evolution of EU Data Protection

In 1995, the EU created the Data Protection Directive (DPD) to regulate the processing of digital personal data and to govern how that data moved about within the EU.[22] Over the next decade and a half it became clear, however, that as technology advanced, not only were further protections needed, but they needed to be implemented uniformly.[23] To that end, what would eventually evolve into the GDPR was proposed in January 2012.[24]

The GDPR is intended to protect EU citizens in all of their digital transactions;[25] therefore, it was created with a wide territorial scope that extends past the EU.[26] This means that the GDPR does not only

19. *See infra* Part II.A.i–ii.

20. *See infra* Part II.B.i–ii.

21. *See infra* Part II(C).

22. 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.

23. *See generally Regulations, Directives and Other Acts*, EUR. UNION (Mar. 7, 2019), https://europa.eu/european-union/eu-law/legal-acts_en (explaining that a directive is a legislative act that sets out a goal that all EU Member States must achieve by devising their own laws, while a regulation is a binding legislative act that once passed is applied in its entirety across all Member States).

24. *See, e.g.*, *History of GDPR*, *supra* note 4 (showing that the Commission proposed comprehensive reforms to data privacy January 25, 2012, which were adopted in April 2016 and came into force May 25, 2018).

25. GDPR, *supra* note 3, art. 1 (stating that "[t]his Regulation protects . . . freedoms of natural persons and in particular their right to the protection of personal data.").

26. *See id.* art. 3 (defining the territorial scope of the GDPR as being global so long as the data subject himself is located within the EU and the processing activities

apply to all EU companies operating within the EU, but it further extends its scope to cover any company whose processing activities are related to offering goods or services to persons in the EU, monetarily or otherwise.[27] As a result, essentially any company worldwide that has any sort of digital footprint in the EU will be governed by the GDPR.[28]

The GDPR applies to the processing of all personal data done entirely or partly by automated means and works to govern the free movement of aforementioned data.[29] Personal data in this instance refers to anything that can be used to identify a natural person such as a name or other factors relating to one's appearance or genetic, economic, or social identity.[30] Personal data relating to one's health, sex life, race, sexual orientation, and religious or political beliefs is considered to be a special category, the processing of which is prohibited save for a few exceptions.[31] These exceptions include situations where processing is necessary to protect vital interests of a subject unable to give consent, necessary for the establishment or exercise of a legal claim, or necessary for reasons of public health interests, among others.[32] Another exception on which companies can rely is consent.[33]

The hallmark of the GDPR is the emphasis it places on the necessity of consent for the processing of specific data, and more specifically, "opt-in" consent.[34] "Opt-in" consent is a more affirmative manner of

---

are related to the offering of goods or services).

27. *See id.* ("1. This regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not. 2. This Regulation applies to the processing of personal data subjects who are in the Union by a controller or processor not established in the Union, where 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 subject in the Union. . . .").

28. *See generally id.*

29. *Id.* art. 1(1).

30. *Id.* art. 4(1) (defining personal data).

31. *Id.* art. 9(1).

32. *Id.* art. 9(2)(c), 9(2)(f), 9(2)(i).

33. *See id.* art. 9(2)(a) (stating that the prohibition shall not apply if "the data subject has given explicit consent to the processing of those personal data" mentioned above).

34. *Id.* art. 7.

obtaining consent; no longer able to rely on a subject's silence or on pre-checked boxes that are not easily seen, known as opt-out consent, companies must actively seek and receive consent.[35] Under the GDPR, consent must be demonstrable, freely given, and can be withdrawn at any time.[36]

2. Too Many Rules?: The Myriad Obligations Under the GDPR

Before turning to the obligations owed by an entity taking part in data collection and processing under the GDPR, it is important to distinguish if the entity in question—whether a single person or an entire company—is a 'controller'[37] or 'processor'[38] as each have separate and distinct roles under the GDPR.

The controller is responsible for ensuring that the appropriate measures governing the processing of data have been put in place to keep all actions compliant with the GDPR.[39] These measures can include oversight of any processors with whom the controller may have contracted to deal with the data collected.[40] In contrast, the

35. *See* Rita Heimes, *How Opt-In Consent Really Works*, IAPP (Feb. 22, 2019), https://iapp.org/news/a/yes-how-opt-in-consent-really-works/ (contrasting opt-in versus opt-out consent and discussing how companies can shift marketing tools to conform with GDPR opt-in requirements).

36. GDPR, *supra* note 3, art. 7(1), 7(3)–(4) ("[T]he controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data . . . [t]he data subject shall have the right to withdraw his or her consent at any time . . . [w]hen assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract . . . is conditional on consent to the processing.").

37. *See generally id.* art. 4(7) (defining controller as "the natural or legal person, public authority, agency, or other body . . . [which] determines the purposes and means of the processing of personal data").

38. *See also id.* art. 4(2) (referring to processing as "any operation or set of operations which is performed on personal data . . . such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available"). *See generally id.* art. 4(8) (identifying a processor as "a natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller.").

39. *Id.* art. 24(1) (stating that the controller "shall implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation").

40. *Id.* art. 28(1) (requiring that a "controller shall only use processors providing sufficient guarantees to implement appropriate technical and organizational

processor is the entity that actually carries out the processing of data.[41] For controllers and processors dealing with the processing of data related to the offering of goods and services that are not located in the EU, yet still under obligations imposed by the GDPR under the territorial scope outlined in Article 3(2),[42] a representative established in the EU must be appointed.[43]

Of the myriad obligations due under the GDPR, the obligations dealing with the transfer of data to third countries are at issue in determining a GATS violation because they relate to the differing treatment between countries as a whole.[44] These transfers are predominantly determined by adequacy decisions made by the European Commission.[45] Currently, there are eleven countries that fall

---

measures").

41. *Id.* art. 28.

42. *Id.* art. 3(2) ("This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where 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 Union.").

43. *See id.* art. 27(2)–(4) (mandating that appointed representatives "be established in one of the Member States where the data subjects, whose personal data are processed in relation to the offering of goods or services to them, or whose behavior is monitored, are" and that the representative "be addressed to or instead of the controller or the processor by, in particular, supervisory authorities and data subject, on all issues relating to processing").

44. *See id.* arts. 44–45.

45. *See id.* art. 45 (requiring that in order for there to be a "transfer of personal data to a third country," the transfer must be to a third country "where the Commission has decided that the third country . . . ensures an adequate level of protection"); *see also Adequacy Decisions*, EUR. COMMISSION, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (last visited Oct. 6, 2019) (describing the steps involved for an adequacy decision to be awarded, starting with a proposal from the European Commission, followed by an opinion from the European Data Protection Board, an approval from representatives of EU countries, and finally the adoption of the decision by the European Commission). *See generally Binding Corporate Rules (BCR)*, EUR. COMMISSION, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en (last visited Nov. 15, 2019) (showing that Binding Corporate Rules are a method through which multinational companies—i.e. those with a definitive European Headquarters—can transfer data between subsidiaries across borders); Paul M. Schwartz, *Global Data Privacy: The EU Way*, 94 N.Y.U. L. REV. 771, 793–94 (2019) (highlighting that Binding Corporate Rules are used for companies with global operations in the sense that they may have multiple worldwide headquarters

under the adequacy decision provision outlined in Article 45,[46] not including the United States (prior to July 2020) and Canada, each of which are governed by partial adequacy decisions with different terms.[47] Canada's agreement is similar to the other adequacy decisions in form; however, it is limited to specific companies and sectors as opposed to being a generalized agreement.[48]

Prior to July 2020, the United States' agreement differed slightly in that it was in its second iteration.[49] Transfers were originally governed by an agreement called Safe Harbor,[50] which was invalidated in 2015 by a case brought before the Court of Justice of the European Union (CJEU), *Schrems v. Data Protection Commissioner*.[51] As of July 2016, the United States was covered under the Privacy Shield system, a framework that required companies to self-certify as being compliant with data protection regulations.[52] In July 2020, this system was struck down by the decision in the case *Data Protection Commissioner v.*

---

and offices, not for non-EU companies that are simply accessible from the EU—for those, reliance on adequacy decisions is still crucial).

46. *See Adequacy Decisions*, *supra* note 45 (listing the current countries covered by an adequacy decision: Andorra, Argentina, Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay, and the United States—under limitations).

47. *See* 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, 2014 O.J. (L 207) 1 [hereinafter EU-U.S. Privacy Shield] (rendering the terms under which transfers of data can take place from the EU to the United States for companies certified by Privacy Shield); *see also* Commission Decision of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act, 2002 O.J. (L 2) 13 [hereinafter EU-Canada Commission Decision] (pointing out the specific Canadian companies and sectors that are covered by the adequacy decision and allowed to transfer personal data from the EU).

48. *See generally* EU-Canada Commission Decision, *supra* note 47.

49. *See generally* EU-U.S. Privacy Shield, *supra* note 47.

50. *E.g.*, *U.S.-EU Safe Harbor Framework*, FED. TRADE COMMISSION, https://www.ftc.gov/tips-advice/business-center/privacy-and-security/u.s.-eu-safe-harbor-framework (last visited Oct. 6, 2019).

51. Case C-362/14, Maximillian Schrems v. Data Prot. Comm'r, 2015 EUR-Lex CELEX LEXIS ¶ 107 (Oct. 6, 2015).

52. *See Privacy Shield Overview*, PRIVACY SHIELD FRAMEWORK, https://www.privacyshield.gov/Program-Overview (last visited Oct. 6, 2019) (displaying the requirements for companies under the Privacy Shield framework).

