# The Best of Both Worlds? Free Trade in Services and EU Law on Privacy and Data Protection

Yakovleva, S.; Irion, K.

DOI
10.21552/EDPL/2016/2/9

Publication date
2016

Document Version
Author accepted manuscript

Published in
European Data Protection Law Review

This is a prepublication version of the article S. Yakovleva and K. Irion, "The Best of Both Worlds? Free Trade in Services, and EU Law on Privacy and Data Protection," (2016) *European Data Protection Law Review* 2(2): 191-208.

# The Best of Both Worlds? Free Trade in Services, and EU Law on Privacy and Data Protection

*Svetlana Yakovleva and Kristina Irion*

*The article focuses on the interplay between European Union (EU) law on privacy and data protection and international trade law, in particular the General Agreement on Trade in Services (GATS) and the WTO dispute settlement system. The argument distinguishes between the effects of international trade law in the EU legal order on the one hand, and, on the other hand, how EU data protection law would fare in a hypothetical challenge under the GATS. The contribution will apply international trade law and the general exception in GATS Article XIV to typical requirements stemming from EU data protection law, especially on transfers of personal data to third countries. The article enumerates the specific legal risks for defending EU law on privacy and data protection and explains the practical implications of its hypothetical challenge under the GATS. These insights could be useful for the EU's negotiators of the future bi- or multilateral free trade agreements, notably the Transatlantic Trade and Investment Partnership and the Trade in Services Agreement.*

## I. Introduction

Originally an economic union itself, the European Union (EU) recognises and welcomes the positive welfare effects of international trade. The EU was a founding member of the World Trade Organization (WTO) and a party to the core international trade agreements, i.e. the 1994 General Agreement on Trade and Tariffs (GATT) and the General Agreement on Trade in Services (GATS). At the present time, the EU is negotiating the next generation of bi- or multilateral free trade agreements on trade in services, especially in the area of e-commerce. These are the EU–Canada Comprehensive Economic and Trade Agreement (CETA),[1] the EU–US Transatlantic

Svetlana Yakovleva is a Senior Research Master Student at the Institute for Information Law (IViR), University of Amsterdam. For correspondence: svyakovleva@gmail.com.

Kristina Irion is a Senior Researcher at the Institute for Information Law (IViR), University of Amsterdam; Associate Professor at the School of Public Policy (SPP), Central European University, Budapest. For correspondence: k.irion@uva.nl.

The authors would like to thank Dr. S. Gaspar-Szilagyi for a valuable discussion of the interplay between EU law and international law and Dr. M.R. Taylor for English proofs.

[1] Negotiations on CETA finished in August 2014; at the moment CETA is undergoing ratification procedures in Canada and the EU <http://ec.europa.eu/trade/policy/in-focus/ceta/> accessed 8 April 2016.

Trade and Investment Partnership (TTIP)[2] and the multilateral Trade in Services Agreement (TiSA).[3]

After the Lisbon Treaty took effect in 2009, the EU has increasingly been seen as a constitutional legal order.[4] The Charter of Fundamental Rights of the European Union (the Charter) guarantees the rights to privacy and the protection of personal data respectively. EU data protection law substantiates these fundamental rights and regulates the processing of individuals' personal data. While it aims to create an internal digital market for personal data flows, the transfer of personal data to third countries is much more restricted.

WTO law and EU law are two distinct jurisdictions. EU law claims to be an autonomous legal order,[5] irrespective of the EU being a member of the WTO and a party to the GATS. In today's interconnected world, personal data is an essential ingredient of electronic trade in services, to which extensive EU data protection law can be readily perceived as a barrier to free trade. Debating the tensions between data protection law and free trade rules quickly exposes the different traditions and philosophies in EU law and in other jurisdictions, notably in the United States (US).

This article focuses on the interplay between EU law on privacy and data protection one the one hand, and, on the other hand, international trade law, in particular the GATS. It queries the effects of either legal order within the jurisdiction of the other and aims to answer the question of whether EU data protection law would be susceptible to a challenge under WTO law. In order to answer the research question, EU law and WTO law are introduced and the latter is then applied to EU data protection *aquis* and its rules on the transfer of personal data to third countries.

The issue is not new, as both GATS and EU law on data protection have been in force for more than 20 years. Parts of the ever-evolving body of literature on EU privacy and data protection law deal with international transfers of personal data.[6] WTO law, including GATS, developed into its own branch of scholarship within public international law.[7] The co-existence of EU law and WTO law cuts across both

[2] Negotiations on TTIP started in Sumer 2013.
[3] Negotiations on TiSA started in March 2013.
[4] See G de Burca, 'The European Court of Justice and the International Legal Order after Kadi' (2010) 51(1) Harvard International Law Journal, 5, R A Wessel 'The Dynamics of the European Union Legal Order: An Increasingly Coherent Framework of Action and Interpretation' (2009) 5 European Constitutional Law Review, 117.
[5] Starting as early as in 1963 from Case 26-62 *NV Algemene Transport- en Expeditie Onderneming van Gend & Loos v Netherlands Inland Revenue Administration* [1963] ECLI:EU:C:1963:1.
[6] C Kuner, 'Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law' (2015) 5(4) International Data Privacy Law 235; C Kuner, 'Developing an Adequate Legal Framework for International Data Transfers' in S Gutwirth et al (eds), *Reinventing Data Protection?* (Springer 2009); C Kuner, 'Regulation of Transborder Data Flows Under Data Protection and Privacy Law: Past, Present, and Future' (2010) TILT Law and Technology Working Paper No 016/2010 <http://papers.ssrn.com/abstract=1689483> accessed 8 April 2016; Lee Andrew Bygrave, *Data privacy Law: An International Perspective* (OUP 2014).
[7] Peter van den Bossche and Werner Zdouc, *The Law and Policy of the World Trade Organization. Text, Cases and Materials* (3rd edn, Cambridge University Press 2013); Mitsuo Matsushita, Thomas J

fields of law and has been the subject of some academic enquiry. However, little specific attention has been paid to the particularities of EU-style personal data protection regulation and, if so, mostly in the context of the EU–US Safe Harbour Agreement.[8]

Recently, in line with the rising prominence of privacy and data protection law, these issues have been taken-up more frequently by legal scholars.[9] However, very few of them elaborate on the interplay between specific GATS disciplines and EU privacy and data protection rules.[10] This literature at times proceeds from contestable conclusions about EU law on data protection. In addition, although uncertainty is inherent in any complex legal enquiry, the literature quickly arrives at the conclusion that WTO law and jurisprudence is unpredictable and uncertain. In this article, we carry out a more precise legal analysis of the effects of the GATS in EU law and how EU data protection law would fare in a hypothetical challenge under the GATS.

The article is structured as follows. Following this introduction, the next section describes the essentials of privacy and data protection in EU law, paying special attention to the regulation on the transfer of personal data to third countries. The third section offers an introduction to the GATS, WTO law and the attendant dispute resolution system before positioning the EU as a member with its own set of obligations and commitments. The fourth section then applies the GATS to EU data protection law in order to clarify the legal assessment and to obtain an understanding of the potential tensions and risks of non-compliance. The article concludes with summarising the findings and discussing their legal and practical implications. It offers a perspective on how this analysis could be relevant for policy-makers and legal research in connection with the next generation of international free trade agreements, such as CETA, TTIP, and TiSA.

---

Schoenbaum, Petros C Mavrodis and Michael Hahn, *The World Trade Organization. Law, Practice and Policy* (OUP 2015); J Pauwelyn, 'Rien Ne Va Plus? Distinguishing Domestic Regulation from Market Access in GATT and GATS' (2005) 4 World Trade Review 131.

[8] J Reidenberg, 'E-Commerce and Trans-Atlantic Privacy' (2001-2002) 38 Houston Law Review 717; G Shaffer, 'Managing US-EU Trade Relations Through Mutual Recognition and Safe Harbor Agreements: 'New' and 'Global' Approaches to Transatlantic Economic Governance?' (2002) EUI Working Papers RSC No 2002/28 <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=406940> accessed 8 April 2016 , E Shapiro, 'All Is Not Fair in the Privacy Trade: The Safe Harbor Agreement and the World Trade Organization' (2003) 71 Fordham Law Review 2781.

[9] P Keller, *European and International Media Law: Liberal Democracy, Trade and New Media* (OUP 2011); S Wunsch-Vincent, 'Trade Rules for the Digital Age' in M Panizzon, N Pohl and P Sauvé (eds), *GATS and the Regulation of International Trade in Services* (Cambridge University Press 2008); DA MacDonald and CM Streatfeild, 'Personal Data Privacy and the WTO' (2014) 36 Houston Journal of International Law 625; E-U Petersmann, 'Transformative Transatlantic Free Trade Agreements without Rights and Remedies of Citizens?' (2015) 18 Journal of International Economic Law 579.

[10] CL Reyes, 'WTO-Compliant Protection of Fundamental Rights: Lessons from the EU Privacy Directive' (2011) 12 Melbourne Journal of International Law 141; RH Weber, 'Regulatory Autonomy and Privacy Standards under the GATS' (2012) 7 Asian Journal of WTO & International Health Law & Policy 25.

