Governing Cross-Border Data Flows: Reconciling EU Data Protection and International Trade Law

ACADEMISCH PROEFSCHRIFT

ter verkrijging van de graad van doctor
aan de Universiteit van Amsterdam
op gezag van de Rector Magnificus
prof. dr. ir. K.I.J. Maex
ten overstaan van een door het College voor Promoties ingestelde commissie,
in het openbaar te verdedigen
op woensdag 21 april 2021, te 14.00 uur

door Svetlana Iakovleva
geboren te Ryazan
Promotiecommissie

Promotor: prof. dr. I. Venzke Universiteit van Amsterdam
Copromotor: dr. J.V.J. van Hoboken Universiteit van Amsterdam
Overige leden: prof. dr. mr. M.M.M. van Eechoud Universiteit van Amsterdam
prof. dr. C. Eckes Universiteit van Amsterdam
dr. K. Irion Universiteit van Amsterdam
dr. G. Vidigal Universiteit van Amsterdam
prof. dr. C.B. Kuner Vrije Universiteit Brussel
prof. dr. J.T. Kurtz European University Institute

Faculteit der Rechtsgeleerdheid
Concise Table of Contents

LISTS OF FIGURES ........................................................................................................................................... 8
LIST OF ABBREVIATIONS ................................................................................................................................. 9
ACKNOWLEDGEMENTS .................................................................................................................................... 10
1. INTRODUCTION ........................................................................................................................................... 11
2. PERSONAL DATA TRANSFERS IN INTERNATIONAL TRADE AND EU LAW: A TALE OF TWO ‘NECESSITIES’ .......................................................................................................................... 28
3. PRIVACY PROTECTION(ISM): THE LATEST WAVE OF TRADE CHALLENGES ON REGULATORY AUTONOMY ................................................................................................................................. 70
4. RECONCILING DATA PRIVACY AND GLOBAL DATA FLOWS THE EU WAY ................................................................................................................................................................. 132
5. EU FRAMEWORK FOR TRANSFERS OF PERSONAL DATA: CRITIQUE AND DIRECTIONS FOR REFORM ........................................................................................................................................... 183
6. CONCLUSIONS .............................................................................................................................................. 245
REFERENCES ....................................................................................................................................................... 257
SHORT SUMMARY ............................................................................................................................................... 311
SAMENVATTING ............................................................................................................................................... 320
Table of Contents

LISTS OF FIGURES ............................................................................................................. 8
LIST OF ABBREVIATIONS ................................................................................................. 9
ACKNOWLEDGEMENTS ..................................................................................................... 10

1. INTRODUCTION .......................................................................................................... 11

1.1 Setting the scene: background and problem definition .................................................. 13
  1.1.1 International trade in data: what’s at stake? ................................................................. 13
  1.1.2 EU data privacy framework ...................................................................................... 15
  1.1.3 Tension between external trade policy and domestic data privacy framework ............ 16
  1.1.4 Restrictions on personal data flows: a barrier to digital trade? ................................. 18
  1.1.5 Clash between EU Charter and EU international trade commitments ....................... 19

1.2 Research questions and methodology ........................................................................ 22

1.3 Outline of the thesis .................................................................................................... 26

2. PERSONAL DATA TRANSFERS IN INTERNATIONAL TRADE AND EU LAW: A TALE OF TWO ‘NECESSITIES’ ........................................................................ 28

2.1 Introduction ................................................................................................................ 28

2.2 EU data protection and international trade law ............................................................. 28
  2.2.1 The EU regime for transfers of personal data outside the EEA ................................. 28
    2.2.1.1 Historical background ....................................................................................... 29
    2.2.1.2 The notion of transfer ..................................................................................... 34
    2.2.1.3 Restrictions on transfers .................................................................................. 38
    2.2.2 Compatibility of the EU regime for data transfer with international trade law .......... 42

2.3 Two necessities: a catch-22 for the EU ..................................................................... 47
  2.3.1. Framing the Issue ................................................................................................. 47
  2.3.2 Trade law necessity and EU Restrictions on data transfers ...................................... 54
  2.3.3 Necessity under EU law ......................................................................................... 64
  2.3.4 The incompatibility of two ‘necessities’ .................................................................. 66

2.4 Ways forward .............................................................................................................. 67

2.5 Conclusion .................................................................................................................. 69

3. PRIVACY PROTECTION(ISM): THE LATEST WAVE OF TRADE CHALLENGES ON REGULATORY AUTONOMY ........................................................................... 70

3.1 Introduction ................................................................................................................ 70

3.2 The expansion of the notion of ‘protectionism’ .......................................................... 76
  3.2.1 Defining protectionism: key disagreement ............................................................... 78
  3.2.2 Protectionism and the classical free trade idea .......................................................... 79
  3.2.3 Protectionism and ‘embedded liberalism’ of GATT 1947 ....................................... 81
  3.2.4 The new protectionism and the neoliberal discourse: towards an ever-broader conceptualisation of ‘protectionism’ ............................................................... 85
    3.2.4.1 The ‘new protectionism’ ................................................................................. 85
    3.2.4.2 ‘Fair trade’ .................................................................................................... 86
    3.2.4.3 Neoliberal discourse ...................................................................................... 90
3.2.4.4 The impact of neoliberal discourse on the formation and functioning of the international trading system ................................................................. 92

3.3 Digital protectionism: the latest wave of trade constraints on regulatory autonomy .................... 98
  3.3.1 The digital trade discourse(s) .................................................................................. 100
  3.3.2 Framing data protection as ‘digital protectionism’ in the digital trade discourse .............. 102
  3.3.3 Business interests behind the ‘digital trade’ discourse ............................................ 107
  3.3.4 Measures banning ‘digital protectionism’ in recent trade agreements ......................... 110
  3.3.5 The ‘Digital protectionism’ label as a trigger to redefine ‘barriers to trade’ .................. 115

3.4 The baseline between privacy protection and prohibitionism: the role of discourse .................. 117
  3.4.1 Normative approaches to privacy and data protection ............................................. 118
  3.4.2 Limitations of the economic approach to privacy and data protection ..................... 121

3.5 Concluding remarks: towards a new digital trade regime .............................................. 128

4. RECONCILING DATA PRIVACY AND GLOBAL DATA FLOWS THE EU WAY ................................................................. 132
  4.1 Introduction .............................................................................................................. 132
  4.2 EU horizontal provisions: a critical evaluation ........................................................... 139
    4.2.1 Background ........................................................................................................ 139
    4.2.2 Relationship with the general exception ............................................................ 140
    4.2.3 An undesirable parallel with the national security exception .............................. 145
      4.2.3.1 Interpretation of the national security exception at the WTO ......................... 146
      4.2.3.2 Interpretation of the digital trade exception for privacy and data protection ...... 151
    4.2.4 A different threshold for digital trade exceptions ............................................. 152
    4.2.5 Undermining the goal of liberalisation of cross-border data flows ....................... 156
    4.2.6 Downsides of the EU-centric approach ............................................................ 158
  4.3 Thresholds alternative to ‘necessity’, ‘it considers necessary’ and ‘it deems appropriate’ tests .... 161
    4.3.1 Non-circumvention ............................................................................................ 162
    4.3.2 Non-avoidance .................................................................................................. 165
    4.3.3 Reasonableness ................................................................................................ 169
    4.3.4 Prohibition of ‘arbitrary or unjustifiable discrimination’ or a ‘disguised restriction on international trade’ ................................................................. 171
      4.3.4.1 Blurring the borderline between the chapeau and necessity test of the general exception 173
      4.3.4.2 Chapeau as an expression of the principles of good faith and prohibition of abuse of right 174
      4.3.4.3 Factors in assessment of ‘arbitrary or unjustifiable discrimination’ .................. 175
    4.3.5 Towards the goldilocks exception for privacy and data protection in future EU trade agreements ................................................................. 176
      4.3.5.1 Undesirability of replicating the standard of chapeau in digital trade exception for privacy and data protection ......................................................... 176
      4.3.5.2 The need for a restrictive mechanism in the digital trade exception for privacy and data protection ................................................................. 179

4.4 Conclusion .............................................................................................................. 182

5. EU FRAMEWORK FOR TRANSFERS OF PERSONAL DATA: CRITIQUE AND DIRECTIONS FOR REFORM .................................................. 183
  5.1 Introduction .............................................................................................................. 183
  5.2 Constitutional contours of the EU’s framework for transfers of personal data .............. 185
    5.2.1 The relationship between the EU Charter and EU secondary data protection law ...... 185
    5.2.2 ‘Essential equivalence’: from EU secondary law to EU Charter and then back again .... 189
5.2.3 The concept of the ‘essence’ of fundamental rights ................................................................. 193
5.2.4 The ‘essence’ of the fundamental rights to privacy, protection of personal data and judicial
remedy............................................................................................................................................. 195
5.2.5 The ‘essence’ and restrictions on transfers of personal data outside the EEA .......................... 201

5.3 Weaknesses of the EU’s framework for transfers of personal data from the EU Charter perspective
......................................................................................................................................................... 203
5.3.1 The foreign surveillance issue after Schrems II ........................................................................ 208
5.3.2 Inadequacies of adequacy decisions ....................................................................................... 216
5.3.2.1 Adequacy decisions: between protection of fundamental rights and trade politics .......... 216
5.3.2.2 Limitations of adequacy decisions inherent in legal instruments with extraterritorial
application........................................................................................................................................... 220
5.3.3 Limited scalability of EU framework for transfers of personal data ........................................ 228

5.4 Directions of thought on how to improve the EU framework for transfers of personal data outside
the EEA ............................................................................................................................................. 234
5.4.1 Improving the operation of the current framework ................................................................. 235
5.4.2 Greater scalability .................................................................................................................... 237
5.4.3 Redesign .................................................................................................................................. 241

5.5 Conclusion .................................................................................................................................... 244

6. CONCLUSIONS ............................................................................................................................ 245

REFERENCES ................................................................................................................................. 257

Secondary sources ............................................................................................................................ 257

Primary Sources ............................................................................................................................... 289
Legal Texts .......................................................................................................................................... 289
International Treaties and Conventions ............................................................................................. 289
Proposed International Agreements .................................................................................................. 291
Council of Europe .............................................................................................................................. 292
European Union: Treaties and Charter .............................................................................................. 292
European Union: Regulations and Directives .................................................................................... 293
European Union: Proposed Legislation .............................................................................................. 293
European Commission Implementing Decisions: Adequacy Decisions ............................................ 293
European Parliament .......................................................................................................................... 294
EU Council Decisions .......................................................................................................................... 295
EU Member States National Legislation ............................................................................................ 295
The Netherlands: Parliamentary Documents ...................................................................................... 295
Foreign legislation ............................................................................................................................... 295
Russia .................................................................................................................................................. 295
China .................................................................................................................................................. 295
Canada ................................................................................................................................................ 295
Official Documents ............................................................................................................................ 295
United Nations .................................................................................................................................... 295
Organisation for Economic Co-operation and Development (OECD) .............................................. 295
Asia-Pacific Economic Cooperation (APEC) ....................................................................................... 296
World Trade Organization (WTO) ..................................................................................................... 296
General Agreement on Tariffs and Trade (GATT) .............................................................................. 296
European Union .................................................................................................................................. 297
European Commission .......................................................................................................................... 297
Council of the European Union ........................................................................................................... 299
Council of Europe ............................................................................................................................... 299
Article 29 Working Party ..................................................................................................................... 299
European Data Protection Board (EDPB) ............................................................................................ 300
Case Law ........................................................................................................................................ 303
  Court of Justice of the European Union (CJEU): Judgements .................................................. 303
  Court of Justice of the European Union (CJEU): Advocate General (AG) Opinions ............... 304
  European Court of Human Rights (ECtHR) ................................................................................. 304
  World Trade Organization (WTO) .............................................................................................. 305
  General Agreement on Tariffs and Trade (GATT) ................................................................. 307
  International Centre for Settlement of Investment Disputes .................................................... 307
  National Cases ......................................................................................................................... 308
  Germany ...................................................................................................................................... 308
  Ireland ......................................................................................................................................... 308

Electronic Sources ....................................................................................................................... 308

SHORT SUMMARY .................................................................................................................. 311

SAMENVATTING ...................................................................................................................... 320
Lists of Figures

Figure 1: Overlap between the EU Charter and Trade ‘Necessities’ …………………………………63
Figure 2: Protectionism in economic and pluralist discourses ………………………………………70
## List of Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>AI</td>
<td>Artificial Intelligence</td>
</tr>
<tr>
<td>APEC</td>
<td>Asia-Pacific Economic Cooperation</td>
</tr>
<tr>
<td>APEC CBPR</td>
<td>Asia-Pacific Economic Cooperation Cross-Border Privacy Rules</td>
</tr>
<tr>
<td>BCR</td>
<td>Binding Corporate Rules</td>
</tr>
<tr>
<td>CCPA</td>
<td>California Consumer Privacy Act</td>
</tr>
<tr>
<td>CETA</td>
<td>Comprehensive Economic and Trade Agreement</td>
</tr>
<tr>
<td>CJEU</td>
<td>Court of Justice of the European Union</td>
</tr>
<tr>
<td>CPTPP</td>
<td>Comprehensive and Progressive Agreement for Trans-Pacific Partnership</td>
</tr>
<tr>
<td>DG</td>
<td>Directorate General</td>
</tr>
<tr>
<td>DPA</td>
<td>Data Protection Authority</td>
</tr>
<tr>
<td>ECEFP</td>
<td>Executive Committee on Economic Foreign Policy</td>
</tr>
<tr>
<td>ECCHR</td>
<td>European Convention on Human Rights</td>
</tr>
<tr>
<td>ECIPPE</td>
<td>European Centre for International Political Economy</td>
</tr>
<tr>
<td>ECtHR</td>
<td>European Court of Human Rights</td>
</tr>
<tr>
<td>EDPB</td>
<td>European Data Protection Board</td>
</tr>
<tr>
<td>EDPS</td>
<td>European Data Protection Supervisor</td>
</tr>
<tr>
<td>EEA</td>
<td>European Economic Area</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>EU Charter</td>
<td>Charter of the European Union</td>
</tr>
<tr>
<td>GATS</td>
<td>General Agreement on Trade in Services</td>
</tr>
<tr>
<td>GATT</td>
<td>General Agreement on Tariffs and Trade</td>
</tr>
<tr>
<td>GDPR</td>
<td>General Data Protection Regulation</td>
</tr>
<tr>
<td>ICCPR</td>
<td>International Covenant on Civil and Political Rights</td>
</tr>
<tr>
<td>ICT</td>
<td>Information and Communications Technology</td>
</tr>
<tr>
<td>ITO</td>
<td>International Trade Organisation</td>
</tr>
<tr>
<td>JEFTA</td>
<td>EU-Japan Economic Partnership Agreement</td>
</tr>
<tr>
<td>KORUS FTA</td>
<td>United States-Korea Free Trade Agreement</td>
</tr>
<tr>
<td>MFN</td>
<td>Most Favoured Nation</td>
</tr>
<tr>
<td>NAFTA</td>
<td>North American Free Trade Agreement</td>
</tr>
<tr>
<td>NGO</td>
<td>Non-Governmental Organisation</td>
</tr>
<tr>
<td>OECD</td>
<td>Organisation for Economic Co-operation and Development</td>
</tr>
<tr>
<td>OPC</td>
<td>Office of the Privacy Commissioner</td>
</tr>
<tr>
<td>PIPEDA</td>
<td>Personal Information Protection and Electronic Documents Act</td>
</tr>
<tr>
<td>PNR Agreement</td>
<td>Personal Name Records Agreement</td>
</tr>
<tr>
<td>SCC</td>
<td>Standard Contractual Clauses</td>
</tr>
<tr>
<td>TBT Agreement</td>
<td>Agreement on Technical Barriers to Trade</td>
</tr>
<tr>
<td>TEU</td>
<td>Treaty on European Union</td>
</tr>
<tr>
<td>TFEU</td>
<td>Treaty on the Functioning of the European Union</td>
</tr>
<tr>
<td>TiSA</td>
<td>Trade in Services Agreement</td>
</tr>
<tr>
<td>TRIPS</td>
<td>Agreement on Trade-Related Aspects of Intellectual Property Law</td>
</tr>
<tr>
<td>TTIP</td>
<td>Transatlantic Trade and Investment Partnership</td>
</tr>
<tr>
<td>UDHR</td>
<td>Universal Declaration of Human Rights</td>
</tr>
<tr>
<td>USITC</td>
<td>United States International Trade Commission</td>
</tr>
<tr>
<td>USMCA</td>
<td>United States–Mexico–Canada Agreement</td>
</tr>
<tr>
<td>VCLT</td>
<td>Vienna Convention on the Law of Treaties</td>
</tr>
<tr>
<td>WTO</td>
<td>World Trade Organization</td>
</tr>
</tbody>
</table>
Acknowledgements

Although writing a PhD thesis can be at time an isolating experience, I was privileged to be guided, supported and encouraged by multiple people.

I would like to thank my PhD supervisors, Professors Joris van Hoboken and Ingo Venzke for having faith in me being able to lift this project up while working part time at De Brauw Blackstone Westbroek, for their time and effort in guiding me along the way, and for their thorough reading of my drafts. Their input was invaluable in bringing the quality of my work to the next level. I am also grateful to them for their positive reinforcement and encouragement. My sincere gratitude also goes to my parents for always being there for me, for their unconditional love and support throughout yet another study and research project of mine as well as for their support with my relocation to the Netherlands, without which this project would have never been possible. I am deeply indebted to Daniel for his patience, constant support and encouragement to make small steps towards completing this project and for letting me see the light at the end of the tunnel even when that light was meek and far away. I would also like to thank my friends for their support throughout this project, and in particular, Olga Zrilina, Radmila Nikitina, Svetlana Romaniko, Maria Taylor, Momchil Tsonev, Maya and Oleg Zupnik. I would like to acknowledge my current and former colleagues from the University of Amsterdam and De Brauw Blackstone Westbroek for the insightful conversations, collaboration and support. I would particularly like to single out Ot van Daalen, Sarah Eskens, Marco Fabbri, Kristina Irion, and Joao Pedro Quintais from the University of Amsterdam; and Axel Arnbak, Ties Boonzajer Flaes, Maaike Boomgaard, Wessel Geursen, Salima Guettache, Christien de Kruif (who also helped with proofreading the Dutch summary), Geert Potjewijd, Esther Rosenkrantz, and Helma van der Wal (who also helped with designing the visuals) from De Brauw Blackstone Westbroek. I am also grateful to Alice Garner for her meticulous proofreading of this manuscript. Last but not least, I am grateful to my cat Charlie for radiating positive vibes while sleeping on my work table at almost all times of me working on this thesis.
1. Introduction

Between 2014-2016, a wave of protests swept across Europe. In Brussels, Amsterdam, Rome, Barcelona, Berlin, and more, thousands of people filled the streets chanting slogans: ‘Stop TTIP, TiSA & CETA now!’ ‘No TTIP, TiSA & CETA!’ ‘We need TTIP like a fish needs a fishing rod!’ The source of the public discontent was the ‘new generation’ of trade agreements that the EU was covertly negotiating with some of its most important trading partners: the Transatlantic Trade and Investment Partnership (TTIP) with the United States, the Comprehensive Economic Trade Agreement (CETA) with Canada, and the Trade in Services Agreement (TiSA) with 22 members of the World Trade Organisation (WTO), together representing approximately 70 per cent of world trade in services.1 The protests were sparked not only by the substance of the agreements, namely their perceived threats to EU domestic policy in areas such as the environment, agriculture, culture and the media, but also by the process that created them, namely its secrecy and lack of democratic legitimacy and accountability. Although the possible implications of these agreements – primarily TTIP and TiSA – on the EU acquis and policy on privacy and data protection escaped the eye of the broader public at that time, they did not go unnoticed by either digital rights and consumer organisations and activists, or by EU institutions not involved in those trade negotiations.2 For the first time, the tension between the liberalisation of digital trade, on the one hand, and data privacy, on the other, became a broader political issue rather than just a topic of a theoretical debate.