Facebook Ireland, Schrems which found the European Commission's adequacy determination to be invalid as the protections offered did not satisfy the equivalence requirements.[53]

Excluded from these eleven decisions are some countries with extremely strict data protection laws, raising the question of why they were not considered adequate.[54] South Korea is one such country.[55] In 2011, South Korea instituted its own data privacy law, known as the Personal Information Protection Act (PIPA),[56] which in many ways mirrors the GDPR, and then in 2015 added the Network Act.[57] Penalties for violating PIPA or the Network Act can be monetary or penal, and can go as high as a fine of 100 million won and ten years imprisonment with labor.[58]

The implementation of these adequacy decisions also raises questions as to the reasoning behind the process. For example,

53. Case C-311/18, Data Prot. Comm'r v. Facebook Ireland Ltd, Maximillian Schrems, 2020 EUR-Lex CELEX LEXIS ¶ 185, 201 (July 16, 2020) ("[T]he limitations on the protection of personal data arising from the domestic law of the United States on the access and use by US public authorities of such data transferred from the European Union to the United States, which the Commission assessed in the Privacy Shield Decision, are not circumscribed in a way that satisfies requirements that are essentially equivalent to those required, under EU law . . . .").

54. *See* Kurt Wimmer, *Third Annual Detlev F. Vagts Roundtable on Transnational Law: Data Protection in a Global World*, 112 AM. SOC'Y INT'L L. PROC. 219, 231 (2018) [hereinafter *Vagts Roundtable*] (illustrating that South Korea has not received an adequacy decision in its favor despite its strict data protection laws providing that violations can result in jail time).

55. *See Adequacy Decisions*, *supra* note 45 (listing South Korea as having been in discussions regarding certification for an adequacy decision since 2015).

56. *See generally* Personal Information Protection Act, Act No. 10465, Mar. 29, 2011, *amended by* Act No. 14107, Mar. 29, 2016 (S. Kor.), *translated in* Personal Data Protection Laws in Korea, https://www.privacy.go.kr/eng/index.do [hereinafter PIPA].

57. *See generally* The Act on Promotion of Information and Communications Network Utilization and Data Protection, etc., Act No. 6360, Jan. 16, 2001, *amended by* Act No. 13520, Dec. 1, 2015 (S. Kor.), *translated in* Personal Data Protection Laws in Korea, https://www.privacy.go.kr/eng/index.do [hereinafter Network Act].

58. *See* PIPA, *supra* note 56, arts. 70–75 (laying out the various penal provisions in PIPA which range from two years imprisonment with prison labor and a fine of up to 10 million won to as high as 10 years imprisonment with prison labor and a fine of 100 million won); *see also* Network Act, *supra* note 57, arts. 70–76 (highlighting penalties of imprisonment of between one and seven years and monetary fines up to three times the amount of damages suffered).

Argentina, which was given adequacy in 2003, had not even implemented its data protection law when the decision was approved.[59] The help provided by the EU also differs between governments with Monaco being given unasked-for assistance in rewriting its data protection laws while requests for assistance from Quebec were ignored.[60]

i. Unintended Consequences: The Results of What is Required of Third-Countries

Data localization is a requirement that all data be hosted in a specific location, often the same country, zone, etc. in which it is being collected.[61] Though no laws requiring this of external companies operating within the EU exist as of yet, the issue is complicated by the GDPR's requirements.[62] For companies from countries not covered by an adequacy decision, data localization is the easiest, and in some cases the only, solution by which to come into compliance.[63]

Even companies that are based in countries with an EU agreement are finding that it might not be sufficient to keep them safe from

59. *See* Jennifer Stoddart, et al., *The European Union's Adequacy Approach to Privacy and International Data Sharing in Health Research*, 44 J. L. MED. & ETHICS 143, 147 (2016) (noting the process by which Argentina received its adequacy decision and that an adequacy decision was awarded before there had been either any implementation of the data protection law or any clear idea of how such a law would be or could be enforced).

60. *See id.* (comparing the disparity of work done to assist with issuing preliminary adequacy reports between Monaco and Quebec, specifically).

61. *See, e.g.*, Bret Cohen, et al., *Data Localization Laws and Their Impact on Privacy, Data Security and the Global Economy*, 32 ANTITRUST 107, 108 (2017) (highlighting the significance of data localization laws on foreign companies).

62. *See* Ravie Lakshmanan, *German Schools Ban Microsoft Office 365 Amid Privacy Concerns*, THE NEXT WEB (July 16, 2019), https://thenextweb.com/privacy/2019/07/15/german-schools-ban-microsoft-office-365-amid-privacy-concerns/ (commenting that lack of a local data center was a contributing factor to Microsoft Office being found non-compliant under the GDPR).

63. *See* David Roe, *Why the Privacy Shield Won't Make You GDPR-Compliant*, CMSWIRE (May 25, 2018), https://www.cmswire.com/information-management/why-the-privacy-shield-wont-make-you-gdpr-compliant/ (arguing that the best way for a company to become GDPR compliant is to localize all data in an EU-based subsidiary).

having to localize data.[64] Less than a month after the GDPR came into effect, Microsoft Office, a United States company certified under Privacy Shield, was found to be no longer compliant under the GDPR in Hesse, Germany.[65] A major contributing factor to this decision was the closure of Microsoft Office data servers within Germany, while a proposed solution was to reopen said servers.[66]

B. A SECOND AGREEMENT: WHAT IS THE PURPOSE OF THE GENERAL AGREEMENT ON TRADE IN SERVICES?

1. Goods, Services, and Trade, Oh My: History of the GATS

The GATS was one of the main achievements of the Uruguay Round of WTO commitments and was inspired by its counterpart the General Agreement on Tariffs and Trade (GATT).[67] The GATS is the first multilateral trade agreement to cover services specifically and is intended to contribute to trade expansion globally.[68] Included in the concept of trade expansion is a commitment to promote growth and development worldwide, with a focus on developing countries.[69] Currently, services account for about twenty percent of global trade, but that percentage is rising and does not seem to show signs of stopping.[70] The GATS was an annex to the Marrakesh Treaty

64. *See id.* (relaying that a United States-based company cannot wholly rely on Privacy Shield to make itself GDPR compliant).

65. *Statement by the Hessian Commissioner for Data Protection and Freedom of Information on the Use of Microsoft Office 365 in Hessian Schools*, THE HESSIAN COMMISSIONER FOR DATA PROTECTION AND FREEDOM OF INFO. (July 9, 2019), https://datenschutz.hessen.de/pressemitteilungen/stellungnahme-des-hessischen-beauftragten-f%C3%BCr-datenschutz-und [hereinafter *Statement by Hessian Commissioner*].

66. *See id.* (stating that privacy compliance solutions are in the hands of Microsoft and how it handles its data).

67. *See The General Agreement on Trade in Services (GATS): Objectives, Coverage and Disciplines*, WORLD TRADE ORG., https://www.wto.org/english/tratop_e/serv_e/gatsqa_e.htm (last visited Oct. 4, 2019) [hereinafter *GATS Objectives*] (explaining how the GATS came to be, which countries participate, and which services are covered).

68. *See generally* Press Release, World Trade Org., The General Agreement on Trade in Services: An Introduction (Jan. 13, 2013) (providing background on creation of the GATS).

69. *See id.* (expanding on the intent and purpose behind the GATS).

70. *See, e.g.*, *GATS Objectives*, *supra* note 67 (noting that this trend is attributed

establishing the WTO and, as a result, is one of the agreements signed onto by all WTO members.[71]

The GATS was never intended to prevent Members from regulating supply of services in pursuit of their own policy objectives.[72] What it does do, however, is establish rules to ensure that these Member regulations are created in an objective and impartial manner, and that they do not create unnecessary barriers to trade.[73]

Each Member is required to have a schedule of specific commitments which identifies the services for which market access and national treatment—Articles XVI and XVII of GATS, respectively—are guaranteed along with any limitations that might be attached.[74] In making its commitments, a Member is binding itself to provide a specified level of market access and national treatment and, more importantly, to not implement any measures that would restrict entry into the market by foreign suppliers.[75] Regarding market access, these requirements are further set out in Footnote 8 to the original agreement, which stipulates that a market access commitment is a commitment to the open flow of related services.[76] Member

---

to the growth of the technology sector and the movement of services to the digital sphere).

71. *See id.* (stating that all WTO Members are bound by the GATS—including the EU).

72. GATS pmbl. ("Recognizing the right of Members to regulate, and introduce new regulations, on the supply of services within their territories in order to meet national policy objectives").

73. *See generally GATS Objectives*, *supra* note 67.

74. *See Schedules of Commitments and Lists of Article II Exemptions*, WORLD TRADE ORG., https://www.wto.org/english/tratop_e/serv_e/serv_commitments_e.htm (last visited Oct. 6, 2019) [hereinafter *Schedules of Commitments*] (qualifying two types of commitments, sector specific, those that apply to a particular service, and horizontal, those that apply across all sectors subsequently listed in the schedule); *see also Services: Rules for Growth and Investment*, WORLD TRADE ORG., https://www.wto.org/english/thewto_e/whatis_e/tif_e/agrm6_e.htm#commitments (last visited Oct. 6, 2019).

75. *See Guide to Reading the GATS Schedules of Specific Commitments and the List of Article II (MFN) Exemptions*, WORLD TRADE ORG., https://www.wto.org/english/tratop_e/serv_e/guide1_e.htm (last visited Oct. 27, 2019) (detailing how the GATS Schedules of Commitments work).

76. GATS art. XVI, n.8 (noting importantly that the commitments made include those for related services as well).

commitments entered into force when the GATS was adopted, but they can be improved on or new ones introduced at any time.[77] There also exists a specific procedure through which commitments can be modified or withdrawn.[78]

2. At Your Service: GATS Articles XVI & XVII

In looking to the violations by the GDPR, an analysis should be made under the GATS rather than the GATT.[79] The question of whether data is a good or service (and therefore under which agreement it should be analyzed) is debated among authors.[80] Because this Comment is addressing the transfer and movement of data, this author takes the stance that data is a service and is analyzing it accordingly.[81]

Article XVI on market access pertains to the conditions under which external services are treated when entering a foreign country, requiring the treatment afforded to external services to be similarly favorable to the treatment afforded to like domestic services.[82] Examples of measures that cannot be taken include limitations on the number of

77. *See GATS Objectives*, *supra* note 67.