## II. Privacy and Data Protection in EU Law

The right to privacy is universally recognised as a human right;[11] however, in European constitutional law this guarantee is comparatively strong. The right to personal data protection, as a right separate from the right to privacy, is a more recent development initially rooted in the legal order of the Council of Europe[12] and some EU Member States. This section describes the essentials of privacy and data protection in primary and secondary EU law, paying special attention to the regulation on the transfer of personal data to third countries.

### 1. The Rights to Privacy and Data Protection

Since January 2009, when the Lisbon Treaty gave binding force to the Charter, both the right to privacy and the right to data protection have been fundamental rights in the EU legal order.

Article 7 of the Charter protects the right to respect for private and family life, home and communications. Article 8 of the Charter not only proclaims everyone's right to data protection (paragraph 1), but also lays down the foundations of the EU data protection framework (paragraphs 2 and 3). In other words, the Charter elevates to the constitutional status of EU law the core mechanisms safeguarding this right, ie the principle of fair data processing for specific purposes on a legitimate basis specified by law, the right of access to and rectification of personal data, and the principle of independent supervision over the compliance with these rules.

EU secondary law on data protection, which chronologically precedes the Charter, substantiates the protection of the fundamental rights to privacy and personal data. The EU legal framework comprises several instruments, two of which are relevant for the purposes of this article. The 1995 Data Protection Directive (DPD)[13] sets forth provisions on the lawful processing of personal data in the public and private sectors, among others in relation to commercial activities. The other instrument is the so-called e-Privacy Directive,[14] which harnesses a sector-specific regime on data protection for the electronic communications sector.

The definitions of 'personal data' and the 'processing of personal data' in the DPD are broadly interpreted. Under Article 2(a) DPD, 'personal data' includes any information relating to an identified or identifiable natural person. 'Identifiable' does

[11] The right to privacy is explicitly named in the Universal Declaration of Human Rights (art 12), International Covenant on Civil and Political Rights (art 17) and the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR, art 8).

[12] The Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data No 108 of 28 January 1981.

[13] 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] OJ 2 281/0031 (DPD).

[14] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector [2002] OJ 2 201/0037.

not necessarily mean that the identity of the person should be known. According to Article 29 Working Party (A29WP)[15] it would be enough for information to relate to an individual if the individual can be 'singled out.'[16] The 'processing of personal data' includes any operation or a set of operations upon personal data, including its transfer within the EU and the European Economic Area (EEA),[17] and to any other third country.[18]

The Court of Justice of the European Union (CJEU) has successively strengthened the protection of the fundamental rights to privacy and data protection. Referring to Articles 7 and 8 of the Charter, the Court repeatedly highlighted the importance of the 'effective and complete protection of the fundamental rights and freedoms'[19] and of ensuring a 'high level of protection'.[20] The CJEU also clarified that the validity of EU secondary legislation which creates serious interference with these fundamental rights should be assessed against a strict fundamental rights-based review.[21]

Another important consequence of the Lisbon Treaty is that the EU now has a fully-fledged competence to legislate in the area of data protection (Article 16(2) TFEU).[22] Recently, the EU legislator adopted the General Data Protection Regulation (GDPR)[23] that will replace the DPD in May 2018. The Regulation will unify EU data protection law with the aim to modernise the legal framework in line with the needs of a personal data-intensive economy and society. A review of the e-Privacy Directive is also under way.

---

[15] The Article 29 Working Party is an advisory body set up under Article 29 DPD, composed of representatives of data protection authorities of the EU Member States, the European Data Protection Supervisor and the European Commission.

[16] Article 29 Data Protection Working Party (AWP29), 'Opinion 4/2007 on the concept of personal data' (June 2007) WP 136, 6-7, 12, 14 <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf> accessed 8 April 2016).

[17] The EEA comprises of the EU Member States plus Norway, Iceland and Lichtenstein.

[18] art 2(b) DPD, Case C-362/14 *Maximillian Schrems v Data Protection Commissioner* [2015] ECLI:EU:C:2015:650, para 45.

[19] Case C-131/12 *Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, ECLI:EU:C:2014:317, para 53; for a full analysis of the decision, see the case note by Herke Kranenborg, 'Google and the Right to be Forgotten' (2015) 1 European Data Protection Law Review 70.

[20] *Maximillian Schrems v Data Protection Commissioner* (n 18) para. 72.

[21] Case C‑293/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources*, ECLI:EU:C:2014:238, para 48; *Maximillian Schrems v Data Protection Commissioner* (n 18) para 39; MP Granger and K Irion, 'The Court of Justice and the Data Retention Directive in Digital Rights Ireland: Telling Off the EU Legislator and Teaching a Lesson in Privacy and Data' [2014] 6 European Law Review 835.

[22] H Hijmans, A Scirocco, 'Shortcomings in EU Data Protection in the Third and the Second Pillars. Can the Lisbon Treaty Be Expected to Help?' (2009) 46 Common Market Law Review 1485, 1514-1515.

[23] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), [2016] OJ L 119/1-88.

## 2. Safeguards for the Protection of Personal Data Processed Outside the EU/ EEA

The DPD's dual objective is to ensure the free flow of personal data between EU Member States (also expanded to the EEA) and to ensure the protection of an individual's right to privacy with respect to the processing of personal data through the approximation of Member States' laws on the protection of personal data (Article 1(1) and (2) DPD).

However, modern information systems and economic activities are no longer confined to geographical boundaries. Increasingly, personal data is transferred to third countries outside the EU/EEA, notably in the course of commercial activities. This takes place in two ways. First, personal data is collected directly from a data subject based in EU/EEA by a service provider established and operating from outside the EU/EEA area. Second, personal data that have originally been collected in the EU/EEA are then transferred by the controller to a third country.

In order to ensure that such transfer to a third country does not circumvent the protection afforded to personal data in the EU/EEA, EU law provides for two mechanisms.[24] First, the DPD's scope of application is rather expansive and, second, the transfer of personal data to third countries is specifically regulated in Chapter IV of the DPD.

### 2.1. Scope of Application of EU Data Protection Law

Pursuant to Article 4(1)(a) DPD, EU data protection law applies to the processing of personal data if such processing 'is carried out in the context of the activities of an establishment of the controller' in the EU. A foreign controller is deemed to have an 'establishment' in the EU if it exercises '*a real and effective activity – even a minimal one* – through stable arrangements in the territory of a Member State'.[25]

The CJEU has recently interpreted the notion of the processing of personal data 'in the context of activities of an establishment' very expansively. Even processing of personal data abroad is carried out 'in the context of an establishment' in the EU if the activities of such an establishment are *inextricably linked* to processing of personal data by a foreign controller.[26] In its ruling in the case *Google Spain v AEDP* the CJEU held that the activity of an establishment may be 'inextricably linked' when it raises revenue in the EU to finance a service that is provided by a foreign branch of the company where the processing of personal data originating in the EU takes place.[27] In

[24] Kuner, Regulation of Transborder Data Flows (n 6) 28, *Maximillian Schrems v Data Protection Commissioner* (n 18) para 73.
[25] A29WP , 'Update of Opinion 8/2010 on applicable law in light of the CJEU judgement in Google Spain' (16 December 2015) WP 179 update, 3 <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp179_en_update.pdf> accessed 8 April 2016, internal quotation marks omitted, emphasis added.
[26] *Google Spain v AEPD* (n 19) para 56; A29WP , 'Update of Opinion 8/2010' (n 25) 3.
[27] *ibid*.

the light of the ruling it is thus not necessary for the application of the DPD that the establishment itself processes personal data.[28]

Subsidiary to the situation above,[29] Article 4(1)(c) DPD applies to a foreign controller who makes use of equipment located in the EU for the purposes of processing personal data. Both equipment and its use are interpreted broadly to include any means used by a controller with the intention to process personal data.[30] Although assessed on a case-by-case basis, examples of 'equipment' could be questionnaires used to collect personal data, personal computers, mobile phones or consumer devices (such as step-counters or sleep trackers) on which software is installed through which personal data is collected and send to a controller in a third country.[31]

Once in force, the new GDPR will expand the scope of the application of EU data protection even further. The GDPR would fully apply to the processing of personal data by controllers and processors established outside the EU if their processing is related to offering goods or services, including those provided free of charge, to EU individuals or to the monitoring of individuals' behaviour within the EU (Article 3(2) GDPR).