This thesis explores the difficulties in reconciling these important legal and policy objectives of the European Union. On the one hand, the EU Charter of Fundamental Rights (EU Charter) guarantees the protection of the rights to privacy and the protection of personal data3 as fundamental rights. On the other hand, in its external trade policy, the EU seeks liberalisation of cross-border data flows, maintaining and developing a globally binding rules-based trading system to ensure appropriate access to foreign markets for EU businesses. The fundamental rights protection of data privacy in the EU originated as a prerequisite for the free flow of personal data in the internal market. It was, in other words, intertwined with the economic goals underlying the union. In EU external policy however, until recently, the two objectives had little in common and, therefore, did not come into

---


2 See e.g. EDRI (2015); EDRI (2016); Ling (2016); European Parliament resolution of 8 July 2015 containing the European Parliament’s recommendations to the European Commission on the negotiations for the Transatlantic Trade and Investment Partnership (TTIP) (2014/2228(INI)); European Parliament resolution of 3 February 2016 containing the European Parliament’s recommendations to the Commission on the negotiations for the Trade in Services Agreement (TiSA) (2015/2233(INI)).

3 Throughout this thesis, the fundamental rights to privacy and the protection of personal data will also be jointly referred to as fundamental rights to data privacy.
conflict. The change was caused by the fact that cross-border flows of personal and other data have become the ‘lifeblood of international trade’.4 The area of digital commerce is taking up a growing share of world trade.5 Yet the collection and commercial use of personal data also implicates essential noneconomic values. Those values explain why personal data is protected by the EU Charter, and why it was instantiated with a high degree of specificity by the General Data Protection Regulation (GDPR). Specifically, the thesis examines how these two objectives might be pursued simultaneously.

This topic is highly relevant to current policy debate in the EU on the data privacy implications of cross-border data flows, which takes place against the backdrop of ongoing digital trade negotiations with several trading partners, and the trade policy review (of which digital trade is part) launched by the European Commission in June 2020.6 Furthermore, digital trade is an important part of the EU industrial policy in the next four years.7

This thesis contributes to academic literature by undertaking a comprehensive analysis of the issue of cross-border data flows from an EU data protection and international trade perspective, thus bridging the compartmentalisation of these two areas of law. As compared to existing literature, which typically takes either an international trade or a data protection perspective, this thesis undertakes an in-depth engagement with both areas of law with a specific emphasis on the interaction between them. This approach allows the thesis to propose ways of bridging the gap between international trade and EU rules governing cross-border data flows while preserving the normative values underlying each of these sets of rules.

The societal relevance of this work lies in the necessary reconciliation of European citizens’ rights, guaranteed under the EU Charter, with the realities of global digital commerce which will contribute to economic growth and job creation. The governance of cross-border flows of personal data must be at once solidly anchored in EU law and values, and capable of being ported to the trade law field. This is important because the outcome of trade negotiations will affect each and every person in the EU, as almost everybody uses the internet. Guaranteeing sufficient protection of fundamental rights whilst ensuring that society can benefit from digital commerce is the difficult challenge that this thesis aims to meet.

1.1 Setting the scene: background and problem definition

1.1.1 International trade in data: what’s at stake?

The commercial use of personal data enables digital trade and contributes to economic growth. It may also generate individual benefits. However, those benefits often seem both remote and indirect when compared to the risks posed to individuals by the misuse of their data, such as identity theft, access to data by foreign surveillance and law enforcement authorities, profiling, unwanted marketing communications, discrimination, and denial of access to essential services, to name just a few. Unlike data, which can simultaneously be present in multiple locations and fall under the jurisdiction of multiple legal regimes, individuals retain a close connection with a particular State through the institutions of citizenship or residency. It is first and foremost that State that must guarantee the individuals’ human rights and protect them from the undue actions of other States. The level of fundamental rights protection that individuals can expect in the EU member states may not necessarily be upheld once personal data is processed in other countries, such as the US, China or Russia. Simply put, while trade in data is international, protection of individual rights largely remains the prerogative of domestic law, especially when it comes to the protection of the fundamental rights to privacy and the protection of personal data. Although these rights are recognised by important international and regional human rights law instruments, and governed by several regional guidelines, countries across the globe still have important disagreements on the normative rationales underlying the protection of the two rights and the approaches to transfers of personal data.

Cross-border trade in digital goods and services is increasingly dependent on personal data. Globalisation and the decentralisation of production and distribution value chains have made the cross-border movement of information – commercial, machine-generated and personal – crucial for the production and provision of services, both online and offline, as well as the day-to-day management of companies. Projecting this economic reality, promising unprecedented efficiency gains, economic development and growth, onto a global legal landscape compartmentalised by multiple domestic legal systems, is a sobering exercise. When set against the economic benefits driving globalisation, these legal systems must consider how these benefits fit into a broader set of national and regional priorities, such as national security, fundamental rights protection, industrial policy, and cultural values. Differences in the relative weight accorded to each

---

8 In this thesis, the EU acquis is also referred to as ‘domestic’ law.
9 Art. 12 UDHR; Art. 17 ICCPR.
10 Art. 8 ECHR; Convention 108+.
of those priorities vis-à-vis the economic and political gains from cross-border data flows have resulted in a diverse set of diverging domestic rules governing such flows, especially when it relates to identified or identifiable individuals (that is, the definition of personal data in the GDPR).

Companies doing business globally face the challenges of compliance with several data protection regimes and rules for cross-border transfers of personal data in several countries. Having a lot to gain from dismantling restrictions on the free flow of data, a plethora of industry-funded think-tanks try to shape the global policy agenda by painting a grim picture in which protection of data privacy is framed as a barrier to trade and a threat to economic progress.\(^\text{13}\) Using an often one-sided narrative of ‘digital protectionism’, surveillance capitalists portray their practices as ‘inevitable expressions of the technology they employ’\(^\text{14}\) and digital globalisation as the next logical step of economic integration and development.\(^\text{15}\) Individuals, on the other hand, must deal with the limitations of domestic legal systems to enforce their rights effectively against the misuse of their personal data on a global scale. Although individuals do also gain from the free flow and ubiquitous monetisation of their data by companies, for example, in the form of personalised services, they also have a lot to lose. The potential damage to individuals and society as a whole, transcends the direct economic losses from data breaches and identity threats. It includes discrimination and social exclusion; the undermining of human dignity by transforming human experiences into behavioural data; and the shaping of individuals’ behaviour and choices, both on the micro level of what news to read and items to buy, and on the macro level of expressing political preferences. From a global perspective, massive cross-border appropriation of personal data can be compared to resource extraction.\(^\text{16}\) For example, Couldry and Mejias argue that cross-border data flows ‘are as expansive as historic colonialism’s appropriation of land, resources, and bodies, although the epicenter has somewhat shifted’.\(^\text{17}\) In their view, the transformation of human actors and social relations formalised as data, into value, leads to power imbalance (between colonial power and colonised subjects).\(^\text{18}\) Against this backdrop, as Morozov puts it, the EU’s ‘much-cherished commitment to data protection … aimed, above all, at protecting citizens from excessive corporate and state intrusion – is increasingly at odds with the “grab everything” mentality of contemporary capitalism’.\(^\text{19}\)

\(^{13}\) See Morozov (2015).


\(^{15}\) For a discussion, see Section 3.3.

\(^{16}\) Couldry, Mejias (2019), pp. 337-338.

\(^{17}\) Ibid. But see Mueller, Grindal (2019), p. 82, challenging this point of view.


\(^{19}\) Morozov (2015).
1.1.2 EU data privacy framework

Since 2009 (when the EU Charter took effect), the right to the protection of personal data has been a binding fundamental right in the EU (Article 8 of the EU Charter), separate from the fundamental right to privacy (Article 7 of the EU Charter).\(^\text{20}\) The EU Charter has the highest legal status in the EU, on a par with the Founding Treaties. Just as personal data has both economic and societal value, the European data protection regime, first introduced by the 1995 Data Protection Directive, has a dual objective: protecting the fundamental rights and freedoms of individuals, in particular their right to the protection of personal data, and ensuring the free flow of personal data within the European Economic Area (EEA).\(^\text{21}\) Conflicting at first glance,\(^\text{22}\) these objectives are easier to reconcile if seen as cause and effect, or as the ‘why’ and the ‘how’. The harmonisation of data protection rules was a prerequisite for the free flow of personal data without undermining individuals’ rights to the protection of such data originating from EU member states affording a higher level of protection (the ‘why’).\(^\text{23}\) The fundamental rights approach (‘the how’) sets the level of protection of personal data which the EU-wide personal data protection framework should attain. However, the constitutionalisation of the EU has put the economic needs that necessitated the creation of the EU-wide data protection framework in the first place, to the background, and emphasised the non-economic goals of the current European data protection law.\(^\text{24}\) That said, the GDPR, adopted under the EU’s competence to legislate on the fundamental right to the protection of personal data, is still cited as one of the pillars of the EU Digital Single Market.\(^\text{25}\) Recently, robust protection of the fundamental rights to privacy and personal data has also become a part of the EU response to a growing concern about ‘technological’ or ‘digital sovereignty’, with regard to the growing economic and social influence of non-EU (and primarily American) technology companies.\(^\text{26}\) The EU is increasingly using technological or digital sovereignty labels ‘as a means of promoting the

\(^{20}\) Despite the separation of the rights to privacy and the protection of personal data in the EU Charter, this thesis often refers to these two rights jointly. The issue on the relationship between these two rights has generated much academic debate but remains unresolved. For a recent recount of the state of this debate, see Lynskey (2020), pp. 29-32. For a deeper analysis of the intricate relationship between the two rights, see Lynskey (2015) pp. 89-106. For a comprehensive historical account of the issue, see González Fuster (2014).


\(^{22}\) See e.g. Macenaite (2017), pp. 506-507.


\(^{24}\) Lynskey (2013). For further discussion, see Sections 2.2.1.1 and 2.3.3.


\(^{26}\) Madiega (2020), p. 1. For a discussion on how this reflects in the EU trade policy, see Chapter 4.
notion of European leadership and strategic autonomy in the digital field’.27 In the international arena, the EU’s digital strategy, anchored in European values and fundamental rights, ties into the ‘ideal of a social European model’28 alternative to the American model of ‘surveillance capitalism’.29

1.1.3 Tension between external trade policy and domestic data privacy framework

The view that domestic restrictions on international data flows in general, and on personal data flows in particular, are a form of undesirable ‘protectionism’ is now front and centre in academic, public and policy conversations on the topic, as the focus of international trade negotiations shift to digital trade’.30 From this angle, unrestricted cross-border data flows promise global economic growth, and are often perceived as a *bonum in se*.31 However, the tendency of international trade law to liberalise international data flows is at odds with legal regimes that restrict such flows on privacy and data protection grounds, especially that of the European Union.32 As a result, the data flow issue has become ‘the new battlefield’33 between domestic legal regimes, not only between the United States and the European Union, but also between the European Union and its other trading partners.34 While the debate often runs along the line of eliminating ‘digital protectionism’, there is an ideological divide on whether, and to what extent, data privacy protection should fall under or be excluded from the scope of this notion.35

Conflicts are thus bound to arise from the fact that, while international trade law

---

29 Zuboff (2019); Zuboff (2015); Madiega (2020), p. 3.
30 For further discussion see Section 3.3.
31 Ibid.
33 Burri (2017c), p. 408.
34 For example, provisions on cross-border flows of information, including personal data, have been a contentious point in the negotiations of the JEFTA. See Bartl, Irion (2017). Not being able to reach an agreement in trade negotiations, instead of such provisions, the parties included a three-years review clause in the final version of the agreement. Aaronson, Leblond (2018), p. 261. Cross-border flows of personal data from the EU to Japan were ultimately regulated through an Adequacy Decision. For its data protection to be recognised as ‘adequate’ under EU law, Japan has amended its legislation and has undertaken additional commitments in the adequacy decision. The Adequacy Decision for Japan was adopted on 23 January 2019, shortly before JEFTA took effect. European Commission, Press Release: *European Commission Adopts Adequacy Decision on Japan, Creating the World’s Largest Area of Safe Data Flows*, IP/19/421, 23 January 2019.
35 For a discussion see Section 3.3.
increasingly aims to liberalise data flows to facilitate digital cross-border trade, EU data protection law restricts cross-border transfers of personal data outside the EEA. Grounded in the fundamental rights to the protection of privacy and personal data under the EU Charter,\(^{36}\) the rules for transfers of personal data outside the EEA aim to ensure that the level of protection guaranteed in the EU by the GDPR is not undermined as personal data leaves the EEA.\(^{37}\) Although the GDPR does not explicitly refer to any fundamental right except for the fundamental right to the protection of personal data, this does not mean that the GDPR furthers this right alone. This is clear from recital 4 of the GDPR, which requires that the ‘processing of personal data should be designed to serve mankind’. Furthermore, the right to the protection of personal data itself enables a multitude of other fundamental rights and values.\(^{38}\) This right is triggered by any processing of personal data (itself defined very broadly\(^{39}\) ), which is now integral to almost any societal activity. It is a proxy to a wide array of public policy interests from the protection of democracy, human dignity and personality rights, to obtaining a fair share of the economic value derived from personal data.\(^{40}\) According to Rodota, ‘[d]ata protection can be seen to sum up a bundle of rights that make up citizenship in the new millennium’.\(^{41}\)

As a result, unlike the internal trade liberalisation within the EU single market (which led to the emergence of the EU data protection framework in the past), the EU’s external trade liberalisation goal is in tension with the EU data privacy law, due to their opposite normative valences. EU data privacy law can tolerate transfers of personal data outside the EEA only to the extent that these transfers are compliant with the EU Charter and the GDPR. In turn, international trade law can tolerate the EU’s restrictions on personal data transfers only to the extent that they comply with the EU’s international trade liberalisation commitments, including possible exceptions thereto.

\(^{36}\) CJEU, Schrems I, paras. 72-73; CJEU, Schrems II, para. 94; CJEU, Opinion on EU-Canada PNR Agreement, para 214.

\(^{37}\) Art. 44 GDPR, CJEU, Schrems I, paras 72-73; CJEU, Schrems II, paras. 92, 94 See also González Fuster (2016), p. 168.


\(^{39}\) For a discussion see Section 5.3.3.

\(^{40}\) See e.g. Lynskey (2014), p. 573-574; Rouvroy, Poulet (2009), pp. 53-54, 57 (contending that the rights to privacy and data protection have ‘an “intermediate” rather than a “final” value, because they are “tools” through which more fundamental values, or more “basic” rights—namely human dignity and individual personality rights—are pursued;’ that the rights to privacy and personal data protection protect the fundamental value of personal autonomy against the threats of technological evolution, and that they constitute social structural tools for preserving a free and democratic society). See also Delacroix, Lawrence (2019); Hall, Pesenti (2017); Hardinges (2018); Initiatiefnota van het lid Verhoeven over mededinging in de digitale economie; Motie van het lid Buitenweg c.s. over vormgeving van data trusts in Nederland, 16 december 2019, KST351347, 35134, nr. 7 exploring data trusts as a means of sharing value obtained through commercial use of personal data.

\(^{41}\) Rodotà (2009), pp. 77-80.
1.1.4 Restrictions on personal data flows: a barrier to digital trade?

The WTO is the main body administering international trade rules. Both the EU and its member states are parties to the Marrakesh Agreement establishing the WTO. The WTO notably includes a binding dispute-settlement system. The current framework dates back to 1995 and does not regulate specifically cross-border data flows. However, general principles of trade law, such as most-favoured nation and national treatment or market access commitments under the General Agreement on Trade in Services (GATS), do apply to EU restrictions on cross-border data flows. However, the WTO’s role has recently decreased due to political circumstances and the multiplication of regional and bilateral trade agreements. In response to rapid technological change, new international law obligations are emerging through bi- and plurilateral trade venues that by-pass the WTO. So-called ‘new generation’ free trade agreements, entered into by the EU’s most important trading partners, such as Canada, Japan and the US, include provisions obliging parties to allow free cross-border flows of information, including personal data. These disciplines have, for example, been included in the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), and in the recent US-Mexico-Canada Agreement (USMCA), and the US-Japan Digital Trade Agreement. In all such agreements, a free data flow obligation is counterbalanced by an exception, strongly resembling that of the GATS Article XIV(c), that allows parties to derogate from it, in order to adopt and maintain regulation in the public interest. There is also a movement afoot to update WTO rules. Cross-border data flows are high on the agenda in the recently launched negotiations on e-commerce in the WTO between 76 WTO members.

Taking the view that domestic restrictions on cross-border flows of personal data are a barrier to reaping the benefits of global digital trade, an increasing volume of literature either highlights the risk of inconsistency of personal data protection with the rules of the WTO, asks for new rules to ensure free flows of personal data across borders, or both.

---

42 WTO Agreement.
43 Although the Marrakesh Agreement is a mixed agreement from an EU law perspective, Eckes explains that “this mixed nature has, in practice, been replaced by EU dominance”. Eckes (2019), p. 186.
44 Art. 14.11 CPTPP, which states: ‘Each Party shall allow the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business of a covered person’.
45 Under Art. 19.11 of the USMCA, ‘[n]o Party shall prohibit or restrict the cross-border transfer of information, including personal information, by electronic means if this activity is for the conduct of the business of a covered person’.
46 Art. 11 of the US – Japan Digital Trade Agreement.
49 For a discussion on how data protection is being framed as digital trade barrier in the economic digital trade discourse, see Section 3.3.
50 See Section 2.2.2.
The elimination of such restrictions remains one of the contentious issues of most recent trade negotiations in North America, Europe and Asia.\(^{51}\) Meanwhile, as personal data has become an integral part of digital services, the EU constitutional protection of the rights to privacy and the protection of personal data (of which restrictions on personal data transfers is an important pillar), is actually strengthening.\(^{52}\) As a result, with the international trade regime increasingly moving towards ‘free’ digital trade,\(^{53}\) the risk that the EU’s international trade law commitments to liberalise the cross-border movement of services, on the one hand, and the protection of the fundamental rights to data privacy, on the other hand, will clash is very real.