78. *Id.*

79. GATS art. I(1)–(2) (stating that GATS "applies to measures by members affecting trade in services").

80. *Compare* Joshua D. Blume, *Reading the Trade Tea Leaves: A Comparative Analysis of Potential United States WTO-GATS Claims Against Privacy, Localization, and Cybersecurity Laws*, 49 GEO. J. INT'L L. 801, 805 (2018) (taking the position that data is a service), *with* Mira Burri, *The Governance of Data and Data Flows in Trade Agreements: The Pitfalls of Legal Adaptation*, 51 U.C.D. L. REV. 65, 75–76 (2017) (taking the position that data is a good and therefore should be governed under the GATT).

81. MARC BACCHETTA ET AL., SPECIAL STUDIES NO.2: ELECTRONIC COMMERCE AND THE ROLE OF THE WTO 1–3, 50–51 (1998) (addressing the role of the WTO in electronic commerce and analyzing its duties under the GATS, while also commenting that the GATT regime is notably different that the GATS—specifically in regards to national treatment); *see also* Diane A. MacDonald & Christine M. Streatfeild, *Personal Data Privacy and the WTO*, 36 HOUS. J. INT'L L. 625, 633 (2014) (analyzing the restrictions on U.S. cross-border financial services companies from processing data outside of South Korea under the GATS).

82. GATS art. XVI ("With respect to market access through the modes of supply identified in Article I, each Member shall accord services and service suppliers of any other Member treatment no less favourable than that provided for under the terms, limitations and conditions agreed and specified in its Schedule.").

foreign service providers or exclusive service providers, on the total value of transactions, or on the amount of foreign capital invested in suppliers.[83]

Article XVII on national treatment deals with how foreign services are treated within a country in comparison to host country services.[84] The GATS suggests that Members accord to foreign service suppliers either "formally identical or formally different treatment" as they do to domestic suppliers; however, Article XVII(3) clarifies that formally alike or different treatment that modifies competition in favor of domestic suppliers will be considered unfavorable.[85]

Articles XVI and XVII are the most often cited in complaints brought before the DSB for violations of the GATS.[86] There have been thirty cases in which the GATS was cited in the request for consultations,[87] and of those thirty, nineteen cited Article XVI (market access) and twenty-one cited Article XVII (national treatment) as the reasons for bringing a complaint before the DSB.[88]

Whether complaints should and can continue to be brought before the DSB is another matter.[89] WTO cases can be a lengthy and time-

83. *Id.* art. XVI(2)(a)–(b), (f).

84. *Id.* art. XVII(1) (" . . . [E]ach Member shall accord to services and service suppliers of any other Member . . . treatment no less favourable than that it accords to its own like services and service suppliers.").

85. *Id.* art. XVII(2)–(3).

86. For further discussion of other cases of GATS violations see *infra* Part II(C).

87. *See Disputes by Agreement*, WORLD TRADE ORG., https://www.wto.org/english/tratop_e/dispu_e/dispu_agreements_index_e.htm (last visited Oct. 26, 2019) (listing all disputes invoking the GATS and breaking them down by article being allegedly violated).

88. *Disputes by Agreement*, *supra* note 87; *see, e.g.*, Request for Consultations by the Russian Federation, *Ukraine – Measures Relating to Trade in Goods and Services*, WTO Doc. WT/DS525/1 (Jan. 6, 2017); Request for Consultations by Qatar, *Saudi Arabia – Measures Relating to Trade in Goods and Services, and Trade-Related Aspects of Intellectual Property Rights*, WTO Doc. WT/DS528/1 (Apr. 4, 2017); Request for Consultations by Guatemala, Honduras, Mexico and the United States, *European Communities – Regime for the Importation, Sale and Distribution of Bananas*, WTO Doc. WT/DS16/1 (Apr. 10, 1995).

89. *See* Tetyana Payosova et al., *The Dispute Settlement Crisis in the World Trade Organization: Causes and Cures*, PIIE (Mar. 2018), https://www.piie.com/publications/policy-briefs/dispute-settlement-crisis-world-trade-organization-causes-and-cures (explaining that the Appellate Body is in crisis due to the United States blocking the appointment of new officials).

consuming process and, as of December 2019, may no longer be able to proceed.[90] There are, however, other avenues through which to bring a case against the EU under the GATS principles.[91]

i. Exceptional Circumstances: When Can a Member Raise a Defense?

In providing for the requirements around the free flow of services, GATS also provides exceptions[92] for when countries wish to institute a regulation that blocks this flow.[93] These exceptions allow for Members to institute laws that are necessary to, among other things, provide for the protection of privacy in relation to personal data.[94]

In examining whether an exception applies, first the subsection of the article is analyzed then the chapeau.[95] Under the chapeau, it is required that measures be neither arbitrary in their application nor act as unjustifiable discrimination in their effect.[96]

However, despite providing a pathway for a defense in a potential WTO complaint, only once out of the forty-four times that an

90. *See* Blume, *supra* note 80, at 842–43 (laying out the time-consuming process of seeing a case through the DSB from initial consultation to the establishment of a panel, the panel report, to the Appellate Body review and any amendments stemming from that); *see also Appellate Body Members*, WORLD TRADE ORG., https://www.wto.org/1012nglish/tratop_e/dispu_e/ab_members_descrp_e.htm (last visited Oct. 27, 2019) (showing that as of December 10, 2019 there will be one remaining member of the Appellate Body, which is not sufficient to keep the Body running).

91. *See infra* Part IV(B) (discussing the method through which a case could be brought before the ECJ).

92. *See* Thomas Cottier et al., *Article XIV GATS (General Exceptions)*, *in* WTO-TRADE IN SERVICES: MAX PLANCK COMMENTARIES ON WORLD TRADE LAW 287–88 (R. Wolfrum et al. eds., 2008) (noting that the GATS Article XIV dealing with exceptions is modeled off of Article XX of the GATT and is designed to avoid the institution of protectionist policies by Member States); General Agreement on Tariffs and Trade, Oct. 30, 1947, 61 Stat. A-11, 55 U.N.T.S. 194 [hereinafter GATT].

93. GATS art. XIV.

94. GATS art. XIV(c)(ii).

95. *See* Appellate Body Report, *United States – Measures Affecting the Cross-Border Supply of Gambling and Betting Services*, WTO Doc. WT/DS285/AB/R/Corr.1 (adopted Aug. 20, 2007) [hereinafter *US – Gambling*] (laying out the two-tier approach to analyzing exceptions).

96. GATS art. XIV.

exception has been argued under GATS Article XIV, or its counterpart, GATT Article XX,[97] has the exception been successful as a defense.[98] That defense was used by the European Communities to defend France's ban on the importation of asbestos.[99] It would be under these circumstances that any defense to a WTO GATS complaint would be examined.

C. ROADBLOCKS AHEAD: WHAT IS A BARRIER TO TRADE?

A non-tariff barrier is a restriction that results in prohibitions, conditions, or specific market requirements that make the importation or exportation of products or services difficult and/or expensive.[100] NTBs arise from governmental measures, such as complex regulatory environments and determinations of eligibility, among others.[101] Most NTBs are protectionist measures intended to help domestic enterprises at the expense of foreign companies—occasionally these are clear, but more often they are veiled behind measures that do not overtly discriminate.[102]

---

97. GATT art. XX.

98. *See Only One of 44 Attempts to Use the GATT Article XX/GATS Article XIV "General Exception" Has Ever Succeeded: Replicating the WTO Exception Construct Will Not Provide for an Effective TPP General Exception*, PUB. CITIZEN (Aug. 19, 2015), https://www.citizen.org/article/only-one-of-44-attempts-to-use-the-wtos-general-exception-to-only-one-of-44-attempts-to-use-the-gatt-article-xx-gats-article-xiv-general-exception-has-ever/ [hereinafter *One of 44 Attempts*] (describing how of the forty-four cases where an exception was invoked, thirty-three were deemed relevant by the DSB; of those, five failed on the subject matter threshold, eighteen failed on the 'necessary' or 'related to' threshold, and nine on the chapeau).

99. Appellate Body Report, *European Communities – Measures Affecting Asbestos and Asbestos-Containing Products*, WTO Doc. WT/DS135/AB/R (adopted Apr. 5, 2001) [hereinafter *EC – Asbestos*] (noting importantly that this was a GATT Article XX case not a GATS Article XIV case).

100. *See Non-tariff Barriers*, INSTITUTE FOR GOVERNMENt, https://www.instituteforgovernment.org.uk/explainers/non-tariff-barriers (last visited Oct. 6, 2019) (noting that NTBs can include regulations, rules of origin, and quotas).

101. *See generally id.*

102. *See Non-tariff Barriers: Red Tape, etc.*, WORLD TRADE ORG., https://www.wto.o1013nglishish/thewto_e/whatis_e/tif_e/agrm9_e.htm (last visited Oct. 6, 2019); *see also* Panel Report, *United States – Import Prohibition of Certain Shrimp and Shrimp Products*, WTO Doc. WT/DS58/R (May 15, 1998) (finding that measures instituted by the United States intended to protect turtles by requiring all

If a WTO member believes that another member has enacted a regulation that acts as an NTB and works to restrict trade, it is entitled to bring a complaint before the WTO alleging that the practice in question violates one of the trade agreements.[103] For example, in 2003, Antigua and Barbuda brought a complaint against the United States alleging that measures affecting cross-border supply of online betting services were in violation of, among others, the GATS Article XVI—market access.[104] Antigua argued in *US – Gambling* that three federal laws prohibiting the cross-border supply of betting services were contrary to the United States' market access commitments regarding these services.[105] Antigua's argument rested on the fact that because the United States had committed to applying treatment to foreign suppliers that was substantially similar to that of domestic ones, it was in violation of GATS in prohibiting Antigua from operating gambling and betting services within the United States.[106] In finding for Antigua, the DSB agreed that the United States was violating the requirement under Article XVI, with respect to the various commitments laid out in its respective schedules, by not affording Antiguan suppliers of gambling and betting services the treatment specified therein.[107]

In another case brought before the WTO,[108] the United States alleged that China was violating Articles XVI (market access) and XVII (national treatment) due to measures relating to the regulation and importation of specific publications and audiovisual entertainment

---

shrimp imported into the country to have been caught using turtle-excluder devices were in reality a way to discriminate against other WTO members hoping to export shrimp).