### 2.2. Transfer of Personal Data to Third Countries

In principle, EU data protection law only allows the transfer of personal data to a third country if this country ensures an adequate level of protection (Article 25(1) DPD). In the interpretation of the CJEU 'adequate' means 'essentially equivalent' to the level of protection of fundamental rights and freedoms guaranteed by the Charter and the DPD.[32] To the CJEU, this interpretation ensures the continuity of the high level of personal data protection that is guaranteed in the EU even after personal data has been transferred to a third country.[33]

The adequate level of protection in a third country should be assessed in the light of the particular circumstances of each transfer or set of transfers (Article 25(2) DPD). In addition, the European Commission (Commission) conducts abstract assessments of a third country's legal and administrative system in relation to the

[28] A29WP, 'Update of Opinion 8/2010' (n 25) 4-5.
[29] A29WP , 'Opinion 8/2010 on applicable law'(16 December 2010) WP 179, 18 <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_en.pdf> accessed 8 April 2016.
[30] ibid 20.
[31] A29WP , 'Opinion 8/2014 on the Recent Developments on the Internet of Things' (16 September 2014), 10 <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf> accessed 8 April 2016; 'Opinion 02/2013 on apps on smart devices' (27 February 2013), 7 <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf> accessed 8 April 2016; 'Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites'(30 May 2002), 9 <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2002/wp56_en.pdf> accessed 8 April 2016; 'Opinion 8/2010 on applicable law'(n 20) 20-21.
[32] *Maximillian Schrems v Data Protection Commissioner* (n 18) para 73.
[33] *ibid* para 72.

protection of personal data ensured (Article 25(4) and (6) DPD). Where this assessment concludes with a positive finding, the Commission issues a decision on the adequate level of protection in the third country (adequacy decision). This decision is legally binding (Article 288(4) TFEU).[34] An adequacy decision provides the legal basis for transfers of personal data to this third country without additional safeguards, similar to the regime within the EU/EEA.

To date the Commission has issued adequacy decisions with respect to eleven countries. Hence, personal data originating from the EU/ EEA can also be transferred to Andorra, Argentina, Canada, the Faroe Islands, Guernsey, the Isle of Man, Israel, Jersey, New Zealand, Switzerland and Uruguay. Initially, A29WP identified some deficiencies in the level of personal data protection of Canada[35]. After Canada improved its data protection system, the Commission granted an adequacy finding with a decision.[36]

As a special sectoral regime to accommodate commercial transfers of personal data, the EU and the US concluded the Safe Harbour agreement. In 2000, the Commission formally adopted an adequacy decision that incorporated this agreement.[37] In 2015, the CJEU invalidated this decision retroactively for the reason that the Commission did not fulfil the requirements for an adequacy finding under the DPD.[38] Recently, the EU and the US have been negotiating a new scheme for transatlantic personal data flow (the so-called 'Privacy Shield'). In order to confer a legal effect on the Privacy Shield, the Commission has to endorse it with an adequacy decision.[39]

If the Commission, however, finds that the level of protection in a third country is inadequate, EU Member States shall take the measures necessary to prevent any transfer of the same kind of personal data to this third country (Article 25(4) DPD). So far the Commission has never adopted a negative decision on the adequate level of protection in a third country.

By way of derogation, Article 26 DPD holds a list of conditions that permit the transfer of personal data to a third country which does not ensure an adequate level of

---

[34] *ibid* para 52.

[35] A29WP , 'Opinion 2/2001 on the adequacy of the Canadian Personal Information and Electronic Documents Act' (26 January 2001) WP 39 <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2001/wp39_en.pdf> accessed 8 April 2016.

[36] Commission Decision 2002/2/EC 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 [2001] OJ L 2/13.

[37] Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce [2000] OJ L 215/7.

[38] *Maximillian Schrems v Data Protection Commissioner* (n 18) paras 98, 104-106.

[39] Draft Commission Implementing Decision pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-US Privacy Shield <http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf> accessed 8 April 2016.

protection. First, the transfer of personal data is possible if the controller adduces adequate safeguards with respect to the protection of privacy and personal data. By order of relevance, such adequate safeguards are standard contractual clauses, ie pre-formulated contracts which are pre-approved by the Commission (Article 26(4) DPD) and *ad hoc* measures, in particular appropriate contractual clauses (Article 26(2) DPD).[40] Alternatively, the supervisory authorities of EU Member States can authorise a transfer or a set of transfers of personal data subject to adequate safeguards (Article 26(2) DPD). This is the legal basis for binding corporate rules (BCRs), which can be used for international transfers of personal data within a multinational company with establishments in third countries.[41]

Second, personal data can be transferred to a third country under one of the conditions set out in Article 26(1) DPD. In the context of cross-border commerce, the relevant grounds could be the unambiguous consent of the data subject[42] or the performance or conclusion of a contract with or in the interest of the data subject.

The forthcoming GDPR will preserve the dichotomy between countries with and without an adequate level of protection (Article 41 GDPR). A new element will be that the GDPR now explicitly provides for the sectoral assessment of an adequate level of protection (Article 41(3) of the GDPR), for example in the field of commerce as is already done with the Privacy Shield. The GDPR will also codify BCRs as a means for the transfer of personal data (Article 43 GDPR). Finally, it will provide for a much more detailed, but non-exhaustive, list of criteria that should be taken into account by the Commission in its assessment of the adequacy of personal data protection in a third country (Article 41(2) GDPR).

# III. The GATS in the WTO Legal Order

## 1. General Characteristics of the GATS

The GATS is the first multilateral treaty on the liberalisation of international trade in services. It forms part of the 1994 Marrakesh Agreement on Establishing the World Trade Organization (WTO Agreement) as Annex 1B. The primary aim of the GATS is the expansion of international trade in services through the elimination of trade

[40] Working Party on the Protection of Individuals with regard to the Processing of Personal Data, 'Working Document: Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive'(24 July 1998), 3 <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/1998/wp12_en.pdf> accessed 8 April 2016.

[41] BCRs are modelled after corporate codes of conduct. BCRs are approved by EU member states' supervisory authorities. Requirements for the content of BCRs and the approval process are elaborated by A29WP. Guidance on the approval process can be found in A29WP , 'Working Document Establishing a Model Checklist Application for Approval of Binding Corporate Rules' (14 April 2005) WP108 <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2005/wp108_en.pdf> accessed 8 April 2016.

[42] With respect to consent as a ground for cross-border transfer, the 29WP warned that the consent of the data subject 'is unlikely to provide an adequate long-term framework for data controllers in cases of repeated or even structural transfers for the processing in question' (A29WP , 'Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995' (25 November 2005) WP 114, 11).

barriers. The preamble to the GATS also acknowledges the right of the WTO member states to regulate in order to pursue their national policy objectives.[43]

The GATS applies to 'any service in any sector' (GATS I:3 b) with the exception of services supplied in the exercise of governmental authority and services directly related to the exercise of air traffic rights.[44] The GATS covers 'trade in services' in four modes of supply: cross-border supply (mode 1), consumption abroad (mode 2), commercial presence (mode 3) and presence of natural persons (mode 4).[45] Obligations under the GATS are normally categorised in general obligations and specific commitments.

**a. General Obligations: the Most-Favoured-Nation Treatment**

The core general obligation under the GATS is Most-Favoured-Nation (MFN) treatment (GATS Article II). The MFN is automatically and unconditionally binding on each WTO member state from the moment of its accession to the GATS.[46]

Under GATS Article II, each WTO member state shall treat services and service suppliers of a WTO member in a manner 'no less favourable' than 'like' services and service suppliers of any other country. Thus, the principle goal of the MFN is elimination of discrimination between the first and the second. Importantly, the MFN is understood to ban both formal (*de jure*) and informal (*de facto*) discrimination.[47]

Interpretation of 'like' and 'no less favourable' is fully judge-made based on the jurisprudence of WTO adjudicating bodies. To ensure consistency of interpretation of the terms within the GATS the WTO bodies apply the same tests for 'likeness' and 'no less favourable' criteria in the context of the GATS national treatment and most-favoured-nation treatment disciplines.

Services are 'like' if they are 'essentially or generally the same in competitive terms'.[48] If differential treatment of services and service suppliers is solely based on their origin *per se*, they are presumed to be 'like' by reason of origin (the so-called 'presumption approach'), unless it is shown that such difference in treatment is based on other characteristics "relevant for an assessment of the competitive relationship of the services and service suppliers".[49] If one of these characteristics, such as "consumers' tastes and habits or consumers' perceptions and behavior in respect of

[43] Recital 3 of Preamble to the GATS.
[44] art I:3 of the GATS, Annex to the GATS on Air Transport Services, para 2.
[45] GATS art I:2.
[46] Under GATS art II:2 a WTO member may grandfather discriminatory measures prohibited under the MFN that existed as of the date of accession to the WTO provided that they are included in the special Annex on Article II Exemptions. As the DPD was adopted after the EU acceded to the WTO, the EU did not include any exceptions relating to the EU data personal protection framework.
[47] Matsushita et al (n 7) 570 – 571.
[48] WTO, *China – Electronic Payment Services – Report of the Panel* (16 July 2012) WT/DS413/R, paras 7.701-7.702.
[49] WTO, *Argentina – Financial Services - Report of the Panel* (30 September 2015) WT/DS453/R, para. 7.166, WTO, *Argentina – Financial Services - Report of the Appellate Body* (14 April 2016) WT/DS453/AB/R, paras. 6.30, 6.38-6.45.

the products" is reflected in the competitive relationship between services and service suppliers, services and service suppliers are not deemed to be "like."[50]

**b. Specific Commitments: Market Access and National Treatment**

The most important specific commitments are market access and national treatment (GATS Articles XVI and XVII). Specific commitments become binding only if and to the extent that the member country has indicated in its Schedules of Specific Commitments (Services Schedules). These schedules constitute an integral part of the GATS (GATS Article XX:3) and of the WTO accession package of a member.