The recent Schrems II judgement of the Court of Justice of the European Union (CJEU) invalidated, second time around, the EU-US legal framework for transatlantic flows of personal data, the EU-US Privacy Shield. It asserted a high legal standard for systematic transfers of personal data in general and created additional pressure on the EU approach to the governance of personal data transfers from an international trade law perspective. In reaction, one of the US commentators suggests that instead of engaging in further negotiations with the EU on its fundamental rights terms, the US should respond along the lines of international trade law and economic sanctions.\(^{54}\) For example, the US should treat the CJEU’s judgement as a violation of the WTO rules and retaliate using available US trade law mechanisms or impose sanctions against the EU together with countries like UK, Canada, Australia and India.\(^{55}\)

1.1.5 Clash between EU Charter and EU international trade commitments

A clash between the EU’s constitutional protection for personal data (as translated into a framework for cross-border transfers of personal data in the GDPR) and the EU’s trade liberalisation commitments is not in and of itself a reason to cry foul. Both the EU Charter and international trade law contain exceptions that allow each system to tolerate encroachments on their respective rules by the other, within certain limits. As long as the exceptions in both systems are aligned, they can limit the degree of tension between the two systems.

Most prominently among existing exceptions, the majority of international trade agreements governing trade in services provide for so-called ‘general exceptions’, which

\(^{51}\) See e.g. Cerulus, Scott (2019); Pant, Sarma (2019); Fefer (2019).
\(^{52}\) See Section 2.2.1.1.
\(^{53}\) Some countries, such as India, the African group and the Least Developed Countries, however, are critical about the e-commerce provisions in trade agreements, including those liberalising cross-border data flows. See e.g. Work Programme on Electronic Commerce, Report of Panel Discussion on ‘Digital Industrial Policy and Development’: Communication from the African Group, JOB/GC/133, 21 July 2017; Saez, C. (2017).
\(^{54}\) Baker (2020).
\(^{55}\) Ibid.
are modelled after or incorporate mutatis mutandis the one contained in Article XIV of the GATS.\textsuperscript{56} This exception preserves the regulatory autonomy of parties to an international trade agreement and enables them to adopt and maintain measures ‘necessary’ to protect the privacy of individuals in relation to the processing and dissemination of personal data, even if such measures run counter to the member’s international commitments (the trade necessity test). In other words, trade rules start from the premise that cross-border flows should be free, and contain an exception that might allow the EU to protect personal data. Article 52(2) of the EU Charter, in turn, allows the EU to limit fundamental rights if this is ‘necessary’ to meet objectives of general interest to the EU or to protect the rights and freedoms of others (the EU Charter necessity test). As interpreted by the CJEU, this provision allows EU bodies to conclude an international agreement, which involves transfers of personal data outside the EEA, if the conditions laid out in this clause and most importantly that the Charter’s necessity test, are fulfilled.\textsuperscript{57} The EU Charter protects the fundamental right implicated by the processing of personal data and contains an exception that might be sufficient, in certain circumstances, to allow the EU to make commitments concerning cross-border flows of personal data in international trade agreements. Among other things, this thesis explores the tension between these two exceptions and examines various possibilities allowing for the objectives behind them to be met.

Not surprisingly in light of the above, the possibility of the inclusion of a provision on cross-border data flows accompanied by a GATS Article XIV-type exception for data protection in TiSA and TTIP\textsuperscript{58} – both now stalled – sparked a strong push-back from European Parliament, academics and civil society in 2015-2016.\textsuperscript{59} Later, in order to avoid

---

\textsuperscript{56} See, e.g., Art. 28.3(2)(c)(ii) CETA; Art. 8.62(e)(ii) EU-Singapore FTA; Art. 167(1)(e)(ii) EU-Colombia-Peru FTA; Art. 7.50(e)(ii) EU-Korea FTA; Art. 203(1)(e)(ii) EU-Central America Association Agreement; Art. 135(1)(e)(ii) EU-Chile Association Agreement; Art. 23.1(2) KORUS; Art. 21.1(2) US-Singapore FTA; Art. 21.1(2) Dominican Republic-Central America-US FTA; Art. 21.1(2) US – Panama TPA; Art. 32.1(2) USMCA; Art. 29.1(3) CPTPP.

\textsuperscript{57} CJEU, \textit{Opinion on EU-Canada PNR Agreement}, paras 67, 70.

\textsuperscript{58} See Le Roux (2017), p. 731 (‘The USTR includes an essential element that is still not addressed by the European Commission in its initial proposal, which is cross-border data flows. The United States thus remains very offensive on the matter and reproduced what they have already pushed through in the KORUS and the TPP texts.’) A bracketed draft for Article 2 of the Annex on Electronic Commerce to TiSA included a prohibition to ‘prevent a service supplier of another Party from transferring, accessing processing or storing information, including personal information, within or outside the Party’s territory, where such activity is carried out in connection with the conduct of the service supplier’s business’. Coalition For Privacy & Free Trade (2013) (‘The Obama Administration already has recognized the importance of interoperable privacy frameworks to global economic progress and prosperity: . . . The United States is committed to engaging with its international partners to increase interoperability in privacy laws by pursuing mutual recognition, the development of codes of conduct through multistakeholder processes, and enforcement cooperation.’) But see Fontanella-Khan (2013) (noting EU officials’ fear that ‘finding a middle ground with the U.S. would only lower overall E.U. privacy standards’).

\textsuperscript{59} See e.g. Irion, Yakovleva, Bartl, pp. 44-45, 59-60; Fernández Pérez (2016); European Parliament resolution of 8 July 2015 containing the European Parliament’s recommendations to the European
any risk of undermining the fundamental rights to privacy and the protection of personal data, the EU ultimately refrained from including such a provision in the Economic Partnership Agreement between the European Union and Japan (JEFTA) and the revision of the EU-Mexico Free Trade Agreement. In the case of Japan, the absence of such a clause was accompanied by the adoption of a mutual adequacy decision under the GDPR shortly before JEFTA took effect.

In 2018, after a thorny interinstitutional dialogue, the EU developed horizontal provisions on cross-border data flows and the protection of privacy and personal data for its prospective digital trade agreements. They include a specific exception for privacy and data protection, similar to the national security exception of Article XIVbis of the GATS – a text much broader than the above-mentioned general exception. Among other things, the proposed exception explicitly states that GATS-inconsistent measures for the protection of personal data and privacy are allowed, including rules limiting transfers of personal data. The EU has tabled these model clauses in digital trade negotiations ever since, including into the EU proposal for the WTO rules on electronic commerce, which are intended to co-exist with the general exception for privacy and data protection modelled after Article XIV(c)(ii) GATS included in the same agreement.

Unlike the US approach to data flows, already implemented in CPTPP, USMCA and the US-Japan Digital Trade Agreement, the EU’s approach in the above-mentioned 2018 model clauses contains a narrower prohibition on restrictions of cross-border data flows and a broader exception for domestic privacy and data protection rules. Adherence to the US model by countries that maintain a free flow of personal data from the EU, in particular, Canada, Japan and New Zealand, puts pressure on the EU’s restrictions on transfers of personal data.


Both agreements include a commitment to reconsider the issue within three years after the agreement enters into force. See Art. 8.81 of JEFTA, Art XX of the Digital trade title of the Modernised EU-Mexico FTA. See also Fortnam (2017).

European Commission, Adequacy Decision for Japan. Although this decisions is commonly referred to as ‘mutual’, from a legal perspective it these are two unilateral decisions adopted at the same time.

EU model clauses on cross-border data flows; see also Aaronson, Leblond (2018) p. 262; Fortnam (2017).

For an overview and discussion, see Section 4.2.


See e.g. Article X.1(2) of the EU proposal for Chapter X Exceptions of the EU-New Zealand FTA, 25 June 2019. This provision includes a general exception for privacy and data protection modelled after the general exception in the GATS Article XIV(c)(ii). EU proposals for Exceptions chapter for other trade agreements discussed in this thesis are not available as of the time of writing. For a discussion, see Section 4.2.2.

For further discussion see Sections 3.3.4 and 4.2.1.
personal data. The EU is unlikely to agree to the cross-border data flow provisions such as those advanced by the US just mentioned above, for this would mean an unjustifiable derogation from EU Charter-based fundamental rights.\textsuperscript{67} The clash between the US and the EU model is especially apparent in the Brexit negotiations between the EU and the UK, where the UK submitted provisions on cross-border data flows modelled after the US model,\textsuperscript{68} while the EU submitted its model clauses as discussed above.\textsuperscript{69} There is therefore an urgency to evaluate the EU proposal and see how much room the EU has to negotiate with the UK and other trading partners, assuming that the EU \textit{should} continue to protect the rights to privacy and the protection of personal data as fundamental rights.

From an EU internal perspective, the EU’s own framework for transfers of personal data has been criticised on multiple occasions for its broad reach and insufficient and inconsistent enforcement.\textsuperscript{70} An important prerequisite of developing an alternative framework, however, is a deeper understanding of the relationship between Articles 7, 8 and 52(1) of the EU Charter and the GDPR, and the extent to which the EU legislator is free to design the framework for transfers of personal data without overstepping constitutional boundaries. This issue ties into a broader ongoing academic debate on the essence of the EU fundamental rights and the relationship between EU primary and secondary law.

1.2 \textbf{Research questions and methodology}

The main research question answered in this thesis is:

\textit{how should commitments on cross-border data flows in future EU trade agreements be reconciled with the protection of the fundamental rights to privacy and personal data?}

The thesis answers this question in four steps by addressing the following four sets of sub-questions, relating to (1) compatibility, (2) protectionism, (3) reconciliation, and (4) reform of the EU restrictions.

1. \textit{The compatibility question}. Are the primary obligations of the GATS and EU restrictions on transfers of personal data outside the EEA compatible, and if not, can this incompatibility be remedied by the application of the general exception in the

\textsuperscript{67} This is because, as explained in Section 2.3.4, the trade ‘necessity test’ that lies at the heart of the exception for privacy and data protection in US-led trade agreements requires a derogation from fundamental rights beyond the limits set by Article 52(1) of the EU Charter.

\textsuperscript{68} Arts. 18.13 and 18.14 of the Draft Working Text for a Comprehensive Free Trade Agreement Between the United Kingdom and the European Union, Draft UK Negotiating Document.

\textsuperscript{69} Draft text of the Agreement on the New Partnership with the United Kingdom, European Commission, 18 March 2020, p. 135.

\textsuperscript{70} For a discussion, see Section 5.3.
GATS and Article 52(1) of the EU Charter?

2. *The protectionism question.* Do EU restrictions on transfers of personal data outside the EEA constitute protectionism? Where should the line be drawn between protection and protectionism? What roles do more general discourses play in determining what amounts to legitimate protection and what to illegitimate protectionism? How does framing the debate on privacy and data protection in terms of ‘digital protectionism’ affect the normative foundations of domestic regulation on privacy and personal data, and setting appropriate levels of privacy and personal data protection?

3. *The reconciliation question.* Do the model clauses proposed by the EU for digital trade chapters meet the EU’s ambitions of reconciling cross-border data flows under international trade law with the protection of the rights to privacy and personal data as fundamental rights under the EU Charter, whilst maintaining a global rules-based trading system? If they do not reconcile, then what are the issues preventing them from doing so? Are there other ways in which the two policy objectives can be reconciled?

4. *The reform of the EU restrictions question.* What are the weaknesses of the EU framework for transfers of personal data outside the EEA from the EU Charter perspective, and how can they be addressed in a manner both compliant with the EU Charter and conducive to international trade? Do restrictions on transfers of personal data outside the EEA constitute part of the essence of the fundamental right to privacy, to the protection of personal data and to an effective remedy?

Turning to methodological questions, for the most part, the research question calls for a doctrinal analysis of the law from an internal perspective.\(^{71}\) The main research question is evidently normative, asking how competing values and interests should be reconciled. The first normative basis will be the law, even if it will become evident that the law—as an expression of such competition—will not give away the answer.

The thesis thus engages first of all in an argument about what the law is, with a view towards developing it further.\(^ {72}\) This approach is necessary in order to inform the legal arguments in this thesis. First, it engages with the reform of the international trade exception for privacy and data protection in future EU trade agreements. And second, with the reform of the EU framework for transfers of personal data outside the EEA under the

---

\(^{71}\) Smits (2012), p. 3 (defining the doctrinal method as ‘approach, in which rules, principles and case law are considered from the internal perspective and in which law is looked at as being in a relatively autonomous relation to the social, economic and political reality’.)

GDPR in a manner respectful of EU fundamental rights. The doctrinal analysis systematises the legislation and jurisprudence of the CJEU and the WTO adjudicating bodies within the scholarly schemes established in secondary literature from the relevant legal domains, in particular, EU law, European data protection and international trade law. For example, Chapter 2 of the thesis uses close reading of the relevant legal provisions of the GATS and the GDPR, in the light of their interpretation in the CJEU and WTO jurisprudence and secondary literature, to analyse and compare the necessity tests in the EU Charter and in the general exception of trade agreements, modelled after Article XIV GATS. Chapter 4 deconstructs the text of the EU model clauses on cross-border data flows and examines each element of these clauses by comparing it to the existing legal provisions as interpreted in the relevant WTO jurisprudence and secondary literature. Chapter 5 applies the same methods, amplified by an emphasis on the existing legal practice, to evaluate the EU framework for transfers of personal data in the GDPR and to explicate the relationship between the EU Charter and the GDPR in the context of the governance of transfers of personal data outside the EEA.

In order to further support its normative argument, the thesis complements the classical doctrinal method by a historical approach to law, elements of economic analysis of law, and critical legal studies. The interplay between these methods plays a central role in the development of the arguments in Chapter 3, addressing the question of where to draw a line between protection and protectionism, and how the framing of the debate on trade and data privacy affects the degree of regulatory autonomy afforded to domestic privacy and data protection rules. Relying on the literature on economics and the political economy of international trade, Chapter 3 takes a historical perspective to trace how the notion of ‘protectionism’ has evolved over time. The discussion of the role of discourse in shaping the meaning of ‘protectionism’ is also informed by the literature on language and power, which falls under the umbrella term of ‘discourse analysis’. It then applies these insights to the current debate on whether, and to what extent, EU restrictions on transfers of personal data outside the EEA can be viewed as protectionist. The discussion of the dual nature of personal data in Chapter 3 requires a conceptual analysis of personal data, which contraposes its dignitary and economic aspects. An understanding of both the economic nature and life cycle of personal data rests on an external, essentially economic approach. Juxtaposing the legal and economic perspectives on the protection of personal data allows the thesis to put the tension between the two approaches in sharp contrast. This tension

75 Handler (2013).
76 Finnis (2011).
translates into conflicting goals and differing notions as to the right level of regulation, depending on whether personal data is protected as an economic asset or a fundamental right. This part of the discussion draws on the academic literature informed by a law and economics theory of regulation, which addresses regulation from an economic efficiency standpoint.\(^{77}\) By contrast, a discussion of the dignitary aspect is based on the academic literature embracing a moral and legal approach reflecting the value attached to personal data by international human rights and EU law.

There is a variety of international trade agreements that go a step further than the WTO agreements in regulating issues related to electronic commerce and data (WTO plus agreements).\(^{78}\) In analysing the governance of cross-border data flows, the thesis takes an EU perspective, which it juxtaposes with that of the US. For this reason, the scope of WTO plus agreements considered in this thesis is limited to the recent EU-led, already-concluded or draft trade agreements and proposals for trade agreements currently negotiated by the EU: JEFTA, draft Modernised EU-Mexico Free Trade Agreement (FTA), the EU’s proposals for FTAs with Australia, Indonesia, New Zealand, Tunisia and the UK. The above-mentioned proposals for trade agreements are relevant for the analysis in this thesis because they contain specific provisions on cross-border data flows. Bringing JEFTA and the draft EU-Mexico agreements into the discussion gives a historical perspective to the debate on cross-border data flows in the international trade realm. On the US side, the analysis in this thesis includes the already mentioned CPTPP, USMCA and the US-Japan Digital Trade Agreements, which are the only US-led trade agreements that contain a legally binding provision on cross-border data flows. The US model has been chosen as a point of comparison with the EU model, for the reason that it is currently the most influential model which is incorporated in currently concluded international trade agreements. For example, as mentioned above, the UK has adopted the US rather than the EU approach to cross-border data flows in Brexit negotiations with the EU. In the data protection realm, the issue of transfers of personal data from the EEA to the US has been one of the most contentious within the lifetime of the EU data protection framework. The focus on the EU-US relationship, however, does not diminish the fact that the balancing of economic, fundamental rights and other policy objectives in the governance of cross-border data flows is a global issue.

This thesis does not engage with the debate on the classification of goods and services when it comes to cross-border data flows.\(^{79}\) The focus of this thesis is on international agreements covering trade in services and electronic commerce, which is

\(^{77}\) Ogus (1994), pp. 23-54.
\(^{78}\) For a most recent overview of such provisions, see Burri, Polanco (2020).
\(^{79}\) For a discussion, see e.g. Sen (2018), p. 330-335.
referred to as digital trade in most recent trade agreements. The thesis does not cover trade in goods, even though in some cases, measures restricting data flows could be targeting ‘goods attributes’ of a product, such as an Internet of Things device.

It should also be acknowledged that approaching cross-border data flows from an international trade perspective, as adopted by this thesis, is only one way of looking at freedom of information flows more generally. In a broader context, restrictions on data flows implicate other policy objectives, such as freedom of speech, as well as (international) media and communications freedom, which, in a wider sense support political, social and economic activity. As Mueller and Grindal rightly observe, the economic value of data flows is a ‘by-product of the social, communicative and productive capability caused by untrammelled information flows’. ⁸⁰

1.3 Outline of the thesis

The Chapters of this thesis tackle in turn the research sub-questions posed above. Chapter 2 explicates the EU restrictions on transfers of personal data outside the EEA against the background of the concerns that led to the emergence of the EU data protection framework in the 1990s. It then demonstrates the possible tension between these restrictions and existing EU international trade commitments, especially under the GATS. The Chapter further argues that there is a risk that this tension cannot be ameliorated by the application of exceptions provided for in EU and trade law, due to the incompatibility of these exceptions when applied simultaneously. Put simply, Chapter 2 sets out the main issue addressed by this thesis: the conflict between commitments to data protection, and trade liberalisation.

Chapter 3 takes a step back and investigates whether EU restrictions on transfers of personal data outside the EEA are protectionist. One could argue that the balance between digital trade liberalisation and the protection of data privacy should simply be struck by ruling out measures that are protectionist in nature. The problem is, however, that the baseline between legitimate protection and protectionism does not exist. Chapter 3 investigates how views on this baseline are discursively constructed and how this baseline has shifted over time. The Chapter demonstrates how discourse affected the conceptualisation of the notion of ‘protectionism’ in international trade negotiations and WTO case law, and translates these findings into a number of recommendations for future international trade negotiations on digital trade and cross-border data flows. Chapter 3 also shows how discourse can affect the normative foundations of the public policy objectives incorporated into trade law exceptions, such as privacy and the protection of personal data,

⁸⁰ Mueller, Grindal (2019), p. 82.
and, as a result, the level of protection of such objectives in domestic legal systems.