103. *See Introduction to the WTO Dispute Settlement System*, WORLD TRADE ORG., https://www.wto.org/english/tratop_e/dispu_e/disp_settlement_cbt_e/c1s4p1_e.htm (last visited Oct. 6, 2019) (discussing which parties may bring a dispute before the WTO).

104. *US – Gambling*, supra note 95.

105. *See id.* (arguing that the Wire Act, the Travel Act, and the Illegal Gambling Business Act were inconsistent with the United States' commitments under GATS art. XVI).

106. *See id.*

107. *See* GATS art. XVI; *see also US – Gambling*, *supra* note 95.

108. Appellate Body Report, *China – Measures Affecting Trading Rights and Distribution Services for Certain Publications and Audiovisual Entertainment Products*, WTO Doc. WT/DS363/AB/R (Dec. 21, 2009) [hereinafter *China – Trading Rights*].

products.[109] The products in contention were found to have fallen under the category of "sound recording distribution services," which was a section of China's GATS schedule of commitments.[110] The DSB found that because the items in question fell under one of the commitments, the measures prohibiting foreign entities from distribution was inconsistent with Article XVII as it afforded foreign companies less favorable treatment.[111]

III. ANALYSIS

The following will lay out the ways in which the compliance requirements under the GDPR for non-EU companies are such that these companies must either withdraw their services from the EU market completely or shift toward localizing their data within the EU, thus violating acceptable trade practices under the GATS. The first section will illustrate how the system through which adequacy decisions are made is both flawed and arbitrary, resulting in an unequal awarding of decisions and creating a barrier to non-EU companies wishing to do business in the EU.[112] It will then go on to show that because of the difficulties facing non-EU companies, data localization is becoming an attractive alternative to avoid fines under the GDPR.[113]

The second section will demonstrate how the system of awarding adequacy decisions, the compliance requirements for non-EU companies, and the seeming solution of data localization, work together to render the GDPR in violation of the GATS.[114] Finally, Part III will examine whether under Article XIV of the GATS, the EU

109. *See id.* (alleging that provisions in measures instituted by China limited the importation rights of certain reading materials, sound recordings, and films to wholly State-owned enterprises in violation of the GATS).

110. *See The People's Republic of China – Schedule of Specific Commitments*, WTO Doc. GATS/SC/135 (Feb. 14, 2002) (including sound recording distribution services as a commitment meaning that any treatment given to foreign suppliers of such services must conform to that given to domestic suppliers and cannot unfairly restrict competition).

111. *China – Trading Rights*, *supra* note 108.

112. *See infra* Part III.A.i.

113. *See infra* Part III.A.ii.

114. *See infra* Part III.B.i–ii.

could put forward a defense of the GDPR.[115]

A. A DIGITAL BLOCKAGE: WHY THE GDPR IS A BARRIER TO TRADE

1. Is it Enough?: Adequacy Decisions and the Difficulty of Meeting GDPR Standards

The GDPR is an extensive and highly regulatory piece of legislation dealing with data protection.[116] With that in mind, it is natural that other countries outside of the EU will not have the same internal requirements for data protection—some may be more stringent, while others may take a more relaxed approach to the protection of personal data.[117] The European Commission understood this when drafting the GDPR, and sought to resolve issues that might arise from companies doing business transnationally.[118]

To address this, the Commission included the concept of adequacy decisions, a concept that predated the GDPR, having first started during the time of the DPD and incorporated within the same.[119] The idea behind the adequacy decisions is that those countries that have been awarded one are deemed to have data protection legislation on par with that of the EU, thereby ensuring that data subjects could feel secure in any transfer of data from within the EU to that third country.[120]

---

115. *See infra* Part III.C.

116. *See, e.g.*, *Data Protection in the EU*, EUR. COMMISSION, https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en (last visited Oct. 6, 2019) (explaining the outline of what the GDPR is and does, including the various subcommittees and working groups established by the European Parliament to ensure compliance with the regulation).

117. *See Vagts Roundtable*, *supra* note 54 (explaining that while some countries may not meet GDPR requirements, some have in fact exceeded the GDPR in data protection standards).

118. *See Adequacy Decisions*, *supra* note 45 (explaining the importance of the adequacy decisions and the reasoning behind their creation under the requirements set forth in Article 45 of the GDPR).

119. *See id.* (stating that the following countries have received adequacy decisions: Andorra, Argentina, Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay – a total of eleven countries in the twenty-two years the adequacy decisions have been in effect).

120. *See generally id.* (explaining the four-step process by which a country can

In reality, however, there are countries with incredibly strong data protection laws that do not appear on the list, as the EU does not have a monopoly on the concept of safety in personal data processing.[121] South Korea has been waiting since 2015 for a decision despite being a country where a violation of data protection laws can result in imprisonment with prison labor for a term ranging from one to ten years as well as fines as high as 100 million won, which says much about the arbitrariness of the decision making process.[122] As can be seen by the foregoing example, the waiting time for a country to be certified as adequate can be years, resulting in those countries that are waiting being unable to do business easily in the EU in the meantime.[123]

Not on the list of eleven countries with full adequacy are Canada and the United States, both of which are governed by separate agreements.[124] Prior to the implementation of the GDPR, the United States was covered by the Safe Harbor Framework, which allowed companies that were self-certified under its principles to transfer data from the EU to the US.[125] However, in 2015 Safe Harbor was

---

obtain an adequacy decision allowing for the free transfer of data between the EU and that country: a proposal from the European Commission; an opinion from the European Data Protection Board; an approval from representatives of EU countries (the number of countries which must approve is not specific); and the final adoption of the decision by the European Commission).

121. *See Vagts Roundtable*, *supra* note 54 (mentioning that despite South Korea having incredibly strict data protection laws, it has not been granted an adequacy decision).

122. *See* PIPA, *supra* note 56 (noting that PIPA was first enacted in 2011, a year before the GDPR was even proposed in the European Parliament).

123. *See Adequacy Decisions*, *supra* note 45 (showing that South Korea has been "in discussions" around an adequacy decision since 2015); *see also Vagts Roundtable*, *supra* note 54 (noting that in the twenty-two years that adequacy decisions have been being determined, only eleven countries have qualified, making it somewhat of a failed concept).

124. *See* EU-Canada Commission Decision, *supra* note 47 (laying out the rules governing the transfer of data from the EU to Canada and the circumstances under which transfers can occur as transfers are restricted to specific sectors and companies); *see also* EU-U.S. Privacy Shield, *supra* note 47 (instituting the requirements of self-certification under Privacy Shield to allow for companies to transfer data from the EU to the US, and replacing the previously instated Safe Harbor framework after its invalidation by the Court of Justice of the European Union (CJEU)).

125. *See U.S.-EU Safe Harbor Framework*, *supra* note 50 (explaining the Safe

invalidated by *Schrems v. Data Protection Commissioner*, and a new framework, Privacy Shield, was instituted.[126]

This new framework still required companies to self-certify under a set of principles to be considered adequate under the GDPR.[127] Unfortunately, Privacy Shield too came under scrutiny from the CJEU in a case, again brought by Schrems, which in July 2020 resulted in Privacy Shield's invalidation, leaving the United States with no adequacy decision governing the transfer of data.[128] The ruling did leave intact some methods for cross-border data transfer, however many companies will find themselves facing new problems of where they can legally host their data.[129]

Harbor Framework that acted as the predecessor to Privacy Shield before its invalidation in 2015).

126. *See* Schrems, 2015 EUR-Lex CELEX LEXIS, at ¶ 107 (ruling that the Safe Harbor arrangement permitting the transfer of personal data from the EU to the United States must end because it did not provide the requisite legal protection under EU law and was therefore invalid); *see also* EU-U.S. Privacy Shield, *supra* note 47.

127. *See Privacy Shield Overview*, *supra* note 52 (laying out the requirements for companies should they wish to be covered by Privacy Shield, including self-certification processes and maintenance of such certification).

128. *See* Data Prot. Comm'r, 2020 EUR-Lex CELEX LEXIS at ¶ 201; Padraic Halpin, *Irish Supreme Court Rejects Facebook Bid to Block ECJ Data Case*, REUTERS (May 31, 2019), https://www.reuters.com/article/us-europe-privacy-ireland/irish-supreme-court-rejects-facebook-bid-to-block-ecj-data-case-idUSKCN1T112I (explaining how a new privacy case against Facebook—brought by the same man who brought the case invalidating Safe Harbor—that was referred to the CJEU from the Irish Supreme Court could result in the Privacy Shield agreement being invalidated much the same way as the Safe Harbor agreement); *see also Adequacy Decision*, *supra* note 45 (showing that without the Privacy Shield agreement, companies from United States cease to be allowed to have data transferred to the United States from the EU as there is no adequacy decision in place).