In its Services Schedules each country specifies in which sectors, in relation to which modes of supply and to what extent it shall be bound by market access and national treatment obligations. The country can select to be fully bound, to be bound with limitations, or not to be bound by one or both specific commitments in each particular sector and in relation to each of the modes of supply.[51]

A full commitment of market access means a prohibition to maintain, predominantly qualitative,[52] market access barriers included in the exhaustive list of Article XVI:2.[53] In principle, a state that has made a full commitment of market access could nevertheless apply any other limitations.[54] However, in practice, measures, not quantitative on their face, and falling under neither of the prohibited categories of limitations, may still be banned. For example, in *US – Gambling*, the WTO adjudicating bodies qualified total prohibition on the remote supply of gambling and betting services as GATS inconsistent market access limitations. Although *per se* not quantitative restriction, the prohibition amounted to a 'zero quota' on the number of service suppliers and total number of service operations (Article XVI:2 (a) and (c)).[55]

National treatment (GATS Article XVII) requires that 'like' foreign services and service suppliers receive a 'treatment no less favourable' than their domestic counterparts of the WTO member state. Under GATS Article XVII(2) and (3) 'no less favourable' treatment requires *de jure* ('formally identical') or *de facto* ('formally different') treatment that 'does not modify the conditions of competition' in favour of domestic services and service suppliers compared to 'like' services and service

[50] WTO, *Argentina – Financial Services - Report of the Panel*, supra, note 49, para. 7.179; WTO, *Argentina – Financial Services - Report of the Appellate Body*, supra note 49, paras. 6.30, 6.38-6.45.
[51] Guidelines for the Scheduling of Specific Commitments under the General Agreement on Trade in Services (GATS), adopted by the Council for Trade in Services on 23 March 2001, S/L/92, para 39 (2001 GATS Scheduling Guidelines).
[52] Matsushita et al (n 7) 539-540, limitations outlawed by subparas (a) to (d) and (f)) are quantitative; limitation banned by sub-para (e) is a limitation on the kind of legal entity or joint venture through which services may be provided.
[53] If a party wants to preserve certain market access barriers banned by art XVI:2 in sectors and in relation to modes of supply where it undertook a specific market access commitment, such limitations should be included in the Services Schedule in the column 'Limitations on Market Access'.
[54] Matsushita et al (n 7) 539-540.
[55] WTO, *US – Gambling - Report of the Appellate Body* (7 April 2005) WT/DS285/AB/R, paras 238, 251, 252.

suppliers of a WTO member.[56] When analysing whether a measure accords a less favourable treatment the WTO adjudicating bodies do not take 'aims and effects' of such measure into account.[57]

### c. Domestic Regulation

The GATS allows WTO member states to pursue their national policy objectives by adopting regulation affecting trade in services as long as it complies with the requirements of GATS Article VI.[58]

Under Article VI:1 measures of general application affecting trade in services shall be administered in a reasonable, objective and impartial manner. It is therefore not the legislation itself but its application where a GATS violation could potentially occur. Article VI:2 requires procedural guarantees for review of administrative decisions affecting trade in services. Article VI:3 sets forth requirements to authorisation procedures. Articles VI:4 and VI:5 address qualification requirements and procedures, technical standards and licensing requirements. Article VI:6 concerns procedural guarantees for competence verification of professional services providers. Rules envisaged in paragraphs 1, 3, 5 and 6 of Article VI only apply in the services sectors for which the WTO member undertook specific commitments.

### d. Article XIV General Exceptions

If in a dispute under WTO law a member is *prima facie* found in violation of an obligation under the GATS, such a violation can be rectified by invoking one of the general exceptions under GATS Article XIV. This article offers as an affirmative defence in acknowledgment of the right of WTO members to pursue public policy objectives by adopting and enforcing measures inconsistent with any obligation under the GATS. In order to successfully invoke the general exceptions, however, the contested measure has to meet the material requirements of Article XIV (a) to (e) and the *chapeau* of Article XIV. WTO adjudicating bodies interpret general exceptions on a case-by-case basis without developing clear rules of its application.[59]

The material requirements vary depending on the policy objectives underlying the defended measure. This article discusses the test laid down by paragraph (c)(ii) of this Article, as the most relevant, which allows adoption and enforcement of a GATS-inconsistent measure that is

> necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Agreement including those relating to … the protection of

[56] Such interpretation is followed by WTO adjudicating bodies. See eg, *China – Electronic Payment System – Report of the Panel* (n 48) para 7.687; WTO, *Argentina – Financial Services - Report of the Appellate Body* (n 49) para 6.129.
[57] WTO, *Argentina – Financial Services - Report of the Appellate Body* (n 49) para 6.106; WTO, *EC – Bananas III* – Report of the Appellate Body (9 September 1997) WT/DS27/AB/R, para 241.
[58] Pauwelyn (n 7) 132.
[59] Since GATS art XIV has been invoked only twice, in its interpretation the WTO adjudicating bodies heavily rely on the more extensive case law under GATT 1994 art XX, which, essentially, envisages the same set of requirements.

the privacy of individuals in relation to the processing and dissemination of personal data…

The core of the general exceptions is the so-called 'necessity test' that requires 'weighing and balancing' between the following factors.[60] First, the contribution of the measure towards the enforcement of domestic laws and regulations that pursue a public policy interest (not to be confused with the contribution of the measure to the protected interest itself). Thus, should a dispute arise, it is not privacy and data protection that will be balanced against trade, but the effectiveness of a measure intending to secure compliance with these laws and regulations pursuing these or other public policy objectives, the list of which is merely illustrative.[61] Additionally, the restrictive effect of the measure on international trade is weighted in. The less restrictive the measure, and the greater the contribution, the more likely it is that the measure will meet the 'necessity test'.[62]

The *prima facie* case of the necessity of the measure can be rebutted by showing that there are 'reasonably available' alternative less trade-restrictive measures that without prohibitive cost or substantial technical difficulties would allow the defending party to achieve the same desired level of protection of the public interest pursued.[63]

A measure provisionally justified under Article XIV(c)(ii) material requirements should, in addition, meet the test of the Article XIV *chapeau*: it should be applied in a manner that does not constitute 'a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on trade in services.' WTO adjudicating bodies apply the *chapeau* as an open norm[64] in the light of its primary role to prevent abuse or misuse of the right to invoke the exception.[65] The benchmark often used to assess compliance with the *chapeau* is the consistency of the enforcement of the contested measure.[66]

## 2. WTO Jurisdiction and the Dispute Settlement System

[60] WTO, *US – Gambling - Report of the Appellate Body* (n 55) para 306; WTO, *Argentina – Financial Services - Report of the Panel* (n 49) para 7.684.
[61] WTO, *Argentina – Financial Services - Report of the Panel* (n 49) para 7.853; WTO, *US – Gambling - Report of the Appellate Body* (n 55) para 306; WTO, *US – Gambling - Report of the Panel* (10 November 2004) WT/DS285/R, para 6.540.
[62] WTO, *Argentina – Financial Services - Report of the Panel* (n 49) paras 7.685, 7.727, referring to WTO, *Korea – Various Measures on Beef – Report of the Appellate Body* (11 December 2000) WT/DS161/AB/R and WT/DS169/AB/R, para 163.
[63] WTO, *Argentina – Financial Services - Report of the Panel* (n 49) para 7.729 referring to WTO, *US – Gambling - Report of the Appellate Body* (n 55) para 308.
[64] The unwillingness of the WTO adjudicating bodies to develop general rules on the basis of the chapeau was criticized by scholars as this creates uncertainty in the future interpretation of the exceptions. See Reyes (n 10) 27.
[65] WTO, *Argentina – Financial Services - Report of the Panel* (n 49) para 7.743 referring to WTO, *US – Gasoline- Report of the Appellate Body Report* (29 April 1996) WT/DS2/AB/R, 22.
[66] Matsushita et al (n 7) 620, WTO, *US – Gambling - Report of the Appellate Body* (n55) para 351.

WTO law is *lex specialis* in the system of public international law[67] that has its own enforcement mechanism and remedies for breach.[68] The WTO panels and Appellate Body (WTO adjudicating bodies) treat WTO jurisdiction as autonomous and are generally reluctant to apply non-WTO law in dispute settlement proceedings.[69]

The GATS is enforced exclusively through the WTO government-to-government enforcement mechanism – the Dispute Settlement System (DSS).[70] The DSS is a two level system, in which *ad hoc* WTO panels hear complaints in the first instance, and the Appellate Body, a permanent international tribunal, hears appeals to the panels' decisions (Articles 6, 17.1 Dispute Settlement Understanding, DSU[71]). The Dispute Settlement Body (DSB)[72] has to adopt the conclusions – rulings or recommendations – of the WTO adjudicating bodies which then become legally binding under Articles 17.14, 21.1 DSU.

Adopted conclusions do not create binding precedents for future cases, even if the same questions of WTO law arise.[73] Nevertheless, WTO adjudicating bodies are likely to follow the reasoning developed in previous cases, if they find it persuasive, to ensure the security and predictability of international trade law, and to protect the 'legitimate expectations of the WTO Members'.[74]

The only remedy available under WTO law against the party found in violation of the GATS is withdrawing of the WTO-inconsistent measure or bringing it in compliance with the GATS (Articles 3.7, 19.1 DSU). As an ultimate measure to induce compliance with the report, adopted by the DSB, the complaining party may selectively suspend its concession or other obligation under the GATS (the retaliation measures) in relation to the non-implementing party (Article 22.1 DSU). Such countermeasures are subject to the prior approval of the DSB.