Chapter 4 turns to the international trade law aspect of the problem identified in Chapter 2. It questions whether the model clauses on cross-border data flows and the protection of personal data tabled by the EU in all trade negotiations on these issues would allow the EU to resolve that problem whilst maintaining its trade policy objectives. Having identified the weaknesses of the model clauses, Chapter 4 looks for alternatives.

Chapter 5 examines the weaknesses of the EU framework for transfers of personal data outside the EEA from the EU Charter perspective and asks how this framework could be improved to ameliorate the problem identified in Chapter 2. It examines this framework through the lens of geopolitical, legal and economic changes, and the constitutional function of those rules in order to establish whether this framework is still fit for purpose or needs to be improved. Engaging with the idea of future reform, Chapter 5 addresses the relatively unexplored issue of the constitutional contours of EU secondary law framework for transfers of personal data. Relatedly, it explores the flexibility that the EU legislator has under the EU Charter to change the rules of the GDPR on transfers of personal data. It also provides three directions of thought on future reform, roughly corresponding to possible short, medium, and long term strategies for the EU.

Chapter 6 offers conclusions structured as responses to the research questions formulated above and envisions paths for further research.

Research in this thesis is up-to-date until 1 September 2020. After that only a small number of substantive additions and changes have been made. Some parts of this thesis are based on the author’s published work. In particular, Chapter 2 is based on S. Yakovleva, Personal Data Transfers in International Trade and EU Law: A Tale of Two ‘Necessities’, Journal of World Investment & Trade 21 (2020) 881–919; Chapter 3 is based on S. Yakovleva, Privacy Protection(ism): The Latest Wave of Trade Constraints on Regulatory Autonomy, University of Miami Law Review, 74 (2) (2020) 416-519. This thesis also cites individual and co-authored work that preceeded and paved the way to this thesis.
2. Personal data transfers in international trade and EU law: a tale of two ‘necessities’

2.1 Introduction

This Chapter identifies and sets out the key issue addressed in this thesis, namely that of increasing tension between the governance of cross-border transfers of personal data by EU and international trade law. It develops the argument that the EU restrictions on transfers of personal data could conflict with the EU’s commitments under the GATS and post-GATS trade agreements. It contends that such restrictions are unlikely to meet the trade necessity test even in its most lenient interpretation because they arguably go beyond the limits set by the GATS provisions and the general exception. An important contribution of the Chapter to this debate is that the requirement of free cross-border flow of personal data that can be deduced from the EU’s existing trade liberalisation commitments in the context of digitally provided services is not only inconsistent with the GDPR, but is also unlikely to be justified under Article 52(1) of the Charter as a necessary and proportionate derogation from the fundamental right to the protection of personal data. This analysis exposes the EU’s constitutional constraints on implementing such a requirement for the cross-border flow of personal data into the GDPR, which may lead to a catch-22 compliance deadlock for the EU. The Chapter then argues that adjustments of both international trade and EU data protection rules are necessary to overcome this deadlock.

The Chapter proceeds as follows. Section 2 offers a historical background and explains the EU restrictions on transfers of personal data outside the EEA. It then demonstrates a possible inconsistency between these rules and the EU commitments under the GATS. Section 3 juxtaposes the interpretation of the trade necessity test and the EU Charter necessity test and explains why there is a risk of a catch-22 type of compliance deadlock for the EU when the two necessity tests are applied simultaneously. Section 4 outlines ways out of the potential deadlock. Section 5 concludes.

2.2 EU data protection and international trade law

Restrictions on transfers of personal data outside the EEA have been characteristic of the EU data protection framework since its inception. Therefore this Section introduces these restrictions in a historical context, which allows for a deeper understanding of the concerns underlying them. It also explains the prevailing uncertainty surrounding the notion of ‘transfer’ in the EU data protection framework and its evolution over time. This Section then positions the EU restrictions on transfers of personal data against the EU commitments under the GATS and other trade agreements that require liberalisation of such transfers in the context of international trade in services.

2.2.1 The EU regime for transfers of personal data outside the EEA
2.2.1.1 Historical background

Rules governing cross-border transfers of personal data began to emerge in EU member states, alongside the first data protection laws in the 1970s, in response to the increasingly automated processing of personal data. While the first 1970 data protection law of the German federal state of Hessen did not contain any restrictions on transfers of personal data, the data protection laws of Austria, Norway, Sweden, Ireland and Finland, adopted shortly after, did include such restrictions. As classified by Kuner, these restrictions fell into one of the following three categories: (1) requiring an explicit authorisation by a Data Protection Authority (DPA); (2) incorporating provisions on data flows from Article 12 of the Council of Europe Convention 108 (Convention 108); and (3) requiring an individual’s consent or a similar level of protection in the country of destination. Different approaches across EU member states were evidenced not only at the level of regulation, but also at the level of enforcement. On a par with restrictions on the exporting of personal data, some domestic laws also regulated the importing of such data. The strictness of rules governing transfers of personal data at that time was, however, counterbalanced by the relatively small volume of personal data in the overall data flows, which mostly comprised of non-personal data.

Concerns that motivated the adoption of the rules on transfers of personal data, both in EU member states and in other countries, included not only the risk of the circumvention of domestic privacy and data protection rules, but also the risk that national, cultural and economic sovereignty could be undermined by personal data being processed abroad. Examples of risks tied into sovereignty concerns were: inability to administer justice; inability to execute legal judgments; and inability to apply certain national laws to foreign citizens.

---

82 Ibid., p. 27-28.
83 For example, Article 12 ‘Transborder flows of personal data and domestic law’ of the Convention 108 (prior to reform completed in 2018) stated that:
1. The following provisions shall apply to the transfer across national borders, by whatever medium, of personal data undergoing automatic processing or collected with a view to their being automatically processed.
2. A Party shall not, for the sole purpose of the protection of privacy, prohibit or subject to special authorisation transborder flows of personal data going to the territory of another Party.
3. Nevertheless, each Party shall be entitled to derogate from the provisions of paragraph 2:
a) insofar as its legislation includes specific regulations for certain categories of personal data or of automated personal data files, because of the nature of those data or those files, except where the regulations of the other Party provide an equivalent protection;
b) when the transfer is made from its territory to the territory of a non-Contracting State through the intermediary of the territory of another Party, in order to avoid such transfers resulting in circumvention of the legislation of the Party referred to at the beginning of this paragraph.
85 Ibid.
87 Ibid.
information dependency on other states; and political risks resulting from information flows being controlled from another country.\textsuperscript{89}

Increasing adoption of data protection laws across Europe, as well as on the international level, such as the Convention 108 and the OECD Guidelines,\textsuperscript{90} led to a fragmentation of data protection standards.\textsuperscript{91} Despite the recommendation from the European Commission, in an effort to contribute to an organic harmonisation of data protection laws across Europe – by the end of 1989 only seven EU member states ratified Convention 108.\textsuperscript{92} Against the backdrop of increasing cross-border data flows in the 1990s, the lack of a cohesive data protection landscape and the emerging enforcement actions restricting personal data flows between the EU member states (such as the so-called ‘FIAT’ case), prompted the need for harmonised European data protection rules.\textsuperscript{93} This need was given further impetus by the European Commission’s ambition to develop a data processing industry in Europe.\textsuperscript{94} These rules, ‘clearly intended to improve the functioning of the internal market’,\textsuperscript{95} were codified in 1995 in the form of the Data Protection Directive. The Data Protection Directive was based on the EU competence to regulate the internal market,\textsuperscript{96} although critics have described it as ‘a tool of neutralisation of national rights in favour of economic efficiency’.\textsuperscript{97}

It should, however, be noted that not only furthering the internal market, but also the protection of fundamental rights, were codified as equal objectives of the Directive.\textsuperscript{98} As the European Commission noted in its first review of the Data Protection Directive, this Directive ‘enshrined[d] two of the oldest ambitions of the European integration project: the achievement of an Internal Market (in this case the free movement of personal information) and the protection of fundamental rights and freedoms of individuals. In the Directive, both objectives are equally important’.\textsuperscript{99} Despite the latter statement, in practice fundamental rights were viewed – at that time and up until 2009 when the EU Charter became legally binding – as merely ‘derogat[ions] from internal market freedoms’.\textsuperscript{100} From the rights perspective, the assumption was that those rights will not be violated because the

\begin{itemize}
\item \textsuperscript{89} Kuner (2013), p. 29-30.
\item \textsuperscript{90} For example, in 1981, the Council of Europe adopted Convention 108, OECD adopted the 1980 Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.
\item \textsuperscript{92} Lylskey (2015), p. 48.
\item \textsuperscript{93} Ibid., p. 49; Kuner (2010), p. 19, Schwartz (2009), p. 11.
\item \textsuperscript{94} Lylskey (2015), p. 47.
\item \textsuperscript{95} Ibid., p. 49; González Fuster (2014), p. 134; van Hoboken (2014b).
\item \textsuperscript{96} Recitals 3, 5 and 8 Data Protection Directive. For a discussion, see Lylskey (2015), p. 47-50.
\item \textsuperscript{97} González Fuster (2014), p. 135.
\item \textsuperscript{98} Article 1 Data Protection Directive.
\item \textsuperscript{100} González Fuster (2014), p. 135. See also Petkova (2019), p. 148.
\end{itemize}
implementation of the Directive will lead to ‘equivalent’ levels of protection. In its early jurisprudence, the CJEU tended to prioritise market integration ahead of the fundamental rights limb of the Directive.

Moving forward to the twenty first century, the Lisbon Treaty, which took effect in 2009 and made the EU Charter legally binding for the EU, transformed the right to the protection of personal data into a *sui generis* binding fundamental right under Article 8 of the EU Charter, separate from the fundamental right to privacy enshrined in Article 7 of the Charter. It also granted the EU competence to legislate on the protection of personal data as a fundamental right. The EU later relied on this competence to adopt the GDPR. At the same time, just as its predecessor did, the GDPR also pursues the dual objective of safeguarding the fundamental rights, such as that to the protection of personal data, and ensuring the free flow of personal data within the internal market. Furthermore, the EU data protection reforms that led to the adoption of the GDPR were one of the pillars of the Digital Single Market project, presented by the European Commission as the key for making the European Union thrive in the emerging global data economy.

It should also be recalled that back in 2012, the process of drafting the GDPR and the revision of the Data Protection Directive was initiated with a promise to simplify and streamline the mechanisms for cross-border data transfers, and to create more interoperability with the data protection regimes of the EU’s strategic partners, including the US. Despite the ‘intense lobbying by and on behalf of US multinationals to limit what are characterized as unnecessarily restrictive rights for individuals’, the rules for transfers of personal data became even more stringent and only marginally more flexible.

The constitutionalisation of the fundamental rights to privacy and the protection of personal data eventually not only shifted the core normative rationale of protecting these rights within the EU from the predominantly economic goal of ensuring the free flow of personal data in the EU, to the protection of individual rights, but also altered the balance

103 Art. 16(1) of the TFEU.
104 Recitals 1 and 12 GDPR.
105 Art. 1 GDPR.
109 For a discussion of the changes to the EU framework on transfers of personal data outside the EEA introduced by the GDPR, see Section 5.1.
between economic and non-economic values in the EU’s external economic policy.\textsuperscript{110} As Pollicino and Bassini argue, ‘[w]hile at the very beginning of the European constitutionalism protection of fundamental rights [could] justify restrictions to the economic freedoms provided by the treaties, as exceptions to the same’, after the Lisbon Treaty, the level of protection of fundamental rights began ‘to determine the degree of openness of the European Union towards other orders’.\textsuperscript{111} Entrusted with the power to interpret the EU Charter, the CJEU has taken up the role of a guarantor of EU fundamental rights. It played an important role in building up jurisprudence on Articles 7 and 8 of the Charter as well as in the interpretation of the derogation clause of Article 52(1) of the EU Charter in relation to these rights. Some even argue that in the 2015 Opinion concerning the validity of the draft EU-Canada PNR Agreement (the \textit{Opinion on EU-Canada PNR Agreement}),\textsuperscript{112} the CJEU has used data protection ‘as a vehicle to assert EU fundamental rights in an international context’.\textsuperscript{113}

The shift of balance between economic and non-economic values is most apparent in a line of post-EU Charter CJEU jurisprudence. In contrast to its prior case law, the Court’s jurisprudence now prioritised the rights to privacy and data protection ahead of other rights, such as the freedom of expression and information (Article 11) and the freedom to conduct a business (Article 16), and conferred on them the status of ‘leading rights’ in Europe.\textsuperscript{114} As the CJEU noted in \textit{Google Spain}, ‘[i]n the light of the potential seriousness of that interference, it is clear that it cannot be justified by merely the economic interest which the operator of such an engine has in that processing’.\textsuperscript{115} One year before the EU Charter became binding, in the \textit{Satamedia} judgement\textsuperscript{116} the Court took an approach to balancing the right to the protection of personal data against the right to freedom of expression that ‘demonstrates that the protection of personal data weighs heavily relative to that part of freedom of expression which falls under “journalistic purposes.”’ In other words, the CJEU place[d] greater weight on the protection of personal data than on freedom of expression in this context’.\textsuperscript{117} Similarly, although in the \textit{Schrems I and II} cases, the CJEU did not explicitly address the underlying issue of balancing trade and privacy,

\begin{itemize}
    \item \textsuperscript{110} Under the TEU, as amended by the Treaty of Lisbon, negotiation and conclusion of international trade agreements must be guided by the universality and indivisibility of human rights and fundamental freedoms, respect for human dignity and principles of the United Nations and international law (Arts. 2(5) and 21 of the TEU).
    \item \textsuperscript{111} Pollicino, Bassini (2017), p. 262.
    \item \textsuperscript{112} CJEU, \textit{Opinion on EU-Canada PNR Agreement}.
    \item \textsuperscript{113} Kuner (2018), p. 858.
    \item \textsuperscript{114} Petkova (2019), p. 154; Petkova (2016), pp. 430-432. See also Irion (2016), p. 7 (noting that ‘the relative weight the CJEU accorded to the rights to privacy and data protection steadily expanded corresponding to the increasing significance of personal data processing and flows’.)
    \item \textsuperscript{115} CJEU, \textit{Google Spain}, para. 81, emphasis added.
    \item \textsuperscript{116} CJEU, \textit{Satamedia}, para. 56.
    \item \textsuperscript{117} Tranberg (2011), pp. 239–248.
\end{itemize}
Petkova argues that the Court did implicitly put the protection of fundamental rights to privacy and the protection of personal data above the commercial interests vested in transatlantic data flows. The higher importance of the fundamental rights to privacy and the protection of personal data, as compared to other fundamental rights, also reveals itself through the higher ‘strict necessity’ threshold for derogation from these fundamental rights under Article 52(1) of the EU Charter, as is discussed in Section 2.3.3 below. It is also reflected in the desired level of protection of the right to the protection of personal data – ‘effective and complete’ as pronounced by the CJEU. The requirement of ‘complete’ protection could make the balancing of this right with other competing fundamental rights challenging and leave suboptimal room for respecting those other rights. Although Lenaerts, the President of the CJEU, contended that ‘there is no hierarchy of qualified rights under the Charter’, in practice, the CJEU de facto tends to rank fundamental rights to privacy and data protection above other rights in the internal hierarchy of values.

In a broader perspective, EU law scholars link the European fundamental rights discourse to the growing demand for legitimacy following the expansion of the Union’s competences. To Muir, this discourse ‘tends to become a legitimating battle horse for the European Union’ and an increasingly ‘important part of the EU “political messianism.”’ The strengthening of the fundamental rights to privacy and the protection of personal data in the CJEU jurisprudence is, arguably, a part of this broader phenomenon and is liable to affect the balance of competences between the Union and its constituencies. For example, the broadening of the scope of EU privacy legislation in relation to foreign countries’ surveillance practices involving personal data transferred from the EEA by the CJEU in Schrems I and II, is likely to broaden the scope of EU Charter application to the EU member states’ surveillance activities, as Section 2.2 further elaborates. Furthermore, EU competence to legislate fundamental rights to privacy and the protection of personal data increasingly underlies EU ambitions in regulating technology through framing legal challenges, such as those posed by artificial intelligence (AI), as data protection issues. In this sense, despite the shift of EU competence underlying data protection legislation from internal market to fundamental rights, this legislation is still an important pillar of the European project. At the same time, asserting the EU values as

119 CJEU, Google Spain, para. 34; CJEU, Wirtschaftsakademie, para. 28; CJEU, CJEU, Jehovah todistajat, para. 66; CJEU, Fashion ID, paras. 66, 70.
121 Van Hoboken (2014a).
global is also a part of the EU’s political project of expanding the reach of EU law over internet-related issues globally. As Eckes notes, ‘in European law, constitutional law is the new internal market. Indeed, both in importance and in development, European constitutional law is today what the internal market was in the eighties and early nineties. 

In recent years, as mentioned in the Introduction, robust protection of the fundamental rights to privacy and protection of personal data has also become part of the EU’s ‘technological’ or ‘digital sovereignty’ narrative. Although these notions are not directly linked by the EU to the regulation of transfers of personal data outside the EEA in the present day EU policy discourse, they do resonate well with the concerns that led to the development of such regulation in EU member states back in 1970s and 80s.

2.2.1.2 The notion of transfer

Although the concept of ‘transfer’ is central in triggering the application of the restrictions on transfers of personal data, neither the GDPR nor its predecessor – the Data Protection Directive – define the concept of ‘transfer’ of personal data outside the EEA. Although the restrictions on transfers of personal data were in place for more than 20 years, there is still no clarity or specific guidance on what this concept means.