129. *See* Caitlin Fennessy, *The 'Schrems II' Decision: EU-US Data Transfers in Question*, IAPP (July 16, 2020), https://iapp.org/news/a/the-schrems-ii-decision-eu-us-data-transfers-in-question/ (explaining the CJEU ruling and how Standard Contractual Clauses – the contracts between two legal entities to control data flow – can still exist, though under strict scrutiny); Natasha Lomas, *Europe's Top Court Strikes Down Flagship EU-US Data Transfer Mechanism*, TECHCRUNCH (July 16, 2020), https://techcrunch.com/2020/07/16/europes-top-court-strikes-down-flagship-eu-us-data-transfer-mechanism/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAABX2dBLdVm-tQ-9AHYpIkI50d6v_ldIL4BtlPyPOUWe4yf5NQDfxdopUcuySo-ZyyH7-

2. You're Not from Around Here: Data Localization and the Obstacles It Creates

With all of these roadblocks facing non-EU companies, data localization offers a solution to help come into compliance.[130] Generally agreed to be an NTB, data localization requires that data be held on site-specific servers regardless of the location of the holding company.[131] The result is intended to be an enhanced economy in the host country at the expense of the holding company.[132]

While the GDPR itself does not contain any explicit data localization requirements, data localization has essentially become a de facto requirement since the GDPR's implementation.[133] This is especially true for companies based in countries not covered by an adequacy decision as those companies have even less of a choice in how to self-organize to continue to operate within the EU.[134]

O8_MvPvFS6gXJk6nDCh7B3sYuu_jpbu-YuUT0uiurh0q2CPH1hBwgCDM7HVqwtDyMPo-jQ-X3_GrDk_p3DJP-oQqYx_bCn3DHh0Y4Tgq (suggesting that one major effect of this ruling is that more US companies will be pushed to switch to regional data processing for European users).

130. *See* Roe, *supra* note 63 (suggesting that one way to mitigate risk caused by the new GDPR regulations is to create an EU-based subsidiary that would be solely responsible for handling all European data).

131. *See, e.g.*, Cohen, *supra* note 61, at 107 (noting that some speculate that data localization is less about protecting data and more about protecting trade by requiring local data storage as a method to boost domestic technology economies at the expense of foreign competitors); *see also* W. Kuan Hon et al., *Policy, Legal and Regulatory Implications of a Europe-Only Cloud*, 24 INT'L J.L. INFO. TECH. 251, 255 (2016) (laying out possible policy reasons behind the idea of a "Europe-only" cloud while commenting that some, like gaining a commercial advantage over U.S. rivals, may remain undeclared).

132. *See* Cohen, *supra* note 61, at 108 (arguing that despite the idea behind data localization being to privilege the host country at the expense of the foreign company, what in fact occurs are increased costs enacted by said company to offset its loss, costs that then get passed along to the consumer).

133. *See* Lakshmanan, *supra* note 62 (reporting that the lack of a local data center was a contributing factor to banning Microsoft Office 365 from use in German schools once the GDPR came into effect in May 2018).

134. *See, e.g.*, Ivana Kottasová, *These Companies are Getting Killed by GDPR*, CNN BUS. (May 11, 2018), https://money.cnn.com/2018/05/11/technology/gdpr-tech-companies-losers/index.html (illustrating the extent to which companies will have to change in order to work under the GDPR and how some are simply pulling out of the EU rather than paying to compete).

In 2018, Microsoft Office 365, which was previously used by students in the German state of Hesse, was deemed to no longer be in compliance with the GDPR.[135] This decision hinged in part on Microsoft's closing of its German data centers, which would mean the students' data was being transferred to U.S. servers for data processing.[136] An alternative offered was to switch from Microsoft Office to an application with on-premise license, allowing the data to be processed and held locally.[137] Should Microsoft Office return to hosting the data on in-country servers, this alternative would not be necessary.[138] Notably, Microsoft is one of the companies that had self-certified under Privacy Shield.[139] This goes to show that, as had been predicted, Privacy Shield itself may not have been sufficient to protect United States-based companies.[140]

Because of restrictions like those in Hesse governing how the data of EU nationals must be handled, many companies will find it easier to manage compliance by simply localizing all EU data within the EU.[141] Some companies are taking an alternate route and have already withdrawn from the EU as it is simpler to do so than to restructure in a manner as to come into compliance.[142] A handful of those choosing

135. *See Statement by Hessian Commissioner*, *supra* note 65 (announcing that while in general the use of cloud applications by schools is not a problem under the GDPR, the way in which Microsoft handled the data has created a violation).

136. *See* Lakshmanan, *supra* note 62 (detailing the various reasons under the GDPR that Microsoft Office was pulled from schools in Germany).

137. *See Statement by Hessian Commissioner*, *supra* note 65 (outlining possible interim solutions that can be used until an agreement can be reached with Microsoft to allow for its use again in Hessian schools).

138. *See id.* (stating that any privacy-compliant solution is not up to the Hessian Commissioner to propose and enact, but rather must be resolved by Microsoft itself in addressing how the company handles its data).

139. *See Microsoft Corporation*, PRIVACY SHIELD FRAMEWORK, https://www.privacyshield.gov/participant?id=a2zt0000000KzNaAAK&status=Active (last visited Oct. 5, 2019) (showing that even as the decision in Hesse was made to remove Microsoft from schools, Microsoft was certified under Privacy Shield).

140. *See* Roe, *supra* note 63 (explaining that companies cannot solely rely on Privacy Shield to make themselves GDPR compliant and, more to the point, that they should not rely on the framework because of potential risks).

141. *See id.* (suggesting that localizing is the easiest solution—and in some cases it is in fact the best solution for a foreign company).

142. *See, e.g.*, Alex Hern & Martin Belam, *LA Times Among US-Based News Sites Blocking EU Users Due to GDPR*, GUARDIAN (May 25, 2018), https://www.theguardian.com/technology/2018/may/25/gdpr-us-based-news-

to withdraw were at the time Privacy Shield-certified yet clearly felt this was not sufficient to keep them from violating the GDPR, despite the fact that the express purpose of Privacy Shield was to act as an adequacy decision.[143]

i. A Million Euro Problem: GDPR Fine Implementation Since 2018

Despite only being in effect for a little over a year, it has become clear that EU countries are not hesitating to enforce their rights under the GDPR against companies they find to be in violation.[144] The manner in which fines under the GDPR are structured allows for a maximum of either €20 million or 4% of a company's annual worldwide revenue—whichever is greater.[145] Current fines for companies such as Marriott,[146] British Airways,[147] and Google[148] show

---

websites-eu-internet-users-la-times (reporting on the variety of non-EU based companies that shut off access to EU users on the occasion of the GDPR going into effect, including the Los Angeles Times, the Chicago Tribune and all Tribune subsidiaries).

143. *See generally List: Active*, PRIVACY SHIELD FRAMEWORK, https://www.privacyshield.gov/list (last visited Oct. 6, 2019) (listing all the countries currently certified under Privacy Shield and showing that even some that have self-certified still chose to withdraw operations from the EU due to GDPR compliance concerns).

144. *See* Romain Dillet, *French Data Protection Watchdog Fines Google $57 Million Under GDPR*, TECHCRUNCH (June 29, 2019), https://techcrunch.com/2019/01/21/french-data-protection-watchdog-fines-google-57-million-under-the-gdpr/ (reporting on the first major fine to be issued under the GDPR).

145. *See Fines/Penalties*, GDPR-INFO, https://gdpr-info.eu/issues/fines-penalties/ (last visited Oct. 6, 2019) (noting that the €20 million or 4% penalties are for the most severe violations, while lesser violations can be fined a maximum of €10 million or 2% of the companies worldwide revenue, whichever is greater).

146. *See* Matthew Schwartz, *Marriott Faces $125 Million GDPR Fine Over Mega-Breach*, BANK INFO SECURITY (July 9, 2019), https://www.bankinfosecurity.com/marriott-faces-125-million-gdpr-fine-over-mega-breach-a-12753 (reporting that the U.K. Information Commissioner's Office alerted Marriott that it intends to issue a £99,200,396 fine under the GDPR for a data breach).

147. *See id.* (reporting that the U.K. Information Commissioner's Office has also announced it will be fining British Airways £184 million for security failures that led to two data breaches).

148. *See* Dillet, *supra* note 144 (reporting that Google was fined $57 million by CNIL, a French data protection watchdog, for issues with transparency and consent).

that the EU is serious about compliance with the GDPR.[149] While there have been no fines levied on the basis of data transfer to third countries, that does not mean those fines are neither infeasible nor imminent.[150] It is clear from the number of fines issued, even those that seem so small as to be almost negligible, there is a taste for enforcement within the EU.[151]

B. IMPEDING A SERVICE: HOW THE GDPR IS IN VIOLATION OF THE GATS

1. Everyone Can Enter: The Equal Access Requirements of Article XVI

Each Member State in the WTO has, in relation to the GATS, a specific schedule of commitments which relate to specific sectors of services.[152] These govern which services Members must commit to the requirements spelled out in the market access and national treatment articles of the GATS.[153] Commitments can be added at a Member's discretion and systems exist to determine how a Member can remove a service from a schedule.[154]

Article XVI (market access) of GATS requires that WTO Members must provide access to foreign suppliers from these sectors and that those suppliers be treated no less favorably than domestic ones.[155] Additionally, as noted in Footnote 8 of the original agreement, when a market access commitment has been made in a schedule, that

149. *See GDPR Fine Tracker*, COREVIEW, https://www.coreview.com/blog/alpin-gdpr-fines-list/ (last visited Oct. 6, 2019) (showing that since the GDPR came into force a little over sixteen months ago there have been a total of €359,205,300 in fines levied).

150. *See id.* (listing the reasons for each major fine levied to date).

151. *See GDPR Enforcement Tracker*, ENFORCEMENT TRACKER, http://www.enforcementtracker.com/ (last visited Nov. 9, 2019) (listing out by country and company all 103 fines and the reasons for which they were levied under the GDPR since it came into effect in May 2018).

152. *See Schedules of Commitments*, *supra* note 74 (listing out all commitments made by WTO members by country and by sector).

153. *See id.* (explaining what a schedule of commitments determines).