## 3. EU Commitments under the GATS

Both the EU and its Member States are original parties to the GATS and the WTO alike. Under international law, the GATS is legally binding on the EU and its Member

[67] Matsushita et al (n 7) 79-80.
[68] Arguably, customary public international law rules on state responsibilities codified in International Law Commission (ILC) Articles on Responsibility of States for Internationally Wrongful Acts are inapplicable to WTO law. See van den Bossche and Zdouc (n 7) 204.
[69] Matsushita et al (n 7) 79-80.
[70] van den Bossche and Zdouc (n 7) 161.
[71] Annex 2 to the WTO Agreement.
[72] Alter ego of the WTO General Council that consists of diplomats representing the WTO member states (van den Bossche and Zdouc (n 7) 206).
[73] Dispute settlement system training module: s 7.2 <www.wto.org/english/tratop_e/dispu_e/disp_settlement_cbt_e/c7s2p1_e.htm> accessed 8 April 2016; A Chua, 'Precedent and Principles of WTO Panel Jurisprudence' (1998) 16 Berkeley Journal of International Law 171.
[74] Dispute settlement system training module: s 7.2 (n 73), referring to WTO, Japan — Alcoholic Beverages – Report of the Appellate Body (4 October 1996) WT/DS8/AB/R, WT/DS10/AB/R and WT/DS11/AB/R, 107-108.

States.[75] Since the primary focus of this article is on the interaction between WTO law and EU law, only the commitments of the EU will be discussed.

In order to comply with its obligations, the EU must ensure the conformity of its laws, regulations and administrative procedures with the GATS. Should any of those be found inconsistent with the GATS, the EU must abrogate or modify them. Non-conformity with domestic law or the absence of a direct effect in domestic law cannot justify the failure to perform international obligations under the GATS.[76] The EU is, however, free to determine the means and methods of complying with its obligations in its legal order.

The EU is bound by all general obligations under the GATS. It also undertook specific commitments in modes of supply 1, 2 and 3 with respect to the following services that broadly cover the processing of personal data: data processing services, database services and other computer services (in the sector of computer and related business services),[77] telecommunications,[78] travel agencies and tour operators,[79] computer reservations systems[80] and financial services (primarily, insurance and banking).[81]

For each of these services the EU has entered a number of limitations, most of which, however, do not concern the processing of personal data. In mode of supply 4, the EU chose to be unbound, except for a limited number of cases which are irrelevant in the context of this article.

The only exception from the commitment to provide market access that does explicitly concern privacy and data protection is in the banking sector. The EU specifically excluded[82] from its commitments to market access of banking services supplied through mode 1 and 2 the obligation not to

> take measures that prevent transfers of information or the processing of financial information, including transfers of data by electronic means, … where such transfers of

[75] art II:2 of the WTO Agreement, art 26 of the Vienna Convention on the Law of Treaties No. 18232 of 23 May 1969 (VCLT).
[76] art 27 of the VCLT
[77] EU Schedule of Specific Commitments WTO doc GATS/SC/31 of 15 April 1994, s 1.II. B c), d) and e)).
[78] EU Schedule of Specific Commitments Supplement 3 WTO doc GATS/SC/31/Suppl. 3 of 11 April 1997, s 2.C.
[79] EU Schedule of Specific Commitments (n 77) s9.B.
[80] ibid s 11.C.d.
[81] EU Schedule of Specific Commitments Supplement 4 Revision GATS/SC/31/Suppl.4/Rev.1. The Understanding is not a part of the GATS, but is an appendix to the Final Act of the Uruguay Round; Understanding on Commitments in Financial Services. The Understanding is not legally binding per se, it is 'an optional and alternative approach to making specific commitments on financial services' (see official website of the WTO <www.wto.org/english/tratop_e/serv_e/finance_e/finance_e.htm> accessed 8 April 2016).
[82] EU Schedule of Specific Commitments Supplement 4 Revision GATS/SC/31/Suppl.4/Rev.1, para 3 of the Introductory note.

information, processing of financial information … are necessary for the conduct of the ordinary business of a financial service supplier.[83]

The fact that this provision also reserves the right of the members to protect privacy and personal data indicates that the 'financial information' and 'data' mentioned therein include 'personal data.'

## IV. The GATS in the EU Legal Order

Under EU law, the GATS, as an international agreement to which the EU is a party, forms an 'integral part' of the EU legal system.[84] In the hierarchy of EU law, the GATS is situated in between EU primary law, such as the Charter and the founding Treaties, and EU secondary law, such as EU regulations, directives and decisions.[85] This approach is based on the principle of the autonomy of the EU legal order vis-à-vis international law, which should respect the constitutional values and internal division of competences in the EU.[86]

The EU legal order tends not to afford multilateral trade agreements direct effect on the grounds that they are not self-executing and do not directly confer rights on individuals and legal entities.[87] In relation to the GATS, this follows from the 'no direct effect' provisions included by the EU in the Council Decision approving the WTO Agreement and Annexes to it[88] and in the EU Services Schedule.[89]

The same conclusion follows from the settled CJEU jurisprudence on the absence of direct effect of another Annex to the WTO Agreement - the General Agreement on Tariffs and Trade (GATT 1994), as well as its predecessor (GATT 1947).[90] First, direct application of all WTO agreements is precluded by their 'nature

[83] para B.8 of the Understanding on Commitments in Financial Services.
[84] This has also been clarified by the CJEU. See eg Case 181-73 *R. & V Haegeman v Belgian State*, [1974] EU:C:1974:41, para 5, Opinion 2/13 of the Court (Full Court) [2014] ECLI:EU:C:2014:2454, para 180.
[85] This statement follows from the landmark 2008 *Kadi I* case of the CJEU (Case C-402/05 P and C-415/05 P *Yassin Abdullah Kadi and Al Barakaat International Foundation v Council of the European Union and Commission of the European Communities* [2008] ECLI:EU:C:20 08:461, paras 282, 307, 308, 316). Although, this decision is fact-specific, it is believed that this approach applies to the relationship between the EU and international law in general; see de Burca (n 4) 5.
[86] See S Gaspar-Szilagyi, 'The "Primacy" and "Direct Effect" of EU International Agreements' (2015) 21 European Public Law 343, 349.
[87] Paul Craig and Graine de Burca, *EU Law: Text, Cases, and Materials* (6th edn, OUP 2015), 362-363.
[88] Council Decision 94/800/EC of 22 December 1994 concerning the conclusion on behalf of the European Community, as regards matters within its competence, of the agreements reached in the Uruguay Round multilateral negotiations (1986-1994) [1994] OJ L336/1, recital 11 of the Preamble. Although, this Decision, unlike the Schedule of Specific Commitments does not constitute a part of the GATS, the CJEU deferred to it in *Portugal v Council* as an indication of political will of the EU in concluding the WTO Agreement (see Case C-149/96 *Portuguese Republic v Council of the European Union* [1999] ECLI:EU:C:1999:574, para 48), A Semertzi 'The Preclusion of Direct Effect in the Recently Concluded EU Free Trade Agreements' (2014) 51 CML Rev 1125, 1132-1135.
[89] EU Schedule of Specific Commitments under GATS, GATS/SC/31 of 15 April 1994, para 3 of the Introductory Note.
[90] Craig and de Burca (n 87) para 47.

and broad logic'[91], as they are founded on the 'principle of negotiations with a view to entering into reciprocal and mutually advantageous arrangements', which is, in particular, manifested in the flexibility of the dispute settlement mechanism.[92] Second, the provisions of the GATT are not 'unconditional and sufficiently precise so as to confer on persons subject to [EU] law the right to rely thereon in legal proceedings',[93] as contracting parties may unilaterally suspend obligations, withdraw or modify the concessions under the agreement.[94]

Given that the GATT and GATS are both Annexes to the WTO Agreement, share the same dispute settlement mechanism and contain essentially similar obligations, it is highly probable that the CJEU would conclude on the absence of direct effect of the GATS too. By the same token, decisions of the WTO adjudicating bodies on the GATS would also have no direct effect in EU law.[95]

The absence of direct effect of the GATS ensures that, first, although the GATS is situated above secondary law in EU law, private parties cannot directly invoke the GATS or decisions of WTO adjudicating bodies to invalidate provisions of EU secondary law. Neither can these instruments be invoked in disputes resolved by EU Member States' national courts. Second, private parties cannot directly enforce their rights under the GATS even if those are confirmed by a decision of a WTO adjudicating body in national courts. Furthermore, private parties also cannot sue EU institutions under Articles 268 and 340 TFEU for non-contractual damages caused to such parties, eg by retaliation measures resulting from the non-compliance of the EU with a decision of a WTO adjudicating body within a reasonable time.[96]

Nevertheless, absence of direct effect does not mean no effect at all, as the GATS is a part of the EU law *aquis*. Absence of direct effect only dictates that neither the GATS nor decisions of adjudicating bodies can automatically invalidate or override any provision of EU law. In other words, they are not self-executing in EU law but in order to comply with any of them the EU has to adopt legislative measures.