The CJEU specifically addressed this issue only once, in one of its earliest cases on data protection. In its 2003 *Lindqvist* judgement, the CJEU concluded that uploading materials onto an internet page, which can be consulted, and which is hosted by, a person established in a third country, thereby making that data accessible worldwide, does not constitute transfer of data to a third country in the meaning of Article 25 of the Data Protection Directive. The Court also noted that in these circumstances, it is irrelevant whether an individual from a third country has accessed the internet page. The CJEU based its reasoning on what Svantesson calls a ‘reasonableness test’. The Court explained that given that, first, the state of development of the internet at the time

---

130 The European Commission’s proposal for the GDPR also failed to define the term ‘transfer’. For a discussion and approaches to the notion of ‘transfer’ in other international frameworks on data flows, see Kuner (2013), p. 12.
131 CJEU, *Lindqvist*, para. 4 of the conclusions.
Protection Directive was drawn up and, second, the absence (in Chapter IV of the Directive governing transfers of personal data), of criteria applicable to use of the internet:

one cannot presume that the Community legislature intended the expression transfer [of data] to a third country to cover the loading, by an individual in Mrs Lindqvist's position, of data onto an internet page, even if those data are thereby made accessible to persons in third countries with the technical means to access them.\(^{134}\)

In other words, there is no 'transfer' in the meaning of the Data Protection Directive, whenever there is no 'direct transfer' of personal data between the person posting personal data on the server and the person accessing personal data.\(^{135}\) The Court further explained that if those rules were interpreted to mean that there is 'transfer [of data] to a third country' every time that personal data are loaded onto an internet page, that transfer would necessarily be a transfer to all the third countries where there are the technical means needed to access the internet. The special regime provided for by Chapter IV of the directive would thus necessarily become a regime of general application, as regards operations on the internet.\(^{136}\)

There are several reasons to treat this rather narrow interpretation of 'transfer' with caution and, instead, adopt a broader understanding of this notion, 17 years after the Lindqvist judgement. First, the judgement concerns a fact-specific, particular case and may not have a universal application to all cases of online data sharing. To illustrate the point, in explaining its position, the CJEU refers to the ‘action of a person in Mrs Lindqvist’s position’ and ‘actions such as those of Lindqvist’\(^{137}\). Adopting this line of thinking, Kuner argues that making personal data available online can be viewed as cross-border data transfer if it involves 'granting access to the data of other parties on a large scale for business purposes'.\(^{138}\) Second, unlike the Data Protection Directive, the GDPR was drafted in different economic circumstances, where data was increasingly labelled as ‘the new oil’,\(^{139}\) and cross-border data flows as the ‘hallmark of 21st-century globalization’.\(^{140}\)

\(^{134}\) CJEU, Lindqvist, para. 68.
\(^{136}\) CJEU, Lindqvist, para. 69.
\(^{137}\) See e.g. Dutch DPA Publication of Personal Data on the Internet, December 2007, section V, para. 5, p. 50.
\(^{138}\) Kuner (2007), p. 83. Factors that could be relevant in assessing the likelihood of data transfer rules being applicable, include the presence of an establishment of data controller in the country of the individual whose data is processed, the targeting of the individual by company’s activity, and the degree of control over the purposes or means used by the individual to process the data. Ibid., p. 15.
Therefore, one can no longer argue that the legislator could not foresee the application of the rules on transfers of personal data to pervasive transfers on the internet. Third, and most importantly, as already mentioned above, the GDPR was adopted on the basis of the EU competence to legislate on the fundamental right to the protection of personal data, rather than internal market competence, on which the Data Protection Directive was based.141 Analogous with the CJEU’s approach to a broad interpretation of the notions of ‘personal data’142 and ‘controller’ under the GDPR in a recent line of cases,143 is a broad interpretation of the notion of ‘transfer’ of personal data, which could be necessary to ensure ‘effective and complete’144 protection of fundamental rights.

Despite the fact that cross-border flows of personal and other data have become the backbone of present-day digital commerce, online social networks and cloud computing, the uncertainty as to the meaning of ‘transfer’ in the EU data protection framework remains.145 Based on the recent guidance of the European Data Protection Board (EDPB)146 and the CJEU judgement in Schrems II it is only clear that:

1) ‘granting direct access to a database (e.g. via an interface to an IT-application) on a general basis’ constitutes a transfer of personal data in the meaning of the GDPR,147 and

2) data in transit is equally subject to the rules on transfer of personal data outside the EEA under the GDPR.148

Based on the discussion above, this thesis takes the approach that - in the light of the constitutional role of the GDPR to ensure ‘effective and complete’ protection of personal

141 Lynskey criticises the qualification of Mrs. Lindqvist activities as falling under the scope of the Data Protection Directive in the first place, calling the judgement ‘integrationist’. Lynskey (2015), pp. 54-55. It could thus be argued, that a pragmatic approach of the Court to the scope of the rules on transfers of personal data was aimed at counterbalancing the broader scope of application of the Data Protection Directive.

142 CJEU, Nowak, para 34 (stating that)

[the use of the expression ‘any information’ in the definition of the concept of ‘personal data’, within Article 2(a) of Directive 95/46, reflects the aim of the EU legislature to assign a wide scope to that concept, which is not restricted to information that is sensitive or private, but potentially encompasses all kinds of information, not only objective but also subjective, in the form of opinions and assessments, provided that it ‘relates’ to the data subject]

143 CJEU, Google Spain, para. 34; CJEU, Wirtschaftsakademie, para. 28; CJEU, Fashion ID, paras. 50, 66.

144 CJEU, Google Spain, para. 34; CJEU, Wirtschaftsakademie, para. 28; CJEU, CJEU, Jehovan todistajat, para. 66; CJEU, Fashion ID, paras. 66, 70.


146 The European Data Protection Board is a consultative body comprising all EU member states’ data protection authorities. EUROPEAN DATA PROTECTION BOARD, About EDPB, https://edpb.europa.eu/about-edpb_en


148 CJEU, Schrems II, paras. 183-185. See also Kuner (2013), p. 176, agreeing with such approach, but proposing to take the fact that data are merely in transit in the analysis of risk of harm to individuals.
and the increasing prominence of the fundamental rights to privacy and the protection of personal data in CJEU case law, in border-line cases the term ‘transfer’ should be understood broadly. Therefore, for the purposes of this thesis, collection of personal data by a data controller that does not have an establishment in the EEA, from individuals located in the EEA, especially where such individuals are specifically targeted by those controllers, is also considered a ‘transfer’ of personal data outside the EEA under the GDPR. This approach does create an overlap between the rules on transfer of personal data outside the EEA under the GDPR and extraterritorial application of the GDPR framework under Article 3(2) of the GDPR. The problem of this overlap is recognised, but not yet resolved, by the European Commission and the EDPB. Article 3(2) of the GDPR (which extends the scope of the GDPR to the controllers and processors who process personal data related to the offering of goods or services to individuals in the EU or monitoring of their behaviour within the EU) triggers the application of the whole GDPR, which should also include the rules of Chapter V. In addition, a narrow understanding of ‘transfer’ as not including the situations where personal data is collected by entities located outside the EEA would allow multinational companies to structure their data flows in a way that avoids the application of GDPR’s Chapter V altogether. This would be problematic, because unlike Article 3(2) of the GDPR, the rules of Chapter V governing systematic transfers of personal data outside the EEA ‘export’ more than just the GDPR framework. As the following Section explains, the ‘essential equivalence’ standard requires that foreign recipients of personal data must also provide the effective protection of such personal data from access by foreign surveillance

---

149 CJEU, Google Spain, para. 34; CJEU, Wirtschaftsakademie, para. 28; CJEU, CJEU, Jehovan todistajat, para. 66; CJEU, Fashion ID, paras. 66, 70.
150 For a discussion, see the following Section.
151 An argument to the contrary could, however, be based on the EDPB’s guidance and the Standard Contractual Clauses approved by the European Commission. Both the guidance and the Standard Contractual Clauses use the terms ‘data exporter,’ ‘data importer’ and the ‘data subject’. This suggests that a ‘transfer’ in the meaning of the GDPR is always a transfer from a controller or processor in the EEA (‘data exporter’) to a controller or processor outside the EEA (‘data importer’). Therefore, the collection by a controller or processor located outside the EEA of personal data directly from a data subject (as data subject is never considered to be controller or processor of their own personal data) in the EEA does not constitute a ‘transfer’ in the meaning of the GDPR. See, e.g., EDPB, Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, 25 May 2018; Standard contractual clauses (Set I) for controller to controller transfers.
152 The question on the relationship between GDPR Chapter V rules on transfers of personal data and extraterritorial application of the GDPR under Art. 3(2) GDPR remains an open question. See Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), 16 November 2018, version 1.0, for publication consultation; the mentioning of this issue was removed from the version of the guidelines adopted after public consultation; Communication from the Commission, Data Protection Rules as a Pillar of Citizens Empowerment and EUs Approach to Digital Transition - Two Years of Application of the General Data Protection Regulation, COM(2020) 264 final, 24 June 2020, p. 12, calling on the EDPB to clarify ‘the interplay between the rules on international data transfers (Chapter V) with the GDPR territorial scope of application (Article 3)’.
2.2.1.3 Restrictions on transfers

The EU legal framework for personal data protection includes two sets of rules: substantive rules regulating access to, and processing of, any personal data; and the rules governing transfers of personal data outside the EEA. When it comes to the latter, the EU’s current framework is one of the most restrictive in place in any democratic jurisdiction. The EU ‘border control approach’ to transfers of personal data is often contrasted to the United States ‘open skies’ policy on this issue. Regulation of cross-border data flows gives EU domestic data protection rules an international dimension. The EU framework governing transfers of personal data outside the EEA is based on a ‘prohibition with derogations’ principle. Under the GDPR, transfers of personal data to a country or territory outside the EEA or to an international organisation may only occur if the conditions of Chapter V of the GDPR are met.

The EDPB advocates a layered approach to cross-border transfers of personal data outside the EEA. The distinction is also made between systematic, as opposed to occasional and non-repetitive transfers. Transfers of personal data can occur without restrictions only if the destination country, territory, or international organisation ensures an ‘adequate’ level of personal data protection. First introduced by the 1995 Data Protection Directive, the adequacy mechanism predates the EU Charter. But, in the 2015

---

153 This interpretation, however, as explained in Section 2.2.2 may lead to discrimination between EEA and non-EEA service providers, which could violate the most-favoured nation principle under trade law. When collecting personal data necessary for the provision of services in the EEA, non-EEA providers have to comply with all GDPR rules plus Chapter V (which limits the possibilities for collection of such data), while EEA providers do not have to comply with Chapter V if they operate locally in the EEA. It could, therefore, be argued, that the doctrine of parallel interpretation requires that the ‘transfer’ should be interpreted narrowly and not include the initial cross-border collection of personal data from data subjects in the EEA by foreign providers. Under the doctrine of parallel interpretation, if a (trade) agreement contradicts the EU secondary law, the preference will be given to the meaning of the secondary law that is more consistent with the provisions of the agreement. See e.g. CJEU, Commission / Germany, para. 52.
154 Ferracane, van der Marel, (2018b) (‘We identify two main categories of data policies. The first category covers those policies that impact the cross-border transfer of data whilst the second category covers policies that apply to the use of data domestically.’
155 Svantesson (2011), p. 184 (‘The relatively strict border control scheme introduced through this has had a significant impact in other countries striving towards meeting the privacy standard set by the EU’); see also LeSieur (2012), pp. 101, 103–04; Schwartz, Peifer (2017), p. 135 (stating that ‘[u]nlike EU law, U.S. law starts with a principle of free information flow and permits the processing of any personal data unless a law limits this action’.)
156 See LeSieur (2012), p. 93.
157 Art. 44 GDPR.
158 EDPB, Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, 25 May 2018, pp. 3,12,14. Kuner, however, argues that the CJEU’s Schrems II decision may be undermining this layered approach. Kuner (2020b).
160 Art. 45 GDPR.
Schrems I judgement, the CJEU retroactively gave it constitutional meaning.161 ‘Adequate’, as interpreted by the CJEU, means ‘essentially equivalent’ to the level of protection of fundamental rights and freedoms guaranteed by the EU Charter.162 The European Commission unilaterally evaluates the adequacy of the data protection regime of a country, territory, or international organisation on a case-by-case basis, taking into account its legal and administrative mechanisms of personal data protection.163 If the Commission’s assessment results in a positive finding, it issues a legally binding ‘adequacy decision’.164

Currently, only 12 countries have a valid adequacy decision,165 including the mutual adequacy arrangement with Japan.166 An adequacy decision for the US, the so-called EU-US Privacy Shield framework, was invalidated by the 2020 CJEU judgement in Schrems II. The CJEU has concluded that the Privacy Shield does not ensure 'essentially equivalent' levels of protection for personal data transferred to the US, because it cannot remedy the absence of (1) necessary limitations and safeguards in US law with regard to the interferences caused by access to personal data by US surveillance authorities in the national security context, and (2) effective judicial protection against such interferences.167 The Schrems II judgement has confirmed the CJEU’s conclusions in 2015’s Schrems I, which invalidated the Privacy Shield’s predecessor – the EU-US Safe Harbor. Both Schrems I and II judgements embody European discontent with the US foreign surveillance practices168 exposed by Edward Snowden’s revelations. Awareness of the risks of US mass surveillance to Europeans’ privacy has put the rules concerning foreign governments’ access to EU individuals’ data, for national security or law enforcement purposes, in the spotlight of adequacy assessment of a foreign country’s data protection framework.

None of the adequacy assessments has yet resulted in a decision finding that the protection of personal data in a third country is not adequate. In the past, if the Commission

161 For a discussion, see Section 5.2.
162 See, e.g., CJEU, Schrems I, para. 73; CJEU, Schrems II, para. 94.
163 For a list of criteria for assessment, see Art. 45(2) GDPR.
164 ‘Adequacy decisions’ are adopted as Commission implementing acts based on Art. 288 TFEU.
167 CJEU, Schrems II, paras. 168-197. For further discussion, see Section 5.3.1.
168 See Kuner (2015a), p. 2092 (The transfer of national borders to the online space reflects society’s ambivalence about the benefits and drawbacks of globalization: on the one hand we have grown accustomed to the global availability of goods and services, but on the other hand we are unsettled by the breakdown of barriers that seems to threaten our national and regional identities. The Snowden revelations and other recent developments have increased the pace and intensity of these anxieties, but the deep-seated nature of these concerns shows the importance of developing an underlying normative framework to address them.)
was not able to certify the adequacy of personal data protection in the country under assessment, such assessment did not result in any decision at all. This was, for example, the case with the adequacy assessment for Australia.\textsuperscript{169} In 2017, the European Commission started the review of all adequacy decisions that were in force at that time.\textsuperscript{170} The 2019 adequacy decision for Japan appears to be under review at the moment of writing.\textsuperscript{171} The European Commission is currently conducting an adequacy assessment for South Korea;\textsuperscript{172} for the UK following Brexit,\textsuperscript{173} and is actively exploring the possibility of adequacy assessments of the EU’s important trading partners in Asia, Africa and Latin America.\textsuperscript{174}

Transfers of personal data to countries, territories, or international organisations that have not been granted an adequacy decision, can only lawfully occur subject to ‘appropriate safeguards’, named in Article 46 of the GDPR, and put in place by the data controller or processor transferring personal data.\textsuperscript{175} The most commonly used appropriate safeguards include:

- Standard data protection clauses, also known as standard contractual clauses (SCCs), either adopted by the European Commission\textsuperscript{176} or adopted by a DPA of an EU member state and approved by the Commission,\textsuperscript{177} and
- Binding corporate rules (BCRs), approved by competent DPAs, for multinational companies or companies conducting joint economic activity.\textsuperscript{178}

As compared to the Data Protection Directive, the GDPR also introduced two new appropriate safeguards for transfers of personal data, which are not yet operational at the time of writing: approved industry codes of conduct\textsuperscript{179} and certification mechanisms.\textsuperscript{180}

\textsuperscript{170} Stupp (2017).
\textsuperscript{171} Agenda of the 40th EDPB meeting, 20 October 2020, mentioning the Review of the Adequacy Decision of Japan.
\textsuperscript{173} Stolton (2020); Christakis (2020). An adequacy decision for the UK following Brexit could be problematic following the CJEU Schrems II decision. See, e.g., Docksey, Kuner (2020).
\textsuperscript{175} Arts. 46–47 GDPR.
\textsuperscript{177} Art. 46(2)(d) GDPR.
\textsuperscript{178} Arts. 46(2)(b), GDPR.
\textsuperscript{179} Arts. 46(2)(e), 40 GDPR.
\textsuperscript{180} Arts. 40(2), 42(2), 46 GDPR.
when complemented with binding and enforceable commitments by the controller or
processor in the third country to apply the appropriate safeguards, including those in
respect of the data subjects’ rights.

In practice, until recently, SCCs were the most widely used mechanism for
systematic transfers of personal data to countries without an adequacy decision.\(^{181}\) This,
however, is likely to change following the CJEU \textit{Schrems II} judgement. Part of the
questions referred for a preliminary ruling to the CJEU in this case concerned the validity
of the SCCs approved by the European Commission in the light of the EU Charter.\(^{182}\)
Although the CJEU has concluded that the SCCs are valid in the light of the EU Charter,
the Court explained that, in practice, the use of the SCCs is only allowed if they yield a
standard of protection for the transferred personal data ‘essentially equivalent’ to that in
the EU.\(^{183}\) If this is not the case, data exporters must put in place supplementary measures
to remedy the lack of essential equivalence of personal data protection or, alternatively,
suspend or stop transferring personal data.\(^{184}\) The DPAs are obliged to proactively monitor
the use of SCCs for the purposes of transfers of personal data, and must suspend or prohibit
personal data transfers when data exporters fail to implement necessary additional
measures.\(^{185}\) This requirement, especially in the absence of any concrete guidance on what
the additional measures could be,\(^{186}\) makes the use of SCCs problematic for transfers of
personal data outside the EEA, especially to non-democratic countries. The same
requirements are also likely to apply to other appropriate safeguards under Article 46
GDPR.\(^{187}\)

Appropriate safeguards, such as the SCCs and the BCRs are applicable when a
foreign recipient of personal data receives or obtains personal data from an establishment
in the EEA. As a result, foreign companies that collect the personal data of Europeans via
the internet and do not have a local establishment or business partner (for example, mobile
app providers), may only rely on the codes of conduct and certification, none of which

\(^{181}\) IAPP-EY (2019), p. 110 (showing that in 2019 (i.e. prior to the CJEU \textit{Schrems II} judgement) 88\% of
personal data transfers from the EU to the US are based on the SCCs.)
\(^{182}\) CJEU, \textit{Schrems II}, paras. 122-149.
\(^{183}\) CJEU, \textit{Schrems II}, paras. 96, 99, 100, 133-137, 142; Kuner (2020d).
\(^{184}\) For a more detailed summary of the CJEU’s conclusions regarding the SCCs, see Chapter 5 section [x].
\(^{185}\) CJEU, \textit{Schrems II}, paras. 108, 121.
\(^{186}\) At the time of writing, the EDPB has created a task force to work on those guidelines. EDPB, Press
Release, Thirty-seventh Plenary session: Guidelines controller-processor, Guidelines targeting social media
users, taskforce complaints CJEU Schrems II judgement, taskforce supplementary measures, 4 September
2020.
\(^{187}\) EDPB, Frequently Asked Questions on the judgment of the Court of Justice of the European Union in
Case C-311/18 - Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems, 23 July
2020, question 7.
appear to be currently operational.\textsuperscript{188}

If it is not reasonably possible for a company to adopt any of the appropriate safeguards under Article 46 GDPR, a data controller or processor may rely on the specific derogations contained in Article 49 GDPR, which include the explicit consent of a data subject, necessity of transfer for the conclusion or performance of a contract, or necessity for the establishment, exercise or defence of legal claims. Unlike the adequacy mechanism and appropriate safeguards, however, these derogations – in accordance with the EDPB guidance – are only suitable for ‘occasional’ or ‘non-repetitive’ transfers, and cannot be relied upon for the purposes of regular and systematic transfers.\textsuperscript{189} The layered approach adopted in such guidance requires that before using these derogations, data exporters should first ‘endeavour possibilities to frame the transfer’ with one of the adequate safeguards.\textsuperscript{190} Derogations are the only legal grounds that companies from the so-called ‘non-adequate’ countries that have no presence or business partner in the EEA, can use for cross-border collection of personal data in the absence of the codes of conduct or certification. Given that the EDPB guidance is not legally binding, the restrictive interpretation of the derogations’ scope of application could be challenged in courts following the \textit{Schrems II} judgement. In the new circumstances, specific derogations are the only legal mechanisms many companies can rely on for transferring personal data to the US and other countries that have not been afforded adequacy by the EU.