154. *See GATS Objectives*, *supra* note 67 (outlining the process by which a country can add, remove, or amend, a service from its schedule).

155. *See id.* (outlining the process by which a country can add, remove, or amend a service from its schedule).

Member has thus committed to the open flow of related services.[156]

In its original commitments, the EU cited no limitations on market access for telecommunications services or data retrieval.[157] The DSB has ruled that a service that falls into one of the categories of commitments made in a schedule must be governed by regulations consistent with Article XVI. In *US – Gambling*, gambling and betting services were found to be a part of the United States' schedule of commitments, meaning that the United States could not create laws restricting Antigua and Barbuda from providing those services.[158] The GDPR, the measure in question here, arguably fits within the commitments made by the EU and therefore is governed by the EU schedule.[159] Supporting this argument is the fact that the EU did carve out a specific restriction on financial data processing within its commitments, exempting it from the market access and national treatment provisions in the GATS.[160] The specificity of the restriction allows for the inference that since only financial data was mentioned, all other data was excluded from this restriction.[161]

These adjustments to the EU's commitments were made during the tenure of the DPD as the EU's main data protection legislation, meaning the commitments were made at a time when EU lawmakers clearly understood the importance of data protection.[162] However, in

156. *See* GATS art. XVI, n.8 (explaining that when a market access commitment has been made by a Member state, that Member has thereby committed to the open flow of related services contained within that commitment).

157. *See European Communities and Their Member States: Schedule of Specific Commitments*, WTO Doc. GATS/SC/31 (Apr. 15, 1994) [hereinafter *Schedule of Specific Commitments*] (showing that the EU updated its schedule in 1997, yet applies no limits on the transport of electronic signals).

158. *See US – Gambling*, *supra* note 95 (finding that the Wire Act, the Travel Act, and the Illegal Gambling Business Act were contrary to the United States' commitments made under the market access provision of the GATS and therefore placed the United States in violation of the agreement).

159. *See Schedule of Specific Commitments*, *supra* note 157 (showing that under its commitments to Data Processing Services the EU has listed no limitations).

160. *Id.* (listing all the commitments and restrictions made by the EU).

161. *See id.*

162. *See Trade in Services - European Communities and Their Member States - Schedule of Specific Commitments - Supplement 3*, WTO Doc. GATS/SC/31/Suppl.3 (Apr. 11, 1997) [hereinafter *Trade in Services – Supplement 3*] (outlining the change in commitments showing that the EU was aware of the importance of data privacy at the time of enacting).

the time since, there has been no effort made to revisit the EU schedule of commitments in this sector, despite the passing of the GDPR and the stricter data protection laws that accompanied it.[163]

The requirements for non-EU companies under the GDPR show that these companies are being treated less favorably than intra-EU companies in violation of Article XVI (market access).[164] The necessity of establishing an EU-based representative is an additional barrier to entry for non-EU companies,[165] while the potential necessity of a company having to localize all of its processing of EU nationals' data is clear differential treatment.[166] In making its commitments and having failed to carve out an exception for digital services or personal data, the EU had committed to allow the free movement of those services between itself and other WTO members.[167] The barriers erected by the GDPR to the free flow of this data between the EU and third countries have violated this commitment and by extension, Article XVI.[168]

163. *See Trade in Services - European Communities and Their Member States - Schedule of Specific Commitments - Supplement 4*, WTO Doc. GATS/SC/31/Suppl.4 (Feb. 26, 1998) [hereinafter *Trade in Services – Supplement 4*] (showing that the most recent adjustment to the EU's schedule of commitments did not revisit the data sector).

164. *E.g.*, Veronique de Rugy, *The Tariff No One is Talking About*, THE BRIDGE (July 17, 2018), https://www.mercatus.org/bridge/commentary/tariff-no-one-talking-about (arguing that the GDPR acts as a sort of "crypto-tariff" on non-EU companies, imposing costs on them that are not reflected similarly in EU-based companies).

165. *See* GDPR, *supra* note 3, art. 27 ("Where Article 3(2) applies [referring to non-EU companies doing business in the EU], the controller or processor shall designate in writing a representative in the Union . . . [t]he representative shall be established in one of the Member States where the data subjects . . . are.").

166. *See* de Rugy, *supra* note 164 (noting that the United States International Trade Commission expects the costs associated with data processing and storage to rise considerably in addition to the negative effects that will be inflicted as a result of data localization).

167. GATS art. XVI (affirming how commitments work under the market access provision of GATS); *see also Schedule of Specific Commitments*, *supra* note 157 (outlining all the EU commitments to date).

168. *Id.*

2. *Once In, You're All the Same: The Equal Treatment Requirements of Article XVII*

Article XVII (national treatment) of the GATS requires comparable treatment of both foreign and domestic service providers.[169] Non-EU companies are finding, under the GDPR, that they are unable to continue to operate as before within the EU.[170] This is because they either originate in countries not considered to have adequate protections or because they feel that it would be too much of a financial burden to come into compliance.[171] Withdrawing effectively denies these companies access to the entire internal market of the EU.[172]

In contrast, companies located within the EU do not have these restrictions and are afforded the opportunity to operate on an open internal market.[173] The fact that non-EU companies are essentially given the option of withdrawal or data localization (if they originate in one of the 180-plus countries not covered by an adequacy decision) is a clear instance of favorable treatment towards EU companies that modifies the competition on their behalf.[174] While these options are

169. *See id.* art. XVII ("[E]ach Member shall accord to services and service suppliers of any other Member, in respect of all measures affecting the supply of services, treatment no less favorable than that it accords to its own like services and service suppliers.").

170. *See* Hern & Belam, *supra* note 142 (showing a number of non-EU companies that withdrew all their EU operations post-GDPR implementation).

171. *See Opt-ins, Consumer Control, and the Impact on Competition and Innovation: Hearing on the GDPR and CCPA Before the S. Comm. on the Judiciary*, 116th Cong. 3 (2019) (statement of Roslyn Layton, Visiting Scholar, American Enterprise Institute) (naming Williams-Sonoma and Pottery Barn as companies whose websites have gone dark and Klout, Drawbridge, and Verve as companies that have exited the EU completely).

172. *See* de Rugy, *supra* note 164; *see also* Hern & Belam, *supra* note 142 (noting that a consequence of these moves is a "Balkanized" internet).

173. *See* de Rugy, *supra* note 164 (citing concerns that the result of these withdrawals will be a two-tiered internet system). *Contra China – Trading Rights*, *supra* note 108 (illustrating an instance of restriction and the inability of a country to operate freely in an internal market).

174. *See* Hern & Belam, *supra* note 142 (mentioning that some of these companies are choosing to simply purge all their EU user data rather than risk failing to comply with the GDPR); *see also* GATS art. XVII (stating that treatment will be considered "less favorable if it modifies the conditions of competition in favor of service suppliers of the Member" and is not allowed under section 1).

not quite as draconian as measures taken by China to flatly prohibit the importation of certain services, they have the same effect.[175]

In restricting foreign companies from distribution, China was violating the requirement to afford other Members "treatment no less favorable than it accords to its own like services and service suppliers."[176] It was doing so specifically because the items in question fell under the category of one of China's commitments.[177] The restrictions on data transfers outside the EU, which fall under the category of an EU commitment, put an extra burden on non-EU companies, making access to the EU market more difficult, thereby advantaging EU companies.[178] As with China, this is a direct violation of Article XVII.[179]

C. FOR THE PROTECTION OF PRIVACY: CAN THE EU CLAIM A DEFENSE UNDER ARTICLE XIV?

As with most treaties governing trade, GATS contains exceptions.[180] If a case were to be brought before the DSB, the EU could argue its right to maintain the GDPR under one of the listed exceptions.[181] The most likely defense would be under Article XIV(c)(ii), citing protection of individual privacy.[182] While this

175. *Compare China – Trading Rights*, *supra* note 108 (finding that measures China took to prohibit the importation of films, CDs, etc. from the United States violated its commitments), *with* Lakshmanan, *supra* note 62 (illustrating how GDPR requirements have affected U.S.-based Microsoft Office and its presence in Germany).

176. GATS art. XVII.

177. *See China – Trading Rights*, *supra* note 108 (ruling that the items being distributed fell under the entry "Sound recording distribution services" in China's schedule of commitments).

178. *Schedule of Specific Commitments*, *supra* note 157 (listing out the EU's commitments); *see also* GDPR, *supra* note 3, arts. 44–45.

179. *See China – Trading Rights*, *supra* note 108 (finding that China had violated its commitments); GATS art. XVII (showing what is required under national treatment).

180. *See* GATS art. XIV (enumerating the various exceptions allowed under the GATS).

181. *Id.*

182. *See id.* art. XIV(c)(ii) (stating that there is nothing to prevent measures that are "necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Agreement including those relating to: . . . (ii) the protection of the privacy of individuals in relation to the processing and

specific exception could prove to be an excellent defense should the EU have a WTO case brought against it to challenge the GDPR, a problem may arise in how the overall GATS article is analyzed. When analyzing defenses under Article XIV, the DSB orders the analysis with the subsection first, then the chapeau.[183]

While under subsection (iii) the EU could put forward a valid argument that the GDPR falls squarely into the listed exceptions, the argument would fail under the second analysis.[184] Though the GDPR is targeted at privacy protections, to be deemed an acceptable exception it must be shown not to be "applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail."[185] In examining the countries that have not received adequacy decisions despite having strong data protection laws, it becomes clear just how arbitrary the process of making these decisions is.[186]

The best example of arbitrariness in adequacy decision-making is the case of South Korea, where even its strict data protection laws are not sufficient to allow for an adequacy decision.[187] As explained previously, South Korea has some of the strictest data privacy laws globally, with significant monetary and penal penalties for non-compliance.[188] Despite these laws which have existed since 2011,

---

dissemination of personal data").