## V. Application of the GATS to EU Data Protection Law

In this section, the GATS is applied to EU data protection law and implementation measures. Through the application, it is possible to identify which aspects of EU law might be in conflict with the GATS obligations and commitments, and then turns towards their possible justification under general exceptions in GATS Article XIV(c).

---

[91] See Case C-366/10 *Air Transport Association of America and Others v Secretary of State for Energy and Climate Change* [2011] ECLI:EU:C:2011:864, para 74.

[92] *Portugal v Council* (n 87) para 42, internal quotation marks omitted; Case C-280/93 *Federal Republic of Germany v Council of the European Union* [1994] ECR I – 4979 (*Germany v Council*), para 106.

[93] See *Air Transport Association of America* (n 91) para 74.

[94] *Germany v Council* (n 91) paras 108, 110. This conclusion was made in respect of GATT 1947. However, the same is true for GATT 1994 as it essentially builds up on GATT 1947.

[95] Case C-120/06 P *FIAMM and Others v Council and Commission* [2008] ECLI:EU:C:2008:476 ("*FIAMM v Council*"), paras 125-128.

[96] *FIAMM v Council* (n 95) para 120; for analysis see Gaspar-Szilagyi (n 86) 368.

Since EU personal data protection law has never been challenged in the WTO, this hypothetical analysis is informed by WTO law, jurisprudence and literature. However, some legal insecurity persists, owing to the fact that WTO adjudicating bodies have a certain margin of interpretation that cannot be fully anticipated.

## 1. The DPD Falls under the Scope of the GATS

EU data protection law and implementation measures by the Commission and Member States' supervisory authorities qualify as measures affecting trade in services and, as such, fall under the scope of application of the GATS (Articles I:1, XXVIII(a)).[97] The EU undertook specific commitments with respect to services that may include the processing of personal data. The DPD and decisions based on it, such as the Commission's adequacy findings, regulate and thus have an 'effect' on services that include the processing of personal data.[98]

## 2. Compliance of EU Data Protection Law with the GATS

### a. Modes of Supply

The DPD, including its provisions on the transfer of personal data to third countries (Articles 25 and 26 DPD) and on implementation measures of the Commission and EU Member States' supervisory authorities, can affect international trade. These measures can simultaneously affect the supply of services by third country providers through modes of supply 1, 3 and 4, as they are not mutually exclusive.[99] Owing to their differences, subsequent GATS analysis treats the DPD and the rules on transfers of personal data to third countries separately.

### b. The DPD (Excluding Chapter IV on Cross-border Transfers) under the GATS

The provisions of the DPD, excluding Chapter IV on cross-border transfers, pose little, if any, risks of non-compliance with the GATS. These provisions of the DPD apply to domestic and foreign controllers and processors of personal data alike in a non-discriminatory manner and thus, on their face, do not violate national treatment and MFN.[100] They do not prohibit or limit the supply of services in a way that would conflict with market access commitments.

Under GATS rules on domestic regulation, the DPD can be considered a measure of general application[101] and falls as such under the requirements of GATS Article VI:1. The provisions of the DPD (excluding Chapter IV on cross-border

[97] See Reyes (n 10) 10.
[98] For interpretation of threshold requirement 'affecting trade in services' see eg Matsushita et al (n 7) 565-566.
[99] Kuner, 'Extraterritoriality and Regulation of International Data Transfers (n 6) 244.
[100] G Shaffer, 'Managing US – EU Trade Relations through Mutual Recognition and Safe Harbour Agreements: "New" and "Global" Approaches to Transatlantic Economic Governance' RSC No 2002/28 EUI Working Papers, 35.
[101] The DPD has a broad territorial scope, horizontally applies to almost all processing of personal data, and defines 'personal data'broadly. See Reyes (n 10) 18, Weber (n 9) 35.

transfers) do not violate GATS Article VI:1 as it tackles the application of the measures of general application. Insofar the DPD does not have direct effect and is implemented in the legal systems of the EU Member States. EU data protection law does not mount authorisation, qualification, or licensing requirements nor can it be considered a technical standard. Therefore, paragraphs 2, 3, 4, and 5 of GATS Article VI are not triggered.

### c. EU Rules on Transfer of Personal Data to Third Countries under the GATS

The compliance of EU rules on the transfer of personal data to third countries (Chapter IV of the DPD) with the GATS is controversially discussed. There are opinions in the literature suggesting EU measures could potentially violate the EU's commitments on MFN, market access and domestic regulation.[102] It is important to note that this criticism predominantly tackles the Commission's practice of issuing adequacy decisions for certain third countries.

#### *aa. Most-favoured-nation (MFN) Treatment*

EU rules on the transfer of personal data to third countries (Chapter IV DPD) are capable of violating the EU's MFN obligation under GATS Article II. EU law clearly gives preferential treatment to countries which meet the threshold of ensuring an adequate level of personal data protection. Vice versa, services and service suppliers from third countries not affording adequate protection are treated 'less favourably'.

In addition, implementation measures of the rules on the transfer of personal data to third countries are also exposed to counter MFN treatment obligation. They are prone to inconsistency, not fully impartial and do not always translate into achieving a high-level of personal data protection in practice (see section on domestic regulation below).[103] In a dispute settlement procedure, the Commission's practice is vulnerable to finding a violation of the MFN, as the WTO adjudicating bodies do not recognize the aim and purpose of the measure in its assessment of 'less favourable treatment'.[104]

Reyes argues that third countries who received a negative decision testifying to the inadequacy of their national data protection facilities would be discriminated against compared to other third countries which were never the subject of a Commission decision.[105] We tend to disagree because the legal regime for a third country with a negative decision by the Commission and countries whose data protection regime were never assessed is the same (see section 2.2 above). Moreover,

[102] Reyes (n 10) 14-16, Keller (n 9) 353.
[103] For details on the inconsistency of the EU – US Safe Harbour Agreement with the DPD see *Maximillian Schrems v Data Protection Commissioner* (n 18).
[104] Relying on WTO, *Argentina – Financial Services - Report of the Panel* (n 49).
[105] Reyes (n 10) 14-16.

since the inception of the DPD the Commission has never issued a single negative decision. Hence, this scenario is highly hypothetical.[106]

Yet, Reyes and Keller, both note a different treatment of countries, which do not succeed in negotiating a sectoral scheme for personal data flow with the Commission, and those which succeed. They both present as an example the now invalidated EU – US Safe Harbour regime. Keller adds that the arguably more lenient treatment for an adequacy finding in effect afforded the US more favourable treatment compared to other third countries.[107] Arguably, the same claim could be made with respect to the new Privacy Shield between the EU and US that is to replace the Safe Harbour and has triggered widespread criticism.[108]

This argument merits some attention, given that the GATS MFN bans both *de jure* and *de facto* discrimination. The Commission may approve sectoral schemes of personal data flow to a third country with adequacy decisions (Article 25(6) DPD),[109] as it has done in respect of the US Based on a formalistic reading, these decisions are legally binding in EU law and create a legal presumption of the adequacy of personal data protection in the third country. WTO adjudicating bodies, in their turn, only have competence to apply WTO law and would not be bound by any finding of adequacy of EU institutions. Henceforth, it is unclear if - in a hypothetical dispute settlement procedure - the WTO adjudicating bodies would be satisfied with a formalistic reading of EU law or override the legal presumption of adequacy under EU law with its own *de facto* assessment. In the latter case, the EU practice of authorising the transfer of personal data in the commercial sector with the US would be vulnerable to legal challenges under GATS MFN.

Differential treatment between third countries would require justification pursuant to GATS Article XIV as will be elaborated below.

### *bb. National Treatment*

Scholars usually do not raise the issue of non-compliance of EU rules on the transfer of personal data to third countries with the GATS national treatment obligation, as on their face these rules apply to both domestic and foreign controllers without discrimination. However, when personal data is collected directly from a data subject based in EU/EEA by a service provider established and operating from outside the

[106] The argument made by Reyes that Australia was granted an inadequacy finding is not valid. Australia has received a refusal to grant a general adequacy finding from A29WP (see Article 29 Working Party, Opinion 3/2001 on the Level of Protection of the Australian Privacy Amendment (Private Sector) Act 2000 (Report WP 40, European Commission, 26 January 2001) 6). This Opinion is not legally binding (art 29(1) DPD) and, moreover, does not give a final conclusion on the inadequacy of data protection in Australia.

[107] Keller (n 9) 353.

[108] See eg C Kuner, 'Reality and Illusion in EU Data Transfer Regulation Post Schrems' (2016) University of Cambridge Faculty of Law Research Paper 14/2016 <http://ssrn.com/abstract=2732346> accessed 8 April 2016.

[109] eg the EU – US Safe Harbour regime was approved by an adequacy decision (see n 35). The EU – US Privacy Shield, if approved, will also be issued as an adequacy decision (see n 37).

EU/EEA area, a less favourable treatment of such provider as compared to domestic ones could still be contended. In this case, in order to obtain personal data, the provider from a third country has to comply with the rules on transfer of personal data to third countries.

The different treatment would only amount to a GATS violation if it discriminates between 'like' services and service suppliers. It could be contended that a high level of data protection influences the 'likeness' analysis. Arguably, if a high level of protection affects the characteristics of services and is valued by consumers, this could be considered as a characteristic relevant for an assessment of the competitive relationship of the services and service suppliers, which differentiates otherwise similar services and service suppliers.