\subsection*{2.2.2 Compatibility of the EU regime for data transfer with international trade law}

Shortly after the EU data protection framework was introduced in 1995, several commentators flagged the potential inconsistency of the rules for transfers of personal data with the EU’s commitments under the GATS, such as most-favoured nation (MFN) treatment, national treatment and market access, and cannot be justified under the Article XIV GATS general exception.\textsuperscript{191} The EU is bound by these commitments not only under

\begin{itemize}
\item \textsuperscript{188} At the time of writing, the author is not aware of any approved codes of conducts or certification mechanisms serving as appropriate safeguards for international transfers of personal data. The EDPB has, however, adopted some of the necessary guidance on the certification mechanisms. EDPB, Guidelines 1/2018 on certification and identifying certification criteria in accordance with arts 42 and 43 of the Regulation, including Annex 2, 4 June 2019. See also Chiavetta (2018). EDPB has not yet adopted guidance on the codes of conduct as a tool for transfers of personal data outside the EEA.
\item \textsuperscript{189} EDPB, Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, 25 May 2018, p. 4.
\item \textsuperscript{190} Ibid., p. 4.
\item \textsuperscript{191} Swire, Litan (1988), pp. 188-196; Reidenberg (2001), pp. 736-737; Bergkamp (2002), pp. 39-40. On the contrary, Shaffer argued that a hypothetical US claim regarding WTO inconsistency of EU’s framework for personal data transfers ‘would likely not prevail’. Shaffer (2000), pp. 46-51. Asinari admits that EU regime for transfers of personal data may violate the EU’s WTO commitments, but concludes that the violation can be justified under the general exception. Asinari (2002), p. 277. It should however be noted that Asinari’s article predates the WTO’s interpretation of the necessity test in most recent WTO case law as well as the CJEU’s case law on privacy and data protection as fundamental rights. Meddin also argues that
\end{itemize}
the GATS,192 but also under virtually all the EU’s post-GATS bilateral or plurilateral trade agreements.193 Such warnings have intensified over time194 under the influence of several factors: the increasing importance of international transfers of personal data for digital trade; the above-mentioned Edward Snowden’s revelations; the challenge to the validity of the SCCs and the Privacy Shield at the CJEU, which resulted in higher standards for the former and invalidation of the latter;195 the adoption of the GDPR in 2016 (which introduced a stricter enforcement regime); and the recurring pressure to include cross-border data flow provisions in trade agreements, such as TTIP and TiSA.196

Although the GDPR only marginally changed the framework for personal data transfers compared to the 1995 Data Protection Directive, it significantly raised the stakes of violating these rules by introducing harsh penalties, which include a fine of up to 4 % of the total worldwide annual turnover of an undertaking for the preceding financial year.197 Under certain circumstances, this fine could be based not just on the turnover of a business unit that has violated the rules, but instead on the turnover of a multinational entity as a whole.198 Higher stakes for violating the rules on transfers of personal data outside the EEA increase the risks of a collision between international trade law and the EU’s data protection framework. Although the GATS does not specifically regulate cross-border flows of (personal) data, such flows may still be captured by obligations under the GATS applicable to trade in services from one WTO member into the territory of another WTO member (‘mode of supply 1’)199 when data transfers enable cross-border provision of such services.200

Some authors have rightly argued that differences in the treatment by the EU of

---

192 Arts. II, VI and VII of the GATS.
193 Such obligations are part of the most EU’s international trade agreements, the most recent examples being Arts. 9.3, 9.5 and 9.6 CETA, Arts. 8.5, 8.6 of the EU-Singapore FTA, Arts. 8.15-8.17 of the JEFTA.
194 See, e.g., Reyes (2011), pp. 24-26; Keller (2011); Weber (2012); Weber, Staiger (2017), pp. 58-59; MacDonald, Streatfeild (2014); Yakovleva, Irion (2016); Sen (2018); Coldicutt, Sen; Mattoo, Meltzer (2018). In contrast, acknowledging that the EU adequacy assessment may violate the EU’s WTO commitments, Chen envisions the possibility of such violation being justified under art XIV(c)(ii) GATS.
195 CJEU, Schrems II; Manancourt (2020).
197 Art. 83(5) GDPR.
198 Article 29 Working Party, Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679, WP253, 3 October 2017, p. 6; CJEU, Höflner and Elser, para. 21; CJEU, Confederación Española, para. 40; CJEU, Akzo Nobel and others, para. 60; CJEU, Elf Aquitaine, para. 56; CJEU, ICI / Commission, paras. 125-146.
199 Art. I(2)(a) GATS.
services and service providers from countries that have, and those from countries that do not have an adequacy decision, may amount to a violation of the MFN principle. Indeed, even the ‘Article 29 Working Party’ noted in one of its early opinions that ‘some third countries might come to see the absence of a finding that they provided adequate protection as politically provocative or at least discriminatory’. Moreover, restrictive rules for transfers to countries that have not been afforded an adequacy decision have been characterised as discrimination between foreign service providers, especially those who do not have an establishment or business partner in the EEA; and providers from the EEA, thus constituting another potential violation of the GATS, namely the national treatment obligation. For example, if ‘transfer’ of personal data in the GDPR’s Chapter V is to be understood broadly and include the collection of personal data in the EEA by foreign service providers, as discussed in section 2.2.1.2 above, then unlike EEA providers, those providers face stricter requirements for the collection of personal data as compared to their domestic counterparts. In particular, such providers cannot use legitimate business interest as a lawful ground for collecting Europeans’ personal data. While legitimate interest is mentioned as one of the lawful grounds for processing personal data in Article 6(1)(f) GDPR, it does not constitute a lawful ground for a transfer of personal data outside the EEA under Chapter V of the GDPR. The European Commission attempted to remedy this issue by including legitimate interest pursued by the controller or processor, as one of the specific derogations for occasional and non-repetitive transfers in its proposal for the GDPR. However, this provision was later removed during negotiations at the European Parliament. Instead, Article 49 GDPR provides a possibility to rely on 'compelling legitimate interest', which can only be done to a very limited extent. Similarly, the standard

---


202 Article 29 Working Party (full name: ‘The Working Party on the Protection of Individuals with regard to the Processing of Personal Data’) was an advisory body formed under Article 29 of the Data Protection Directive. It consisted of a representative from the data protection authority of each EU Member State, the European Data Protection Supervisor and the European Commission. Article 29 Working Party was replaced by the European Data Protection Board on 25 May 2018, when the GDPR entered into force.


204 See, e.g., Coldicutt, Sen; Yakovleva, Irion (2016), p. 204.

205 Art. 44(1)(g) of the Commission’s initial Proposal for the GDPR (which corresponds to Article 49 of the adopted version of the GDPR) contained the following text: the transfer is necessary for the purposes of the legitimate interests pursued by the controller or the processor, which cannot be qualified as frequent or massive, and where the controller or processor has assessed all the circumstances surrounding the data transfer operation or the set of data transfer operations and based on this assessment adduced appropriate safeguards with respect to the protection of personal data, where necessary.

Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), /* COM/2012/011 final - 2012/0011 (COD).

206 See Lysnkey (2015), p. 44.
for individual’s consent, as a ground for a cross-border transfer of personal data (namely, explicit consent in Article 49(1)(a)) is higher than the equivalent standard in Article 6(1)(a) GDPR mentioning consent as a lawful ground for personal data processing.

The 2020 Schrems II judgement further intensifies the tension between the international trade and EU law frameworks governing transfers of personal data. The central role that access to Europeans’ personal data by foreign authorities in the national security context plays in the CJEU’s assessment of ‘essential equivalence’ of a third country’s legal framework has intensified claims of a double-standard for personal data flows within the EEA and outside the EEA.207 As Article 29 Working Party and academics explain, unlike foreign surveillance programmes, such programmes run by the EU member states are generally not subject to EU law, and specifically the EU Charter.208 The reason for this is that under Article 4(2) of the Treaty on European Union national security is excluded from the EU competence and ‘remains the sole responsibility of each member state’.209 As a result, one could argue that by requiring foreign countries to meet the high EU Charter standards for the protection of the fundamental rights to privacy and personal data that the EU’s own constituencies are not subject to, the CJEU has adopted a measure210 violating the GATS national treatment principle. For example, it has been argued that in some EU member states (for example, Germany, France, the Netherlands, Sweden and the UK), privacy safeguards in the national security context are equally suboptimal or even weaker than those in the US, which have repeatedly been deemed inadequate by the CJEU.211 Although all EU member states are also members of the Council of Europe, and

207 See, e.g., Chander (2020), pp. 8-11; Swire (2016); Roth (2017), p. 65; Baker (2020); Swire (2020); Irion (2020).
208 Irion (2020); Article 29 Working Party, Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes, WP 215, 10 April 2014, pp. 6-7. See also Buchta, Kranenborg (2020), p. 105 (arguing that [a]s follows from article 2 TEU the Union is founded on the values of respect for the rule of law and for human rights. As the CJEU has stated in the Opinion on the accession of the EU to the ECHR, the Union is based on the fundamental premise that each Member State shares with all the other Member States a set of common values which implies and justifies the existence of mutual trust between the Member States that those values will be recognised. Against this background it is justified to leave certain matters to the Member State without further assessment, while for third countries a further assessment as regards those values still remains necessary.)
209 Art. 4(2) TEU states that:
The Union shall respect the equality of Member States before the Treaties as well as their national identities, inherent in their fundamental structures, political and constitutional, inclusive of regional and local self-government. It shall respect their essential State functions, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security. In particular, national security remains the sole responsibility of each Member State. (emphasis added)
210 It is established WTO case law that the notion of ‘measure’ is not restricted by requirement to form, and therefore, can also reflected in judicial decisions. See, e.g., WTO, Panel Report, Saudi Arabia – Protection of IPR, para. 7.49; WTO, Appellate Body Report, US – Shrimp, para. 173; WTO, Appellate Body Report, US – Gasoline, p. 28.
are therefore, subject to the requirements of Article 8 of the European Convention on Human Rights (ECHR), it is generally agreed that – in view of the current CJEU and the European Court of Human Rights (ECtHR) case law – the standard of the EU Charter in relation to surveillance laws and measures is higher than that of the ECHR.\textsuperscript{212}

In the light of the recent CJEU judgement in four cases, including Privacy International, the above-mentioned argument on the violation of national treatment cannot be made successfully.\textsuperscript{213} From the Advocate General’s Opinions in these cases, it follows that the fundamental rights standards developed by the CJEU in a line of cases concerning access to data transmitted by the telecommunications providers\textsuperscript{214} equally apply to EU member states legislation governing access to such data in the national security context\textsuperscript{215}. These standards, however, do not apply when national security authorities ‘exercise that competence directly, using their own resources’ without cooperation of private parties.\textsuperscript{216} The CJEU followed the Advocate General’s opinion and thus reinstated the equal treatment of EU member states and foreign countries following the two Schrems judgements.\textsuperscript{217}

Furthermore, in a recent publication, Buchta and Kranenborg also suggest a way to interpret Article 4(2) TEU in a way that ‘matters relating to national identities and essential State functions are not as such excluded from the scope of Union law but must be taken into account in the application of Union law.’\textsuperscript{218}

As already noted above, the CJEU’s Schrems II judgement may have implications beyond the EU-US Privacy Shield and the SCCs directly addressed by the judgement. Rather, as several scholars argue, the ‘practical response’ to the restrictions introduced by Schrems II is data localisation.\textsuperscript{219} This is exactly what one of the German DPAs recommended companies storing personal data in the US to do.\textsuperscript{220} The DPA also raised similar concerns regarding transfers of personal data to China, India and Russia.\textsuperscript{221} Depending on how restrictive on data flows supplementary measures will be, in the future EDPB guidance, the EU framework may become at risk of violating market access

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{212} Opinion AG in Schrems II, para. 251. Christakis (2018); Irion (2020). An important decision is, however, pending at the Grand Chamber of the ECtHR, which could change the situation. ECtHR, Big Brother Watch and others v. United Kingdom.
\item \textsuperscript{213} CJEU, Privacy International; CJEU, La Quadrature du Net and Others. For a discussion, see, e.g., Cameron (2020).
\item \textsuperscript{214} CJEU, Tele2 Sverige; CJEU, Digital Rights Ireland.
\item \textsuperscript{215} See, e.g., CJEU, Privacy International, para. 84. See also Opinions AG in Privacy International and others.
\item \textsuperscript{216} Ibid.
\item \textsuperscript{217} CJEU, Privacy International, para. 49.
\item \textsuperscript{218} Buchta, Kranenborg (2020), pp. 100-103.
\item \textsuperscript{220} Berliner Beauftragte für Datenschutz und Informationsfreiheit, Pressemitteilung: Nach ‘Schrems II’: Europa braucht digitale Eigenständigkeit, 17 July 2020.
\item \textsuperscript{221} Ibid.
\end{itemize}
\end{footnotesize}
commitments in data processing and database services, where transfers of data are essential for the production and delivery of services.  

2.3 Two necessities: a catch-22 for the EU

2.3.1. Framing the Issue

This Section illuminates the clash between EU law and international trade law regulating trade in services, when it comes to the regulatory framework that both bodies of law require for cross-border transfers of personal data.

In trade agreements, one of the primary mechanisms to accommodate the EU’s autonomy to adopt and maintain regulation inconsistent with its international trade commitments are the so-called general exceptions. The part of the general exception of GATS Article XIV(c)(ii) that is specifically relevant for privacy and data protection reads as follows:

Subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on trade in services, nothing in this Agreement shall be construed to prevent the adoption or enforcement by any Member of measures …

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

(ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts …

Section 3.2 below argues that the trade necessity test – the core of the general exception – could be too narrow to accommodate the EU’s autonomy to maintain the GDPR framework for transfers of personal data. As a result, the EU may be required under the GATS to adjust the rules on cross-border transfers of personal data and, potentially, to abandon the adequacy approach.

From an EU law perspective, entering into a new international trade agreement or complying with an existing one that limits any of the fundamental rights under EU Charter is a derogation from the rights under the EU Charter and thus is subject to its Article 52(1). According to this provision,

[a]ny limitation on the exercise of the rights and freedoms recognised by this

Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others. (emphasis added)

‘General interest recognised by the Union’, according to the Explanations to the Charter covers, in particular, objectives of the Union in its external relations mentioned in Article 3 of the TEU, which include free and fair trade.223 As the CJEU has explained, the derogation clause applies equally to both internal and external legislative acts of the EU, such as international agreements.224 Affirming the supremacy of the EU Charter over the EU’s international agreements, the CJEU confirmed that the EU may neither conclude nor implement through an EU legislative act, any international agreement (or decision of an international adjudicating body based on this agreement) if the conditions laid out in this derogation clause, namely the proportionality and necessity tests (that is, the ‘EU Charter “necessity test”’) are not fulfilled. 225 This conclusion echoes Article 207(3)(2) of the TFEU, imposing a responsibility on the Council and the European Commission to ensure ‘that the agreements negotiated are compatible with internal Union policies and rules’. Then, Article 218(11) TFEU provides a mechanism to ensure that an international trade agreement is compatible with the EU’s constitutional framework before it is concluded by the EU. It allows an EU member state, the European Parliament, the Council or the European Commission to request an opinion from the CJEU regarding the compatibility of a proposed international agreement with the EU Treaties, including the EU Charter. If the CJEU decides that such an agreement is incompatible with the Treaties, the international agreement cannot take effect until, and unless, it is brought in compliance with the Treaties. This provision was used at the request of the European Parliament concerning the EU-Canada agreement on the transfer and processing of Passenger Name Record data,226 which, among other things, mandated transfers of Europeans’ personal data to Canada. In this landmark ruling, having tested these provisions against the requirements of the derogation clause, including the EU Charter necessity test, the CJEU held that the agreement could not be concluded unless revised.227

It is now settled case law at the CJEU that international agreements entered into by the EU must be ‘entirely compatible with the Treaties and with the constitutional principles

223 Explanation on Article 52, Explanations Relating to the Charter of Fundamental Rights, 2007 O.J. (C 303), Art. 3(5) TEU.
224 CJEU, Opinion on EU-Canada PNR Agreement, para. 146.
226 CJEU, Opinion on EU-Canada PNR Agreement.
227 Ibid., paras. 232(2)-232(3).
stemming therefrom’. In particular, such agreements must be compatible with the right to privacy and the right to the protection of personal data. This is crucial to the analysis in this thesis because, if the EU framework for personal data transfers was deemed inconsistent with a trade agreement – for example, for failing to meet the requirements of the trade necessity test contained in the general exception – and the EU was required to bring its laws into conformity with the trade agreement, compliance with the decision of a trade adjudicating body establishing such inconsistency would be a derogation from the fundamental rights codified by Articles 7 and 8 of the EU Charter. It follows from the CJEU’s jurisprudence, however, that before such a decision of an international trade adjudicating body could be implemented, compliance would have to be tested under the requirements of Article 52(1) of the EU Charter. Yet, trade law’s necessity test, when viewed as a derogation from the EU’s fundamental right to privacy and the protection of personal data, is unlikely to meet the EU Charter necessity test. Put another way, the trade necessity test obligates the EU to derogate from fundamental rights more than the EU is legally allowed to do under Article 52(1) of the EU Charter.

To sum up, not only could the EU framework for personal data transfers be found to be in violation of the EU’s international trade commitments, but also international trade commitments requiring (unrestricted) transfers of personal data outside the EEA may be found inconsistent with the EU Charter. Simultaneous application of the two necessity tests (trade law and Article 52 of the Charter), thus puts the EU in a catch-22 situation, as discussed in Section 2.3.4 of this Chapter.

An important doctrinal point should be clarified before moving on. Although international trade agreements are binding on the EU and constitute an ‘integral part’ of its legal system, in the hierarchy of EU legal order, EU primary law (including the EU Charter) prevails over the EU’s international trade commitments. Moreover, neither international trade agreements nor the decisions of international trade adjudicating bodies

---

228 Ibid., paras. 67, 70.
229 Ibid., paras. 70, 119.
230 For further discussion, see section 2.3.3.
231 See, e.g., CJEU, Haegeman, para. 5; CJEU, Opinion 2/13, para. 180.
232 CJEU, Kadi, paras. 282, 307, 308, 316; recital 11 of the Preamble to 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. 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. CJEU, Portugal / Council, para. 48. See also CJEU, Air Transport Association of America and others, para. 74; CJEU, Portugal / Council, para 42; Germany / Council, paras. 106, 108, 110. See also Eckes (2019), p. 152.
have direct effect in the EU.\textsuperscript{233} This approach is based on the principle of the autonomy of the EU legal order in relation to international law, which cannot affect the constitutional values and internal division of competences in the EU.\textsuperscript{234} From an international law perspective, the absence of direct effects of international court decisions in domestic legal systems is not uncommon.\textsuperscript{235} The prerogative of domestic constitutional law to decide how international decisions affect their internal legal frameworks can be viewed as an internal control mechanism that supports the legitimacy of international adjudication.\textsuperscript{236} This mechanism, therefore, ‘relieves international legal decisions from the burdens of legitimation that they are not always capable of bearing by opening up another mechanism of democratic legitimation.’\textsuperscript{237} Furthermore, the principle of autonomy of the EU legal order exemplifies a pluralist approach to the global legal order.\textsuperscript{238}

The EU’s stance in relation to international law and adjudication, nevertheless, does not make the EU’s obligations under international trade law less binding from an international law perspective. Under international law, the EU must perform its obligations in good faith.\textsuperscript{239} Moreover, the EU may face liability and retaliation under international trade law if it fails to comply with its trade commitments or a decision of a trade-adjudicating body, even if such compliance is not possible due to constraints contained in EU primary law.\textsuperscript{240} This is why constitutional restrictions on compliance with such obligations or decisions could present a serious problem. This problem can manifest itself in at least two different contexts. First, in the context of the existing international trade norms, specifically those contained in the GATS. Second, in the context of international


\textsuperscript{234} Starting as early as in 1963 from CJEU case van Gend & Loos. Eckes explains that the CJEU’s choice to protect supremacy of EU law from obligations originating outside the EU ‘is a necessary consequence of the Union’s complex constitutional set-up’. Eckes (2012), pp. 232, 244-249. See also Gaspar-Szilagyi (2015), 349.