183. *See id.* art. XIV ("Subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on trade in services, nothing in this Agreement shall be construed to prevent the adoption or enforcement by any Member of measures."); *see also U.S. – Gambling*, *supra* note 95 (outlining the two-tiered approach to analyzing exceptions to the GATS).

184. *See id.* (looking at whether the measure is "arbitrary or unjustifiable discrimination").

185. *Id.*

186. *See Adequacy Decisions*, *supra* note 45 (stating that an adequacy decision can be amended or even revoked at any time by request of the European Parliament); *Vagts Roundtable*, *supra* note 54.

187. *See also* Network Act, *supra* note 57, arts. 70–76. *See generally* PIPA, *supra* note 56, arts. 70–75 (showing the steep penalties for non-compliance).

188. *See* PIPA, *supra* note 56, arts. 70–75 (laying out the penalties for failure to comply with the protection of data privacy as required by the law, including prison sentences of anywhere from two to ten years, and monetary fines up to 100 million won).

South Korea is still waiting on a decision regarding adequacy after applying for one in 2015.[189]

However, other examples also point to the combination of unjustifiable discrimination and arbitrariness in the decision-making process. Argentina, one of the only eleven countries granted adequacy,[190] was granted its adequacy before even implementing its data protection law.[191] When Monaco, which is not currently a country covered by an adequacy decision, was working to enact laws to obtain such a decision, the organization tasked with producing preliminary reports on adequacy sought to assist it.[192] In direct contrast, however, when assessing Quebec and Canada, no steps were taken to assist in adjusting the system.[193] Just these three examples of the application of the adequacy decisions make it clear how arbitrary and easily influenced the process is.

Arguing that data protection is a fundamental right and protected under Article XIV(c)(ii) becomes more difficult the more closely the adequacy process is examined.[194] The less transparency employed by

189. *Compare Adequacy Decisions*, *supra* note 45 (noting that South Korea has been in adequacy talks since 2015), *with* Stoddart, *supra* note 59, at 147 (explaining that Argentina hadn't even instituted its protection laws before receiving an adequacy decision).

190. *See Vagts Roundtable*, *supra* note 54 (pointing out that only eleven countries have been granted adequacy in twenty-two years and that even after accounting for the twenty-eight member states of the EU, there are still 156 countries not covered by an adequacy decision).

191. *See* Stoddart, *supra* note 59, at 147 (noting that before it had implemented its data protection law or even had expressed any clear idea of how enforcement would be approached, Argentina was awarded an adequacy decision).

192. *See id.* (explaining that Commission nationale de l'informatique et des libertés (CNIL)—the organization that issues preliminary adequacy reports—took "positive steps not only to seek clarification in the law but also to broker a deal to ensure that these practices did eventually meet the requirements of the Data Protection Directive," a clear exercise of discretion in favor of Monaco).

193. *See id.* (comparing the inaction in the case of Quebec, where CNIL took no steps to contact any governmental figure to clarify how provincial and federal data laws worked in concert, to the excessively helpful steps taken with Monaco).

194. *See, e.g.*, Monika Ermert, *EU Parliament Hearing: Data Protection not a Trade Barrier but a Fundamental Right*, INTELL. PROP. WATCH (June 18, 2015), https://www.ip-watch.org/2015/06/18/eu-parliament-hearing-data-protection-not-trade-barrier-but-fundamental-right/ (reporting the discussions around the implications of the GDPR before its creation and implementation and the assertions that it would be the "gold standard" for privacy protections without acting as a

the decisionmakers, and the more countries with objectively strong data-protection laws that fail to receive decisions, the more arbitrary the process appears.[195] As a result, a defense that the GDPR is an acceptable exception would probably fail under the chapeau of Article XIV.

That a defense put forward by the EU would most likely fail is in line with the history of the GATS Article XIV and its counterpart, GATT Article XX.[196] In the years since the establishment of the WTO, defenses under the exceptions articles have been raised on forty-four occasions,[197] and only once has a defense been raised under the GATS.[198] Of those forty-four occasions for which an exception has been invoked, only once has the invocation succeeded.[199] Parties have failed for a number of reasons: in twelve cases, the panel or appellate body deemed the exception irrelevant; of those remaining, five failed to meet the subject matter threshold, a further eighteen failed the qualifier threshold,[200] and then of the remaining nine, eight failed under the chapeau.[201] The one case that did succeed was *EC – Asbestos*, a case invoking GATT Article XX.[202] In the one case where the GATS Article XIV was invoked, *US – Gambling*, the WTO panel

barrier).

195. *E.g.*, Stoddart, *supra* note 59, at 147–48 (highlighting the absolute lack of transparency or clear precedent apparent in the European Commission's decision making process around the adequacy decisions); *see also Adequacy Decisions*, *supra* note 45 (providing only the barest details about the adequacy process).

196. *See One of 44 Attempts*, *supra* note 98 (showing that a defense invoking the GATT Article XX/GATS Article XIV exceptions has succeeded only three percent of the time—or phrased differently, has succeeded once).

197. *See id.* (tracking the history of the GATT Article XX/GATS Article XIV since its introduction after the establishment of the WTO).

198. *See US – Gambling*, *supra* note 95 (invoking the GATS Article XIV(a) and (c) as a defense); *see also* Cottier et al., *supra* note 92 (noting the single instance of the GATS Article XIV being invoked, despite it failing).

199. *One of 44 Attempts*, *supra* note 98 (showing that only one invocation of the GATT Article XX was successful).

200. *See* GATT art. XX (showing that a matter be "necessary" or "related to" one of the exceptions to meet the qualifier threshold).

201. *One of 44 Attempts*, *supra* note 98 (laying out how and why various invocations of the exceptions have failed).

202. *See generally EC – Asbestos*, *supra* note 99 (invoking successfully a GATT Article XX(b) defense for France's ban on the importation of asbestos and products containing asbestos by showing that the measure was necessary to protect life or health and that no other reasonable alternative exists).

found that the United States failed the necessity threshold.[203]

This history of invoking the GATS Article XIV/GATT Article XX shows the unlikelihood of success for any future respondent hoping to use these exceptions as a defense.

IV. RECOMMENDATIONS

Part IV of this comment lays out two recommendations to the EU and to the international community, respectively, to resolve the tension between data protection and the global free flow of information caused by the GDPR. The first section suggests that the EU look to ways to eliminate any possibility of de facto data localization requirements. It also suggests that the EU also find ways to expand the adequacy decisions granted, creating a system that is both more transparent and less arbitrary.

The second section recommends an avenue that the international community could use to bring a case against the EU outside of the WTO by bringing a policy argument before the European Commission.

A. WHAT CAN EU DO?: POSSIBLE EU RESPONSES TO THE ISSUES RAISED

The first step the EU can take to mitigate some of the issues caused by the GDPR is to pass a regulation determining that no Member state be permitted to enact an express data localization law. Both Germany and France have already proposed instituting express data localization laws, proposals which were not well received by the European Commission.[204] That the Commission reacted negatively to those laws bodes well for any proposed legislation forbidding others from doing the same.[205] However, any regulation forbidding data localization

203. *See US – Gambling*, *supra* note 95 (finding that the measures implemented were not necessary to protect public morals (GATS art. XIV(a)) because there existed reasonable alternatives to the measure enacted).

204. *See* Blume, *supra* note 80 (commenting on the proposed Schengen Cloud that would localize data within the EU).

205. *See* Sam Pfeifle, *Is the GDPR a Data Localization Law?*, IAPP (Sept. 29, 2017), https://iapp.org/news/a/is-the-gdpr-a-data-localization-law (arguing that data localization can lead to the Balkanization of the internet which should be avoided if possible).

would have to go through the entire process of proposal and deliberation before being enacted, making it more of a long-term solution.[206] Regardless, it would be well worth the EU's time to commence the passage of such a law to pre-empt any future attempts to require data localization.[207] Any EU legislation prohibiting country-specific data localization laws will not, however, address the main issue—the difficulty of compliance with the GDPR for non-EU countries and companies.

The more important solution is to work on adjusting the adequacy decisions. The fact that there have only been eleven countries to receive such a decision in the twenty-two years since the decision-making process has started speaks to an inadequacy in the process itself.[208] To rectify this the EU can do one of two things: firstly, it can streamline the process;[209] secondly, it can work closely with countries to identify where the issues are and what can be done specifically to fix them.[210] A crucial part of streamlining the adequacy decision process would be making it more transparent and the decisions more clear-cut.[211]

206. *See generally How EU Decisions are Made*, EUR. UNION, https://europa.eu/european-union/eu-law/decision-making/procedures_en (last visited Oct. 6, 2019) (outlining the process of enacting a law in the EU starting with the initial impact assessments and consultations, then the proposal of the initiative by the Commission, the review by the European Parliament and the Council, the amendments proposed by those bodies, the return of the legislation to the Commission for the incorporation of the amendments, then finally back to the Parliament for a final vote).

207. *See* Cohen, *supra* note 61, at 108 (noting the negative impacts of data localization laws on the free flow of data and trade).

208. *See Vagts Roundtable*, *supra* note 53.

209. *See* David Meyer, *South Korea's EU Adequacy Decision Rests on New Legislative Proposals*, IAPP (Nov. 18, 2018), https://iapp.org/news/a/south-koreas-eu-adequacy-decision-rests-on-new-legislative-proposals/ (noting that South Korea has been waiting for an adequacy decision since the it applied in 2015).

210. *See Vagts Roundtable*, *supra* note 54 (pointing out that the EU took initiatives to try to help Monaco adjust its systems yet, despite being asked, did not afford Quebec the same courtesy).