For example, in business-to-business computer services, data localisation in Europe has evolved into a recurrent requirement of enterprise customers, which significantly alters the competitive relationship between services and service suppliers.[110] Thus, even though services involving data transfers to countries with an adequate level of protection do receive a more favourable treatment, this would not qualify as violation of national treatment because the services are not 'like'.

By contrast, individual consumers, while clearly valuing privacy and data protection,[111] often act irrational with the result that their preference does not manifest in their choices (the so-called 'privacy paradox').[112] For the time being, a high level of data protection cannot (yet) be held to have distinctively entered in the competitive relationship between consumer facing services and service suppliers. Accordingly, it can be concluded that here may be a risk of violation of the national treatment by EU rules on transfer of personal data to third countries, insofar as the EU will not be able to prove that the difference in treatment of third country services and service providers as compared to EU services and service providers is based on the characteristic relevant for an assessment of the competitive relationship of the services and service suppliers.

A differential treatment between EU/ EEA Member States and a third country would be submitted to GATS Article V, which provides for a justification based on 'Economic Integration', next to the general exceptions in GATS Article XIV.

***cc. Market Access***

[110] K Irion, 'Cloud services made in Europe after Snowden and Schrems' (23 October 2015) Internet Policy Review http://policyreview.info/articles/news/cloud-services-made-europe-after-snowden-and-schrems/377 accessed 8 April 2016.

[111] Commission, Data Protection, Special Eurobarometer 431 (June 2015) <http://ec.europa.eu/public_opinion/archives/ebs/ebs_431_en.pdf> accessed 10 May 2016. See also F Costa-Cabral and O Lynskey 'The Internal and External Constraints of Data Protection on Competition Law in the EU' (2015) LSE Law, Society and Economy Working Papers 25/2015, 17, 25-26 <http://eprints.lse.ac.uk/64887/1/Lynskey_Internal%20and%20External%20Constraints%20of%20Data%20Protection%20_Author_2015.pdf> accessed 8 April 2016 .

[112] K Irion and G Luchetta, *Online Personal Data Processing and the EU Data Protection Reform* (Centre for European Policy Studies 2013), 35-36.

In principle, limitations on the transfer of personal data to third countries can constitute a market access restriction. For example, in the banking sector the requirement to refrain from taking measures preventing the transfer of data (in general) by electronic means constitutes a market access obligation.[113] At the same time, this provision explicitly states that it does not restrict the right of a member to protect personal data, personal privacy and the confidentiality of individual records and accounts so long as such right is not used to circumvent the provisions of the GATS.

EU rules on the transfer of personal data to third countries, on their face, do not appear to fall under any of the banned market access limitations under GATS Article XVI:2. In the literature it is argued that the default prohibition on the transfer of personal data to third countries with inadequate protection effectively constitutes a 'zero quota' violating GATS Article XVI:2(a) and (c).114 In our assessment, this argument disregards the derogations in Article 26 DPD, which provide for a number of legal conditions to transfer personal data lawfully to third countries which do not afford an adequate level of personal data protection. In the light of these derogations, a finding of GATS inconsistent 'zero quota' market access barriers can hardly be made.

***dd. Domestic Regulation***

As a part of the DPD, the provisions of Chapter IV on the transfer of personal data to third countries qualify as measures of general application affecting trade in services. Hence, they are subject to the requirements of GATS Article VI:1 on domestic regulation in the sectors for which the EU entered into specific commitments, and should be administered in a reasonable, objective and impartial manner.

The way in which the Commission implemented these provisions may create a risk of violating the reasonableness requirement, because they are more restrictive than necessary to achieve the public policy goal pursued by them. Not because they set forth a prohibition of transfer of personal data to third countries with inadequate protection, as mistakenly argued by Reyes.[115] Rather, because in combination with the provisions on the geographical scope of application of EU data protection law, they create 'two sets of overlapping requirements with the same purpose that are not coordinated with each other'.[116]

As an illustration, online collection of personal data from an EU/EEA data subject by a controller located in a third country with inadequate protection and without an establishment in the EU/EEA may simultaneously trigger the application of EU data protection law and its rules on cross-border transfer of personal data.

[113] s B.8 of the Understanding on Commitments in Financial Services.
[114] By analogy with WTO, *US – Gambling - Report of the Appellate Body* (n 55); Reyes (n 10) 22; Weber (n 9) 33-34.
[115] Reyes, supra, note 10, p. 20.
[116] Kuner, 'Extraterritoriality and Regulation of International Data Transfers (n 6) 244.

There is a lack of coordination, as was noted by Kuner, as regards to the legal transfer mechanisms. However, it would be still reasonable to attach specific safeguards to transfers of personal data to a third country in order to prevent the circumvention of EU law.

Furthermore, not all of the Commission's adequacy decisions, such as the one on Canada,[117] require that the third country itself restricts the onward transfer of personal data to countries with inadequate protection.[118] This clearly undermines the very purpose of the EU-style limitations and may cause WTO adjudicating bodies to question the measure's reasonableness. Soon the GDPR will incorporate the rules for onward transfer of personal data to another third country or international organisation in the list of factors for the assessment of adequacy (Article 41(1)(a)).

In addition, the present practice exhibits procedural and substantive shortcomings. In particular, the Commission's country-by-country adequacy assessments may fall short of the impartiality and objectivity of the administration of the rules in question. There are no formal criteria on when and how third countries' personal data protection regimes are to be assessed for their adequacy.[119] In substance, the Commission's adequacy decisions do not seem precisely a legal-only assessment or even-handed. According to Kuner, adequacy decisions 'are far from always being objective and logical, and do not provide a watertight standard of data protection'.[120] Scholars and pundits have expressed concerns that political or economic factors inherent in international relations with the EU are also taken into account.[121]

Some literature claims that the rules on the transfer of personal data to third countries violate GATS Articles VI:3 and VI:4(b).[122] This is doubtful because the provision of Article VI:3 concerns authorisation requirements, of which the relevant rules, when considered as a whole, are not an example. Neither can they be qualified as qualification requirements and procedures, technical standards and licensing requirements, which are regulated by GATS Article VI:4. The system of derogations in Article 26 DPD is flexible enough to accommodate different needs for lawful transfers of personal data to third countries without an adequate level of data protection.

---

[117] Kuner shows that Canadian data protection law does not prohibit onward transfers of personal data, but holds the exporter of personal data accountable for its processing in another jurisdiction (see C Kuner, 'Regulation of Transborder Data Flows (n 6) 21).

[118] Kuner, 'Developing an Adequate Legal Framework' (n 6) 267.

[119] Reyes (n 10) 20.

[120] Kuner, 'Developing an Adequate Legal Framework' (n 6) 271.

[121] With respect to the example adequacy decision on New Zealand, Bygrave demonstrates that the amount of trade between the EU and a foreign country also plays a role in adequacy assessments (Bygrave (n 6) 194 referring to A29WP Opinion 11/2011 on the level of protection of personal data in New Zealand (4 April 2011, WP 182)). Kuner argues the European Commission decision on the adequacy of data protection in Argentina was influenced by political factors (Kuner, 'Developing an Adequate Legal Framework' (n 6) 265).

[122] Reyes (n 10) 20; Weber (n 9) 37.

The analysis above has identified three potential violations of GATS obligations by EU measures in relation to the rules on the transfer of personal data to third countries in Chapter IV of the DPD. In a hypothetical dispute under WTO law, a member who did not succeed in obtaining an adequacy decision by the Commission could make a claim against the EU for possible violations of GATS MFN, national treatment and GATS Article VI:1 on domestic regulation.

### *ff. Applying the General Exceptions of GATS Article XIV*

In the next step it will be assessed whether these *prima facie* violations could be justified under the general exception of GATS Article XIV(c)(ii). This paragraph is specifically about justifying a non-compliant measure that claims to be necessary to secure compliance with – here – EU data protection law, which in itself is not inconsistent with the GATS. As explained earlier, reliance on the general exceptions of GATS Article XIV has to meet a series of legal requirements and their interpretations, such as the 'necessity test' and the *chapeau* of GATS Article XIV.

Among scholars and pundits there is a concern that reliance on GATS Article XIV may not succeed owing to the overall experience with WTO jurisprudence and the low success rate so far.[123] In general, the literature notes a significant degree of legal uncertainty and unpredictability whenever WTO adjudicating bodies apply GATS Article XIV. For the purpose of this article, the general critique of WTO law matters, yet concerns about how the Commission applies the rules on the transfer of personal data to third countries weight heavily too.

It is true that the provisions on the transfer of personal data to third countries are designed to secure compliance with EU data protection standards set forth in the DPD[124] that, in themselves, are not inconsistent with the GATS.[125] The questions are whether these limitations on data transfers are 'necessary' to secure compliance with the above-mentioned provisions of the DPD, and whether the application of these limitations is consistent enough not to constitute 'a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on trade in services' in violation of the GATS Article XIV *chapeau*.