\textsuperscript{236} Ibid., pp. 196-197.


\textsuperscript{238} Krisch (2012), p. 103 (describing ‘a model that requires each polity, in an exercise of public autonomy through its institutions, to define the terms on which it interacts with others’ as an example of example of ‘systemic pluralism’). De Búrca’s reply to Weiler in Dialogical epilogue, See Weiler (2012), p. 282. In her own contribution to the book, De Búrca criticises the CJEU’s approach and suggests that some version of Solange approach, to which she also refers to as a ‘soft constitutionalist’ (or ‘soft pluralist’) approach would be preferred. De Búrca (2012). There are, however, some divergences of view in scholarship on the exact meaning of the terms: what De Búrca refers to as ‘pluralism’, other scholars label ‘dualism’ for example. See, e.g., Besson (2009), p. 262-263, Kokott, Sobotta (2012). The CJEU, however, did imply in its decision that the Solange approach could be possible in different circumstances. Kokott, Sobotta (2012), p. 1019.

\textsuperscript{239} Art. 31.1 VCLT.

\textsuperscript{240} Art 27 VCLT.
negotiations concerning cross-border data flows and exceptions for privacy and data protection to be included in future trade agreements, including the ongoing digital trade talks at the WTO.

With respect to the first context, it should be acknowledged that the possibility of a conflict between EU law and EU obligations under the (existing) GATS and WTO legal framework cannot be avoided because the rules are already there. Indeed, it could be argued, from a pluralist perspective, that it should not necessarily be avoided, given divergent moral convictions on data privacy. Instead, it can be viewed as an expression of pluralism. In other words, the absence of clear answers at the point of possible conflict could normatively be a preferred option compared to a clear hierarchy between conflicting norms, so that both international trade and EU law legal orders can decide autonomously on their stance on the issue, without having to fully align their perspectives. In such a pluralist structure, the conflict could be addressed in other ways, notably through dialogue and mutual permeation of rules following a potentially unfavourable outcome for the EU of a WTO dispute settlement, should one occur. At the heart of the normative argument in favour of such a pluralist approach is that it provides space for ‘intense social contestation about the locus of authority and the right collective for decision-making’ on matters surrounded by deep-seated disagreement. Furthermore, ‘[p]luralism is also closer to foundational ideals of political order – namely public autonomy … the plural, divided identities, loyalties, and allegiances that characterize postnational society are better reflected in a multiplicity of orders than in an overarching framework that implies ultimate authority,’ In addition, a pluralist structure offers a potential for adaptation and builds in checks and balances into the global legal order.

The GMO dispute between the EU and the US, where two fundamentally opposing approaches clashed, is often cited as an example of successful cooperation that can be achieved in a pluralist setting. Despite the clash, the WTO Panel, which found against the EU, did so on narrow, formal grounds and avoided any pronouncement on the substance of the EU’s precautionary approach to GMOs, as opposed the risk-based

241 For example, Krisch argues that pluralism seeks to discern a model of order that relies less on unity and more on the heterarchical interaction of the various layers of law. Legally, the relationship of the parts of the overall order in pluralism remains open—governed by the potentially competing rules of the various sub-orders, each with its own ultimate point of reference and supremacy claim, the relationships between them are left to be determined ultimately through political, not rule-based processes.


242 Ibid., pp. 78, 189-190, 206.

243 Ibid., p. 106.

244 Ibid., pp. 78, 103.

245 Ibid., pp. 190-222.
approach mandated by the SPS Agreement.\textsuperscript{246} This has been explained by the incentive of the WTO to preserve its own legitimacy and maintain social acceptance of its dispute-settlement system, as well as to avoid the risk that the EU would simply not comply with a ‘hard’ decision against it (an option, however, that seems available only to more powerful WTO Members).\textsuperscript{247} On the EU side, the WTO dispute settlement reports has had a profound effect on EU domestic rules on GMOs, and the CJEU has integrated WTO law into its jurisprudence, despite its reluctance to grant it direct effect.\textsuperscript{248} The pressure for compliance, arguably, came from the high costs of non-compliance with the WTO Panel’s report.\textsuperscript{249} In sum, the political dialogue that ensued after the unfavourable WTO dispute settlement reports led to ‘far-reaching convergence on both principles and processes around the SPS approach.’\textsuperscript{250}

There are at least two reasons, however, why a pluralist approach is unlikely to play out in the same way in relation to the clash between the rules on data privacy in the current circumstances. First, and most importantly, unlike the GMO debate, the clash between the EU approach to governing cross-border data flows and data privacy protection, and other countries, such as the US, which could potentially result in a confrontation at the WTO, concerns not only EU secondary, but also EU primary law, as this Chapter demonstrates. The new legal reality, in which the EU Charter is binding and constitutes a part of EU primary law, considerably limits the potential of trade law to shape EU governance of data privacy protection as compared to the GMO case. As a result, the EU may have to face the costs of trade retaliation, – no matter how high – should its framework for transfers of personal data outside the EEA be found to be inconsistent with the GATS. If retaliation resulted in a suspension of personal data flows into the EU, this would directly cut across the EU digital trade policy, which aims to liberalise such flows.\textsuperscript{251} It is, however, possible that WTO adjudicators – in the spirit of a pluralist approach – would not come down too hard on the EU on the data privacy issue. For example, in his 2000 article, Shaffer argues that ‘[u]nder media scrutiny, WTO dispute settlement panels would prefer to refrain from engaging in a close balancing of competing trade and privacy interests, and rather review the process by which the European Union takes account of foreign privacy protections.’\textsuperscript{252}

Second, although, as mentioned above, the CJEU has used the tool of treaty-consistent interpretation to interpret EU law in the light of international law, including WTO law, it has not done so in areas with high salience, such as issues of the EU’s banana market and

\textsuperscript{248} Krisch (2012), pp. 215-216.
\textsuperscript{249} Ibid., pp. 9-10, 20-21.
\textsuperscript{250} Ibid., p. 216.
\textsuperscript{251} For a discussion, see Section 4.2.5.
\textsuperscript{252} Shaffer (2000), p. 51
import of hormone treated meat.\textsuperscript{253} In the latter case, the EU has been incompliant with its WTO commitments and has faced trade retaliation measures from the US and Canada for more than 20 years.\textsuperscript{254} It is equally unlikely that the CJEU will take into account EU trade obligations under the WTO Agreements in its future jurisprudence on the issue of transfers of personal data, as it has already refrained from doing so in both Schrems I and Schrems II concerning transfers of personal data from the EU to the United States. As explained above, in some of its judgements the CJEU has implicitly ranked the fundamental rights to privacy and the protection of personal data above other relevant fundamental rights, such as the right to conduct business.

In the context of international negotiations of future trade agreements, the risk of a clash between the two necessities, as described above, makes replication of the GATS general exception for privacy and data protection problematic from an EU law perspective. This thesis addresses that problem in Chapter 4. The main legal reason for this is, as previously mentioned, that the EU institutions must ensure the compatibility of any trade agreements they negotiate with internal EU policies and rules.\textsuperscript{255} Preserving uncertainty as to whether the proposed agreement is compatible with the EU \textit{acquis} (which could be viewed as a normatively preferred option from a pluralist perspective), could result in a CJEU judgement under Article 218(11) TFEU finding such an agreement incompatible with the EU \textit{acquis}. This would, ultimately, require a re-negotiation of the agreement, which would not only delay the conclusion of the agreement, but also result in the additional costs of renegotiation and forfeited benefits from delayed trade concessions under the proposed agreement. It is worth recalling that the conflict about the proper regulatory approach to GMOs in agriculture, which was used to illustrate why a pluralist approach could be normatively more desirable, itself resulted from a situation where European negotiators on the SPS Agreement did not insist on wording that would have shielded the EU approach to sanitary and phytosanitary measures in certain areas (based on the precautionary principle rather than a risk-based approach relying on science as justification for trade-restrictive measures).\textsuperscript{256} In view of the above-mentioned TFEU provisions, as well as the fact that the rights to privacy and the protection of personal data

\begin{itemize}
    \item \textsuperscript{253} Krisch (2012), p. 205.
    \item \textsuperscript{254} Although the EU never adjusted its legislation in compliance with the WTO decisions, the issue has been settled recently through EU giving Canada and the US concessions on import of hormone free beef. See European Commission, Press Release: \textit{The European Union and the United States sign an agreement on imports of hormone-free beef}, 2 August 2019; Miles (2017).
    \item \textsuperscript{255} Art. 207(3)(2) TFEU.
    \item \textsuperscript{256} Krisch (2012), pp. 215-216, explaining that the EC found itself with few allies and had to give in if negotiations were to continue—it was keen on a successful conclusion because it sought to reduce obstacles to its own market access in other countries and did not want to see this relatively low-priority issue threaten negotiations on other, more central parts of the Uruguay Round.
\end{itemize}
are binding fundamental rights in the EU, a similar outcome is simply not possible as a matter of EU law in the trade negotiations affecting EU data protection framework. Another related reason, according to which, data protection cannot be traded in international trade negotiations, as well as its commitment to safeguard its full autonomy to protect the rights to privacy and the protection of personal data as fundamental rights, is an important internal political message to the public.\textsuperscript{257} From a political perspective, replication of the GATS general exception for privacy and data protection, in conjunction with a provision on cross-border data flows in the EU’s future trade agreements, is also very likely to be opposed by the European Parliament. This may also lead to the European Parliament’s refusal to consent to the trade agreement.\textsuperscript{258} For example, the European Parliament strongly opposed replication of the GATS general exception in the failed TTIP and TiSA.\textsuperscript{259}

2.3.2 Trade law necessity and EU Restrictions on data transfers

To be justified under the general exception contained in GATS Article XIV, a prima facie inconsistent measure has to meet one of the material requirements of the general exception set forth in Article XIV (a) to (e) and the introductory clause (or chapeau) of this Article. This general exception applies horizontally to measures that violate any obligation under the GATS. The wording of the general exception is remarkably consistent in most US- and EU-led trade agreements, in that they all closely follow GATS Article XIV.\textsuperscript{260} This is why the interpretation of the trade necessity test at the WTO may be relevant also in the context of other trade agreements.

This general exception requires a two-tier assessment: first it has to be established whether the contested measure meets one of the substantive requirements of paragraph (c); second, there is an examination of whether the contested measure satisfies the requirements

\textsuperscript{257} For a discussion, see Section 4.2.1.
\textsuperscript{258} For a discussion on the increased role of the European Parliament both at the stage of negotiation and adoption of international trade agreements after the Lisbon Treaty, and how the Parliament has used this role in practice see Eckes (2019), pp. 153-166.
\textsuperscript{259} European Parliament resolution of 8 July 2015 containing the European Parliament’s recommendations to the European Commission on the negotiations for the Transatlantic Trade and Investment Partnership (TTIP) (2014/2228(INI)). European Parliament resolution of 3 February 2016 containing the European Parliament’s recommendations to the Commission on the negotiations for the Trade in Services Agreement (TiSA) (2015/2233(INI)). In its resolution on TiSA (para. 1(c)(iii)), the European Parliament recommended European Commission:
… to incorporate a comprehensive, unambiguous, horizontal, self-standing and legally binding provision based on GATS Article XIV which fully exempts the existing and future EU legal framework for the protection of personal data from the scope of this agreement, without any conditions that it must be consistent with other parts of the TiSA.
The Resolution on TTIP contains an identical recommendation in para 2(xii).
\textsuperscript{260} The most recent examples of EU trade agreements where the GATS art XIV was closely reproduced include Art. 28.3(2)(c)(ii) CETA, Art. 8.62(e)(ii) EU-Singapore FTA, and Art. 8.3 JEFTA.
of the *chapeau* of the exception. The necessity test is the core of the first stage of the assessment.

Article XIV(c)(ii) has never been applied by a WTO panel. However, privacy and data protection is not the first public policy interest in tension with trade liberalisation. The interpretation of the necessity test in WTO cases touching upon other public policy interests listed in GATS Article XIV(c) and Article XX of the General Agreement on Tariffs and Trade (GATT) 1994 – applicable to international trade in goods instead of services, which also feeds into the application of ‘necessity’ in the GATS, and vice versa – can inform the interpretation of paragraph (c)(ii). The method used to interpret ‘necessity’ applied by WTO adjudicating bodies is fairly consistent irrespective of the specific public interest invoked to justify the measure, be it the protection of public morals, public health, or securing compliance with a WTO-consistent law.

Existing WTO case law has established a high threshold for meeting the necessity test, which in some cases has been almost impossible to meet.

The assessment of the necessity of a GATS-inconsistent measure applied by the WTO adjudicating bodies (first expounded in *Korea – Various Measures on Beef* and recently confirmed in *US — Tariff Measures*) requires ‘weighing and balancing’ of the following factors:

1. The relative importance of the protected public interest(s) pursued by such contested measure,
2. The contested measure’s contribution to the achievement of objective pursued, manifested in the existence of a ‘genuine relationship of ends and means between the objective pursued and the measure at issue’,

---


262 See e.g. WTO, Appellate Body Report, *US-Gambling*, para. 291.


3. The trade restrictiveness of the measure,\(^{268}\) followed by an assessment of whether, in the light of importance of the interests at issue, a less trade restrictive alternative is ‘reasonably available’.

In application to EU restrictions on transfers of personal data, the ‘relative importance’ factor would be a translation of the requirement that the contested restrictions be designed to secure compliance with the laws and regulations relating to the protection of privacy and personal data. As the WTO Appellate Body stated in *US – Gambling*, the process of assessing ‘necessity’ “begins with an assessment of the ‘relative importance’ of the interests or values furthered by the challenged measure.”\(^{269}\) The more important the interest, the heavier it weighs in the assessment, and the heavier it weighs in the justification of a relatively more restrictive measure. In prior cases, the WTO adjudicating bodies have assigned different values to the various public policy objectives mentioned in the general exceptions of GATS Article XIV and GATT Article XX. For example, the protection of human health and life have been recognised as ‘vital and important in the highest degree’,\(^{270}\) the aim of protecting environment as ‘important’,\(^{271}\) and the protection of the tax collecting systems against tax evasion as being ‘of vital importance’.\(^{272}\) Some case law suggests that the level of international support of the interest at stake\(^ {273}\) or the actual (as opposed to desired) contribution of the measure to achieve a claimed level of protection of public policy interest\(^ {274}\) could weigh in this assessment. Beyond this factor, it is unclear how the WTO adjudicators assess the importance of different non-economic values. No objective has been characterised as ‘unimportant’.

Assessment of factors 2 and 3 in the list above comprises a weighing and balancing of the contribution of the measure to the protected interest, with the trade restrictiveness of the measure in light of the relative importance of the protected interest or the underlying values of the objective pursued.\(^ {275}\) On a continuum between ‘indispensable’ and ‘making a contribution to’, ‘necessity’ is understood as being closer to ‘indispensable’ rather than

---

\(^{268}\) Assessment of this factor was left out in WTO, Appellate Body Report, *EC - Asbestos*, p. 179.


‘making a contribution to’. Thus, the greater the contribution of the contested measure, and the less restrictive it is, the more likely it is to satisfy the necessity test. It is, however, debatable whether this or the following factor is decisive in the assessment of necessity in practice.

If the defending party has succeeded in making a *prima facie* case of ‘necessity’, the complaining party may rebut it by showing that a less trade-restrictive measure was ‘reasonably available’ to the defending party. This assessment includes a ‘comparison between the challenged measure and possible alternatives …, and the results of such comparison should be considered in the light of the importance of the interests at issue.’ ‘Reasonably available’ is interpreted as allowing a WTO member to achieve the *same level of protection* of the public interest or objective pursued without prohibitive cost or substantial technical difficulties. Based on this interpretation, the comparison of alternative measures does not typically involve a fully-fledged proportionality assessment, which is arguably the case in the assessment of the trade-restrictiveness of the measure. Rather, this comparison involves the balancing of the administrative and enforcement costs of alternative measures granting the same level of protection to a public interest at issue against the trade costs of such measures. It is generally agreed that the factors in the assessment of ‘necessity’, which, on the one hand, include weighing and balancing, and on the other, the assessment of reasonable availability of a less trade-restrictive measure, contain a logical contradiction and are incompatible: the first assessment leaves WTO members much less regulatory autonomy than the other. This has resulted in a disagreement between two groups of academics, one of which argues that the weighing and balancing in the assessment of necessity requires a fully-fledged proportionality or cost-benefits assessment. The other group, however, contends that the analysis of necessity turns on the assessment of reasonable availability of a less trade-restrictive measure.

In most instances, the WTO adjudicating bodies do base their reports on the

---


281 Regan (2007); McGrady (2009); Lang (2007).


assessment of reasonable availability of a less trade-restrictive measure, and rightly so. This is a more lenient approach than the proportionality assessment, which arguably allows WTO members to choose the level of protection of the public interest at issue.\textsuperscript{285} In \textit{US-Gambling}, the Appellate Body explicitly equated the absence of necessity with the reasonable availability of another WTO consistent measure.\textsuperscript{286} However, the risk that those bodies will conduct a fully-fledged cost-benefit analysis always remains. For example, in one of the most recent WTO Panel reports, the Panel based its analysis on the weighing and balancing of the three factors mentioned above \textit{without} engaging into a comparison of the contested measure with reasonably available alternative measures.\textsuperscript{287} Furthermore, in practice, the WTO members’ autonomy to choose and maintain their own level of protection could be much narrower than it may seem at first glance, notably because it can be narrowed depending on how the adjudicating bodies interpret the term ‘same level’ of protection.