211. *See* Stoddart, *supra* note 59, at 147–48 (showing how arbitrary the adequacy decision-making process really is and that some countries are held to different standards than others); *see also* Wilbur Ross, *EU Data Privacy Laws are Likely to Create Barriers to Trade*, FIN. TIMES (May 30, 2018), https://www.ft.com/content/9d261f44-6255-11e8-bdd1-cc0534df682c (arguing that while privacy is an important issue, the guidelines of the GDPR and its

In a rapidly expanding digital world, more of everyday life is migrating to the internet and with that migration, the hosting of personal data.[212] The expansion of the adequacy decisions, or at the very least an adjustment to the process of awarding them, is necessary to maintaining this growing digital world.[213] Keeping countries waiting years to be able to operate freely in the EU will stifle digital innovation and could result in the EU being left behind—arguably the opposite of what the GDPR is intended to do.[214] To encourage the free flow of data, the adequacy decision process must be updated.

B. WHAT CAN WE DO?: AN AVENUE FOR BRINGING A CASE AGAINST THE EU.

Should the EU, or more specifically the European Commission, choose not to independently address the internal process by which adequacy decisions are made, then the onus would shift to the international community to bring a case to induce this change. As noted in Part II(B)(ii) of this Comment, any attempt to bring a case against the EU before the WTO would likely prove futile as a result of the current state of the DSB with the Appellate Body no longer operational.[215] A complaint to the DSB, however, is not the only way in which a case could be brought, as there exist two intra-EU paths to challenge the effects that the lack of transparency in the adequacy decision process has on non-EU companies doing business or located in the EU.

One of the many institutions that make up the EU is the European

---

implementation are too vague and encourage an unpredictable regulatory environment).

212. *See* Grant Kirkwood, *The Three Phases Of Digital Transformation: Simplifying Migration To The Hybrid Cloud*, FORBES (July 20, 2017), https://www.forbes.com/sites/forbestechcouncil/2017/07/20/the-three-phases-of-digital-transformation-simplifying-migration-to-the-hybrid-cloud/#4e659a6619ff (illustrating the many ways in which people's lives are moving online and how this is affecting the fundamental ways in which companies must now adapt to operate well in a digital world).

213. *See id.*

214. *See* de Rugy, *supra* note 164 (noting that Europe lags behind in the technology sector and suggesting that some of the intent behind the GDPR was to ameliorate that).

215. *See supra* Part II.B.ii (commenting on the dissolution of the DSB Appellate Body due to the United States' blocking of new appointees).

Ombudsman.[216] Responsible for overseeing the integrity of the EU institutions as a whole, the Ombudsman investigates complaints about maladministration by EU governing bodies.[217] Among the types of poor administration investigated are abuse of power, discrimination, disproportionate application of law, and lack of transparency.[218] Both transparency and proportionality, as principles, are enshrined in the EU constitutional framework as being essential foundations of an effective democracy.[219]

The services of the Ombudsman are available to citizens or residents of EU countries, or to EU-based companies.[220] Therefore, a non-EU company originating in a country not covered by an adequacy decision—South Korea, for example—but located for business purposes in France, could be positioned to submit a complaint concerning the European Commission's lack of action in addressing the lack of transparency and discrimination in its adequacy decisions to the Ombudsman.[221] In making its complaint, the company could argue that making South Korea wait five years (and still ongoing) for an adequacy decision when it has some of the strictest data protection regulations is discriminatory and is having a disproportionate effect

216. *See generally Institutions and Bodies*, EUROPA.EU, https://europa.eu/european-union/about-eu/institutions-bodies_en (last visited Feb. 25, 2020) (listing out all of the institutions and bodies that make up the European Union).

217. *See European Ombudsman*, EUROPA.EU, https://europa.eu/european-union/about-eu/institutions-bodies/european-ombudsman_en (last visited Feb. 25, 2020) (laying out the role of Ombudsman and how that role is meant to work within the EU governing system).

218. *See, e.g.*, *id.* (outlining the types of investigations of poor administration the Ombudsman oversees).

219. *See* Robert Panizza, Directorate-General for Internal Policies, *Briefing for the PETI Committee*, POL'Y DEP'T FOR CITIZENS' RTS. & CONST. AFF. – EUR. PARLIAMENT (Mar. 2019) (describing the paramount importance of transparency across all EU institutions and bodies as "essential prerequisites of a democracy based on the rule of law"); *see also* Consolidated Version of the Treaty on European Union art. 5.4, Mar. 30, 2010, 2010 O.J. (C 83) 18 [hereinafter TEU] ("The institutions of the Union shall apply the principle of proportionality as laid down in the Protocol.").

220. *See European Ombudsman*, *supra* note 217 (stating who can bring a complaint to the Ombudsman against an EU institution).

221. *See id.* (highlighting specifically that EU-based associations or businesses have standing to bring a complaint of maladministration against an EU institution to the Ombudsman).

on the company's ability to do business in the EU.[222]

The European Commission's continued lack of transparency around how adequacy decisions are awarded and the arbitrary and discriminatory way in which the decisions have thus far been awarded puts the Commission in clear violation of the general EU principles of transparency and proportionality.[223] Bringing a complaint against the Commission would be the first step in addressing the changes that are crucial to fixing the adequacy decision system.[224] While this process is a good move in encouraging the Commission to change its process for awarding adequacy decisions, it is not a full solution to the problem as the Ombudsman does not have the power to issue injunctions.[225] The CJEU, however, does possess that power[226] and often non-EU companies located in Europe have brought their claims before the CJEU for a violation of an individual economic right or of a violation of a general principle of EU law.[227]

The European Court of Justice released Opinion 1/94 in 1994, which responded to European Community (the precursor to the EU) questions regarding under whose competence the GATS fell, and

222. *See Adequacy Decisions*, *supra* note 45; *supra* Part III.B.ii.

223. *See Adequacy Decisions*, *supra* note 45 (showing how opaque the European Commission's procedure for offering an adequacy decision is); TEU, *supra* note 219, art. 5.4 (incorporating GATS principles into EU law); Panizza, *supra* note 219 (stressing the importance of transparency in all EU governing bodies).

224. *See Make a Complaint*, EUR. OMBUDSMAN, https://www.ombudsman.europa.eu/en/make-a-complaint (last visited Feb. 25, 2020) (outlining the complaint process for any individual or company wishing to bring a complaint against an EU institution for maladministration).

225. *See European Ombudsman*, *supra* note 217 (outlining what the Ombudsman has the power to do).

226. *See Court of Justice of the European Union (CJEU)*, EUROPA.EU, https://europa.eu/european-union/about-eu/institutions-bodies/court-justice_en (last visited Mar. 3, 2020) [hereinafter *CJEU*] (providing an overview of the powers of the CJEU, including the power to sanction EU institutions).

227. *See, e.g.*, Case C-213/89, The Queen v. Sec'y of State for Transp. ex parte Factortame Ltd., 1990 E.C.R. 1-2433 (showing the power of the CJEU (then the ECJ) to take immediate review of a case and issue a preliminary injunction if necessary); Case C-72/15, PJSC Rosneft Oil Co. v. Her Majesty's Treasury, Sec'y of State for Bus., Innovation, & Skills, 2017 EUR-Lex CELEX LEXIS ¶¶ 30–32 (Mar. 28, 2017) (arguing that sanctions were enforced against Rosneft in violation of the EU principles of proportionality).

which ultimately incorporated the GATS principles into EU law.[228] The incorporation of these principles into the Common Commercial Policy of the EU, through Articles 206 and 207 of the Treaty on the Functioning of the European Union, gives exclusive competence to the EU in this subject matter.[229] Arts. 206 and 207 are the hook by which EU law will apply to any case brought before the CJEU arguing a violation of the GATS under EU law.[230]

Using again the above example of a South Korean company doing business in France, the first step—should the Commission decline to review the issue—is for the company to bring a case before the French national courts for a violation of their right to freely pursue its business as any other EU company can.[231] The case could then be referred through a preliminary question to the CJEU by showing that due to a lack of an adequacy decision by the Commission (acting in violation of EU transparency and proportionality principles) the right of the South Korean company to freely pursue economic activity without being discriminated against has been impaired.[232]

It is through this system of bringing a case before the CJEU that the issues around the transparency and proportionality of the Commission's process for awarding adequacy decisions can be addressed by a body with the power to issue an injunction requiring substantive changes to the process.[233]

228. Opinion 1/94, Competence of the Community to Conclude International Agreements Concerning Services and the Protection of Intellectual Property, 1994 E.C.R. I-5267 [hereinafter Opinion 1/94].

229. Consolidated Version of the Treaty on the Functioning of the European Union arts. 206–207, May 9, 2008, 2008 O.J. (C 115) 47 (outlining Common Commercial Policy).

230. *Id.*

231. The company would be advised to make its argument under the Common Commercial Policy. *See id.*

232. *See* TEU, *supra* note 219, art. 5.4 (allowing, in essence, for the system of awarding adequacy decisions but not permitting them to be awarded in such an arbitrary way as to impede business).

233. *CJEU*, *supra* note 226 (outlining the competences of the Court of Justice).

V. CONCLUSION

Under Articles XVI and XVII of GATS, the EU has an obligation not to institute any measures that favor domestic suppliers of services over foreign ones.[234] The requirements contained in the GDPR with respect to the operations of non-EU companies and the requirement of an adequacy decision for a country where the transfer of data to said country is sought, place an undue burden on these companies, disfavoring them against EU companies.[235] In doing so, the GDPR is acting in violation of the GATS Articles XVI (market access) and XVII (national treatment).[236] Because the process by which these adequacy decisions allowing for the transfer of data to third countries is both arbitrary and unfairly applied, the EU does not have access to the exception for data protection listed at subsection (c)(ii) of Article XIV of the GATS because any analysis fails under the chapeau.[237] Therefore, unless changes are made to either the adequacy decision process or the ways in which data may be transferred out of the EU to third countries, the GDPR will remain in violation of the GATS and open to potential litigation by affected companies.

234. *See supra* Part II.B.
235. *See supra* Part III.A.
236. *See supra* Part III.B.
237. *See supra* Part III.C.