In terms of the 'necessity test', the contribution of the limitations on transfer of personal data to ensuring compliance with EU data protection law is sufficiently undermined by the way in which they are currently implemented. As shown above, adequacy decisions of the Commission are not purely based on legal considerations,

[123] Reyes (n 10) 2. Looking at the practice of the application of GATS art XIV and the analogous art XX of GATT 1994, Citizen.org argues that these general exceptions are not effective because, as of August 2015, they have succeeded only in one out of 44 cases. 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' (August 2015) <www.citizen.org/documents/general-exception.pdf> accessed 8 April 2016.

[124] Kuner, 'Regulation of Transborder Data Flows' (n 6) 27-28; Bygrave (n 6) 191.

[125] The GATS-inconsistency of one provision does not render other provisions of the same law or regulation GATS-inconsistent (WTO, *Argentina – Financial Services - Report of the Panel* (n 49) paras 7.622, 7.625).

but are to a considerable extent distorted by political and economic factors. Adequacy assessments are not governed by procedural rules which would guarantee that they are administered in a reasonable, objective and impartial manner. The onward transfers of personal data from third countries affording an adequate level of personal data protection is not always limited. Enforcement of limitations on the transfer of personal data is piecemeal as more than one third of the EU Member States' supervisory authorities are not able to carry out their tasks, some of them being underfinanced and understaffed.[126]

EU rules on transfers of personal data to third countries, however, do not create an absolute ban on trade and are thus not immensely trade-restrictive. Both, adequacy assessments and compliance with the derogations under Article 26 DPD, are, nevertheless, costly and time consuming.[127] Therefore, some negative effect of these rules on international trade in services cannot be denied. Given the importance of the purpose to avoid circumvention of EU data protection standards, weighing and balancing of their relatively low contribution towards ensuring compliance with these standards, on the one hand, against a similarly low negative effect on trade, on the other hand, is a close case.

The 'necessity' of these rules could be successfully challenged if the complaining party invokes that there are less restrictive alternatives, such as the principle of accountability, adopted in Canada and many Asia-Pacific Economic Community countries.[128] The latter could be deemed 'reasonably available' because, arguably, it preserves the right of the EU to ensure the same level of protection of personal data transferred to a third country and to prevent circumvention.[129] To Kuner, the accountability principle attains this result and is more effective in practice as it does not impose limitations on the cross-border transfer of personal data. Instead, it renders the data exporter responsible for all processing of personal data abroad.[130] As a result, the rights of EU/EEA data subjects can be more successfully enforced in their own country and the problem of the enforcement of these rights against foreign controllers and processors outside the EU/EEA, inherent in the current adequacy framework, would not arise.[131]

Even if the provisions on the transfer of personal data to third countries were to be deemed necessary, there is still an argument that the inconsistent implementation of these provisions by the Commission[132] will not withstand the test of the *chapeau* of GATS Article XIV. For example, should a violation of the GATS occur in a situation where the EU has denied a third country's application for adequacy assessment or a

[126] Kuner, 'Regulation of Transborder Data Flows' (n 6) 29.
[127] Reyes (n 10) 32.
[128] Kuner, 'Developing an Adequate Legal Framework' (n 6) 269-271.
[129] ibid.
[130] ibid.
[131] ibid.
[132] Reyes (n 10) 25, 34. The same argument is expressed by Bygrave (n 6) 199.

request to negotiate a sectoral scheme similar to that of the US-EU Privacy Shield, the *chapeau* can hardly be satisfied.

## 3. Consequences and Practical Implications

In the hypothetical event that a WTO adjudicating body finds that the implementation and administration of EU rules on personal data transfers to third countries violates the GATS, and such violation cannot be justified under the GATS Article XIV(c)(ii) exception, the consequences for the EU appear to be more trivial than one might expect.

Since inconsistency with the GATS is caused by the implementation and administration of EU rules, there is no risk that the EU would have to repeal or modify the underlying legislation (ie the DPD) in order to comply with the GATS. Articles 7 and 8 of the Charter, which in any case supersede the GATS, and the provisions of the DPD are not *per se* inconsistent with the GATS.

Owing to the absence of a direct effect of the GATS and decisions of WTO adjudicating bodies in EU law, measures implementing or administrating EU data protection law that are found GATS-inconsistent would not be automatically invalid or inapplicable. In order to rectify a violation of the GATS, or to satisfy the necessity test and the chapeau of Article XIV(c)(ii), the Commission would have to modify its practice of conducting adequacy assessments of third countries' level of protection.

An unreasonable delay in implementing a WTO adjudicating body's decision on the part of the EU does not promise severe practical repercussions either. The main aim of the WTO DSS is the elimination of WTO-inconsistent and trade-restrictive measures, and not punishment of the breaching member state. At the discretion of the complaining party, retaliation could amount to substantial countermeasures.[133] However the EU is one of the largest economies in the world. The ratchet effect of such retaliation on a smaller economy may turn out to be more detrimental than it is to tolerate discriminatory administration of EU provisions on data transfer.[134]

Without a claimant, obviously there would not be a case (*Nullo actore, nullus iudex*). The likelihood that a WTO member would initiate DSS proceedings against the EU in the first place is not immediately apparent. The decision to start time-consuming and costly proceedings at the WTO is a political one, and is not solely based on the strength of legal arguments. In practice, it may be more sensible for a WTO member to make an extra effort to negotiate an agreement with the EU, especially once the GDPR takes effect under which sectoral arrangements are explicitly allowed.

[134] van den Bossche and Zdouc (n 7) 203.

## VI. Conclusion

So can the EU have the best of both worlds: enjoy the benefits of free trade in services under the GATS, on one hand, and maintain its data protection legislation, including the limitations on transfers of personal data to third countries presently in the DPD, on the other? This question can neither be answered in the affirmative, nor can it be refuted.

Analysis in this article suggests approaching this issue in three steps. First, whether EU data protection rules *per se* can constitute a violation of the GATS. Second, whether their implementation can be captured by the relevant GATS disciplines. And third, whether once a violation of the GATS is found, it can be justified under Article XIV general exceptions.

On the level of EU data protection rules *per se* the conclusion turns on whether the high level of personal data protection guaranteed under EU law and by third countries with adequate level of protection is proven to affect the consumer characteristics of the relevant services and service suppliers. If this is the case, then there is virtually no risk of EU data protection rules being found in violation of the GATS. If the EU does not succeed in convincing the WTO bodies that consumer characteristics of the relevant services and services suppliers render them not "like" services and service suppliers from a third country, the EU law provisions on transfer of personal data to third countries can trigger both national treatment (Article XVII) and the MFN (Article II) disciples of the GATS.

On the level of application of EU data protection rules, the implementation of the rules on third countries, here mainly the Commission's adequacy assessments, creates a higher risk of violating the GATS MFN discipline and requirements to domestic regulation (Article VI:1). As it concerns the inconsistent application of EU data protection law, the problem is entirely homemade and also by the standards of EU administrative law unreasonable.

When it comes to the justification of hypothetical violations of the GATS by the EU provisions on transfer of personal data to third countries under Article XIV(c)(ii), such violation may not be capable of meeting all the prongs of this exception.

On a more positive note, because both the GATS and decisions of the WTO adjudicating bodies in EU law do not have direct effect, the practical implications of finding the EU data protection rules or their implementation inconsistent with the GATS by the WTO adjudicating bodies would be fairly confined.

In addition, being alert to the GATS-inconsistent application of the rules on transfers of personal data to a third country should translate into a positive incentive for the EU to revisit the administration of its rules. Besides, EU institutions and bodies or Member States authorities, where they implement EU law, have to conform

to administrative standards on impartial and procedurally correct decision-making in EU law too.

To some extent this article's findings could be useful in the context of the freshly negotiated CETA, as well as the ongoing negotiations towards the TTIP and TiSA. All of these agreements build on the GATS and are predestined to incorporate a general exception modelled after GATS Article XIV.

Future trade agreements also show a direct recognition of privacy and data protection as an important public policy objective and a necessary condition for spurring international trade.[135] For example, under Article 16.4 of CETA entitled 'Trust and confidence in electronic commerce', '[E]ach Party should adopt or maintain laws, regulations or administrative measures for the protection of personal information of users engaged in electronic commerce ....'[136] Similar provisions have entered the negotiations of TiSA[137] and TTIP.[138] As long as these provisions do not incorporate binding requirements, such as that measures have to be 'necessary' or 'non-discriminatory', they should not be considered as an attempt to harmonise privacy and data protection regulation via international trade law. Rather they are a recognition of the rising relevance of their protection for international trade in services.[139]

[135] Wunsch-Vincent (n 9) 519-520.
[136] CETA, version reviewed by Canadian Government and the European Commission (29 February 2016) <http://trade.ec.europa.eu/doclib/docs/2014/september/tradoc_152806.pdf> accessed 8 April 2016.
[137] TiSA, Annex on Electronic Commerce (WikiLeaks, 3 June 2015) <https://wikileaks.org/tisa/ecommerce/TiSA%20Annex%20on%20Electronic%20Commerce.pdf> accessed 8 April 2016.
[138] TTIP, EU's proposal for a text on trade in services, investment and e-commerce (31 July 2015) <http://trade.ec.europa.eu/doclib/docs/2015/july/tradoc_153669.pdf> accessed 8 April 2016.
[139] Wunsch-Vincent (n 9) 519-520.