Does the ‘same’ level of protection mean a \textit{desired} level of protection (subjectively determined by the State and not (yet) necessarily achieved) or the \textit{actual} level of protection achieved by the disputed measures? The WTO adjudicating bodies have not been consistent in their answer to this question. For example, in Korea – Various Measures on Beef, based on the \textit{actual} application of the contested measure, judging by the design of the contested measure the Appellate Body ‘assumed’ that ‘Korea intended to reduce considerably the number of cases of fraud occurring with respect to the origin of beef sold by retailers’ rather than to ‘totally eliminate fraud’.\textsuperscript{288} From this perspective, alternative measures (compared to the contested measure) should not be required to achieve a higher level of protection than that \textit{actually} achieved by the contested measure. The level of protection \textit{desired} by the defending WTO member is thus irrelevant. Remarkably, in that case, the alternative measure that, according to Appellate Body, was reasonably available to Korea, involved significantly higher administrative and enforcement costs.\textsuperscript{289} This, however, did not prevent the Appellate Body from concluding that the contested measure

\textsuperscript{286} WTO, Appellate Body Report, \textit{US Gambling}, para. 307 (stating that: ‘[i]t is on the basis of this “weighing and balancing” and comparison of measures, taking into account the interests or values at stake, that a panel determines whether a measure is "necessary" or, alternatively, whether another, WTO-consistent measure is “reasonably available” ’.) \textit{(emphasis added).}
\textsuperscript{287} WTO, Panel Report, \textit{US – Tariff Measures}, paras. 7.232-7.238. It could, however, also be argued, that in that particular case the Panel did not consider reasonably available alternatives because the contested measure did not meet step 2 in the assessment. In particular, as a reason for not engaging in such analysis the Panel states that ‘[t]he Panel's preliminary conclusion, based on a weighing and balancing of the relevant factors, is that the United States has not explained how the chosen measures are apt to contribute to the public morals objective, as invoked by the United States, and how they could therefore be “necessary”’.
\textsuperscript{288} WTO, Appellate Body Report, \textit{Korea – Various Measures on Beef}, para. 178, internal footnotes omitted.
\textsuperscript{289} \textit{Ibid.} para 175.
did not pass the assessment under the third factor. Conversely, in *US – Gambling*, where the alternative measure proposed by the claiming party was dismissed as ‘not an appropriate alternative’, the Appellate Body explained that a ‘reasonably available’ alternative measure should preserve the responding Member’s ‘right to achieve its desired level of protection’.290 Although the Appellate Body did not elaborate on the degree of deference to the WTO member in the assessment of the ‘desired level’, it could still be argued that the choice of this word requires an assessment of what the WTO member aimed for, rather than an objective assessment of what the contested measure actually achieves. In *EC – Seals*, the WTO Panel concluded that because of the exceptions from the ban on seal products, which allowed certain commercial activities within the European Union, ‘the level of protection actually achieved by the measure is as high as the European Union claims the measure initially aimed to achieve’ and that the Panel ‘will bear this in mind in … subsequent analysis of the reasonable availability of a less trade-restrictive alternative measure’.291 Although in that particular case, both the Panel and the Appellate Body nevertheless concluded that a less restrictive measure was not reasonably available to the EU,292 clearly the risk that trade adjudicating bodies may not respect the level of protection asserted by a defending party persists.293

More generally, even if the adjudicating bodies were to afford sufficient deference to the level of protection desired by the State, the analytical exercise of ensuring that an

---

290 WTO, Appellate Body Report, *US – Gambling*, paras. 308, 317, footnotes omitted. (emphasis added). The WTO Appellate Body reiterated the same approach in WTO, Appellate Body Report, *EC – Seal Products*, para. 5.261: ‘in order to qualify as a genuine alternative, the proposed measure must be not only less trade restrictive than the original measure at issue, but should also preserve for the responding Member its right to achieve its desired level of protection with respect to the objective pursued’. (internal footnotes and quotation marks omitted.)


292 WTO, Appellate Body Report, *EC – Seal Products*, para. 5.279; WTO, Panel Reports, *EC – Seal Products*, para. para. 7.504. Both the Panel and the Appellate Body, however, found that the contested EU ban on seal products did not meet the requirements of the Chapeau of Article XX GATT because the exceptions for some commercial activity with seal products in the EU lead to unjustifiable discrimination, and that discrimination could not be reconciled with, or is rationally related to, the policy objective of protecting public morals. WTO, Panel Reports, *EC – Seal Products*, para. 7.648; WTO, Appellate Body Report, *EC – Seal Products*, para. 5.339.

293 From a pluralist perspective, there is an argument that by not establishing ‘in any meaningful sense … concrete rules of decision on the public interest exceptions’ and not settling ‘the lines of authority’ the WTO Appellate Body have ‘moved toward a more pluralist structure. It has created space for states to use WTO law to keep fighting about the proper balance between the WTO policy on liberalization and their own idiosyncratic regulatory goals. This balance is unstable and consistently at issue in WTO legal disputes’. Hakimi (2020), p. 569. Thus, from this perspective, leaving the tests for assessing whether trade-inconsistent measures can be justified under public interest exceptions is a desirable outcome conducive to sustaining the WTO as a forum where ‘trade governance happens’. See also Shaffer (2008), p. 71, arguing that by keeping their opinions ambiguous, WTO adjudicating bodies ‘can shape their decisions to facilitate [compliance by powerful WTO Members] and amicable settlement, and thereby uphold the WTO legal system’.
alternative measure would achieve exactly the same level of protection would be nothing more than educated second-guessing. When the public policy goals pursued by contested measures are non-economic values, in practice it may be especially difficult to accurately define the level of their protection which serves as a benchmark for the comparison of alternative measures. It is equally difficult to determine ex ante whether alternative measures would secure the same level of protection.

Recall that, while the assessment of reasonably available alternative measures is conducted in the light of the importance of the public interest at stake, existing WTO case law does not shed much light on the weight of this factor in the assessment. There is, therefore, a related risk that the importance of the public interest, as determined by the adjudicating bodies, may influence the assessment of whether a less trade restrictive alternative measure is reasonably available. One could argue that the importance of the interest influences the deference to the level of protection chosen by the country. Thus, in Korea – Various Measures on Beef, where the Appellate Body did not make any statement as to the importance of the public interest pursued by the contested measure, the level of deference to the chosen level of protection was lower as compared to US – Gambling, where the Appellate Body agreed that the contested measure protected ‘very important societal interests’.

Relying on the analysis above, one may conclude that the application of trade law’s necessity test to the EU framework for transfers of personal data to third countries, as implemented in the GDPR, may not result in the recognition of the ‘necessity’ of this framework by the WTO adjudicators. Although the chances of this outcome are higher (should trade adjudicating bodies apply the proportionality assessment), the risk remains, even in the case of a more lenient interpretation of ‘necessity’, which amounts to the assessment of reasonably available alternatives to a contested measure. There are at least two reasons for this. First, it could be argued that there is an insufficient nexus between the

---

295 Although there are statements in academic literature to the contrary, the publications that contain argumentation on this point are rather outdated and do not take into account the most recent developments in EU data privacy law, most importantly the CJEU’s post-2009 jurisprudence on the fundamental rights to privacy and the protection of personal data, in particular the Schrems I and II decisions. See, e.g., Asinari (2002); Shaffer (2000). Of the most recent literature, those arguing that EU restrictions would satisfy the necessity test typically do not engage in elaborate discussion and rather presume that since there is an exception for data protection, there is a chance that EU framework can be justified. See, e.g., Chen (2015), p. 219, who limits the assessment to one sentence: ‘Although until now, there hardly has been a case that the responding party won by claiming the general exceptions clause, one could still see the interest of privacy being recognized through the substantial establishment of an exclusive clause for privacy in Article 14 (c) subsection (ii) of the GATS’.
contested restrictions on transfers of personal data, and the aim of achieving a high level of protection. Second, the EU framework for transfers of personal data may be recognised as not the least trade restrictive.

On the first point, it could be argued that the link between the existing EU framework for data transfers and the purpose of ensuring a high level of protection of personal data, particularly from foreign governments’ ability to access this data, is closer to ‘making a contribution to’ rather than ‘indispensable’. As demonstrated above, mechanisms for systematic personal data transfers under the GDPR must ensure that the level of protection that a particular third country ensures in respect to the transferred data is ‘essentially equivalent’ to that in the EU, where the ‘level of data protection’ means not only the quality of the data protection rules, but multiple other factors, including: the respect for the rule of law and human rights, access of public authorities to personal data, the existence and effective functioning of independent supervisory authorities, etc. There is, however, a sizeable gap between the level of protection that this framework should and can deliver in practice. The Transatlantic saga on cross-border data flows is but one illustration of the point.

After the CJEU invalidated the adequacy decision for the US (the EU-US Safe Harbor framework) in 2015 by Schrems I judgement – which also introduced for the first time the ‘essential equivalence’ requirement – against a background of low level of enforcement, personal data continued flowing to the US despite the absence of ‘essentially equivalent’ protection of such data. The 2016 EU-US Privacy Shield framework, which replaced the Safe Harbor and underlay transatlantic personal data transfers for almost four years, did not – as the CJEU confirmed in the Schrems II judgement – remedy the absence of ‘essentially equivalent’ protection of personal data under US law. Although it is too early to judge, some predict that (as happened after the Schrems I judgement), even after Schrems II ‘data will continue to flow across borders; indeed, at the time of writing, it still does, both on the basis of the invalid Privacy Shield and the SCCs without additional safeguards.

On the second point, one could argue that the EU framework is not the ‘least trade restrictive’, especially in relation to businesses not having an establishment or business partner in the EEA. For example, one could argue that ‘it may be difficult to prove that

297 CJEU, Schrems I, para 73; CJEU, Schrems II, para. 94; recital 104 GDPR.
298 Art. 45 GDPR.
299 For further discussion, see Section 5.3.
300 See Sections 5.3.1 and 5.3.2.
301 CJEU, Schrems II.
302 Tene (2020b).
303 See, e.g. Lee (2020).
privacy cannot be otherwise protected’. The fact that compliance with the standard of the recently modified Convention 108 – characterised by Greenleaf as ‘close to the current global average for data privacy laws’ – is in itself insufficient, especially in the light of the CJEU Schrems II judgement, to warrant an adequacy decision from the EU, and demonstrates that the benchmark set by the EU is higher than that recognised by any other international standards. Under recital 105 of the GDPR, when assessing the adequacy of personal data protection in a third country, the EU Commission should take into account accession of that country to Convention 108. However, Article 14(1) of the Convention 108+ allows a Party to the Convention to restrict transfers from another Party to the Convention if ‘bound by harmonised rules of protection shared by States belonging to a regional international organisation’. Given that compliance with the Convention 108+ does not constitute a sufficient ground for adequacy under the GDPR, it is possible that following the assessment by the European Commission of the legal framework of a Party to this Convention, the adequacy decision will not be granted.

One could assert, as a counter-argument, that the level of protection of the fundamental right to personal data protection chosen by the EU – ‘effective and complete’ protection – makes other, less restrictive alternatives unavailable to the EU. In particular, in contrast to the EU Charter, some international standards on personal data protection, such as the OECD 2013 Guidelines on the Protection of Privacy and Transborder Flows of Personal Data and the 2015 Asia-Pacific Economic Cooperation (APEC) Privacy Framework take an instrumental approach to the protection of personal data and therefore warrant a lower level of personal data protection (their primary purpose is to keep restrictions on personal data transfers to a minimum). At the same time, just like the EU Charter and the GDPR, the Convention 108+ recognises the right to the protection of personal data as a human right. Nevertheless, the restrictions on transfers of personal data to countries that are not Parties to this Convention are still less stringent than those under EU data protection framework. As explained above, it is entirely possible that,

---

304 Burri (2017b), pp. 95-96.
306 For a discussion, see, e.g., Duque de Carvalho (2019); Greenleaf (2018a), p. 5.
307 See also Article 29 Working Party, Working document on Adequacy Referential, WP 254rev.01, 6 February 2018.
308 Para. 107 of the Explanatory Report to the modernised Convention 108 clarifies that this provision applies in particular to the member States of the EU.
309 CJEU, Google Spain, para. 34; CJEU, Wirtschaftsakademie, para. 28; CJEU, Fashion ID, paras. 50, 66.
311 For a comparison of these standards with the European framework, see Yakovleva (2018), pp. 8-9.
312 Art. 1 Convention 108+.
313 While Art. 14 of Convention 108+ conditions transfers of personal data to a State or international organization that is not a party to the Convention on the requirement of securing an ‘appropriate’ level of
given the lack of international harmonisation of data privacy rules, trade adjudicators would give little deference to the EU’s desired high level of protection, and would focus instead on the actual level of protection achieved.314 In the absence of reliable statistics on this matter, and the difficulty of producing any concrete evidence of the level of data privacy protection,315 the adjudicators may buy into empirical arguments, such as those offered by Bamberger and Mulligan, that compared the EU data protection regime to the more liberal US approach, and found that, although the latter was not as comprehensive ‘on the books,’ it operated much more effectively ‘on the ground’.316 Assessment of the ‘effectiveness’ of data protection on the ground, does not take into account the non-instrumental protection of fundamental rights to privacy and the protection of personal data as moral values.317 Therefore, from an EU law perspective, it could be viewed as incomplete. However, it is precisely the instrumental approach that could be ultimately adopted by trade adjudicating bodies. As Howse and Langille argue:

where the basis for arguing that a measure is not pretextual is at least partly motivated by noninstrumental moral concerns not universally shared by WTO members, there is a risk that a WTO official or adjudicator who does not share the value in question, or is unfamiliar from its own moral experience with this kind of belief, will begin from a presumption that there is a strong risk of pretextualism. … [T]he WTO insider community is drawn from a world of diplomats and bureaucrats where a certain kind of instrumental-often economic-rationality dominates conceptions of appropriate public policy. As our analysis of the Seal Products dispute has illustrated, using tests or devices that employ instrumental rationality, such as means/ends reasoning, simply does not work to establish the non-pretextual character of noninstrumental moral regulation.318

In addition, some studies suggest that restrictions on transfers of personal data do not sufficiently contribute to ensuring privacy protection against foreign surveillance.319 The dual facts that the EU framework for transfers of personal data provides the same restrictive

-------------------

315 This issue is discussed in more detail in Section 3.4.2.
317 For further discussion see Section 3.4.2.
318 Howse, Langille (2012), p. 429. See also Howse, Langille, Sykes (2015), pp. 105-106. The authors make an argument in relation to the legislation that can be justified under the general exception for public morals. This reasoning is, however, also applicable to other legislation subject to justification under specific thematic exceptions of the general exceptions, such as the one for privacy and data protection.
approach to any information that qualifies as personal data (which includes a broad range of data under EU law), and does not calibrate restrictiveness in relation to the severity of the risk of interference in individuals' fundamental rights, could also be used as an indication that other (more granular and overall less trade restrictive) frameworks are ‘reasonably available’ to the EU. Consequently, the importance of the right to the protection of personal data would be given relatively less weight in a trade dispute. While in EU law it is recognised as a fundamental right — and hence one of the highest values in the EU and on a par with other fundamental rights, trade adjudicating bodies may lean towards an economic approach to privacy and data protection that underlies the existing international standards on data protection mentioned above.

2.3.3 Necessity under EU law

From the CJEU case law, it follows that any legislative act of the EU that involves personal data processing, such as the use or transfer of personal data, constitutes ‘in itself’ a limitation of the fundamental right to the protection of personal data, regardless of whether it can be justified. Such a limitation first triggers the assessment under the requirements of Article 8(2) of the EU Charter. Then, any limitation on this right is only lawful if it meets the requirements of Article 52(1) of the EU Charter, which provides a mechanism for balancing different fundamental rights and freedoms with each other, as well as with other competing policy objectives.

It is the prerogative of the CJEU to conduct a fact-based assessment of whether a derogation is ‘necessary’ in each particular case. As already mentioned above, since 2009, the CJEU has established a higher threshold for derogations from the fundamental rights to privacy and the protection of personal data under Article 52(1) of the EU Charter when balancing these fundamental rights with other competing rights and interests. In a line of cases, most notably Volker und Markus Schecke, Digital Rights Ireland, Tele

\[320\] See Purtova (2018).  
\[323\] Existing CJEU case law suggests that the conditions of lawfulness of personal data processing contained in art 8(2) and art 52(1) of the EU Charter should analysed cumulatively. See, e.g., CJEU, Opinion on EU-Canada PNR Agreement, paras. 137-138, 142ff.  
\[324\] Unlike international trade law, the text of art 52(1) EU Charter explicitly mentions that the assessment of ‘necessity’ should include a fully-fledged proportionality balancing.  
\[326\] CJEU, Volker und Markus Schecke, paras. 77 and 86.  
\[327\] CJEU, Digital Rights Ireland, paras. 51 and 52.
2. Schrems I, Schrems II, and Opinion on EU-Canada PNR Agreement, the CJEU elevated the EU Charter necessity test to the level of ‘strict necessity’ when a derogation from the fundamental rights to privacy and the protection of personal data is at stake. This approach was later taken up by the Article 29 Working Party and the European Data Protection Supervisor (EDPS). It is now settled CJEU case law that the ‘strict necessity’ standard should apply horizontally in all contexts, to both commercial and national security, as long as limitation of the fundamental rights to privacy and data protection is involved.

Just as with the trade necessity test, ‘strict necessity’ under Article 52(1) of the EU Charter in relation to privacy and data protection is hard to satisfy. In assessing ‘strict necessity’, the CJEU determines whether ‘it is possible to envisage measures which affect less adversely that fundamental right of natural persons and which still contribute effectively to the objectives … in question.’ This approach resembles the least-restrictive-means principle in the interpretation of the trade necessity test. While trade law requires that measures aimed at protecting the right to protection of personal data should be least restrictive on trade, conversely, the EU Charter demands that trade rules should be least restrictive of fundamental rights.

According to the CJEU, legislation interfering with fundamental rights to privacy and the protection of personal data can only pass the ‘strict necessity’ if it:

lay[s] down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards, so that the persons whose data has been transferred have sufficient guarantees to protect effectively their personal data against the risk of abuse. It must, in particular, indicate in what circumstances and under which conditions a measure providing for the processing of such data may be adopted, thereby ensuring that the interference is limited to what is strictly necessary. The need for such safeguards is all the greater where

---

328 CJEU, Tele2 Sverige, paras. 96 and 103.
329 CJEU, Schrems I, para. 92.
330 CJEU, Schrems II, para. 176.
331 CJEU, Opinion on EU-Canada PNR Agreement, para 140.
332 See e.g. Article 29 Working Party, Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees), WP 237, 13 April 2016, p. 5.
335 CJEU, Volker und Markus Schecke, para. 86.
personal data is subject to automated processing.\textsuperscript{336}

The CJEU factored in two other general considerations to its analysis: First, the seriousness of the interference that a particular measure limiting the fundamental rights to privacy and the protection of personal data entails\textsuperscript{337} and second, the importance of the interest pursued by the measure. Concerning the latter factor, one might recall that the relative importance of competing interests also takes part in the assessment of trade ‘necessity’. According to the CJEU, the objective of \textit{public security can justify even serious interferences} with privacy and data protection, if such measures meet the ‘strict necessity test’.\textsuperscript{338} However, the economic interests of a private party, as explained above, seem to be at the other end of the importance continuum. Thus, although data protection may not be considered of highest importance in international trade law, cross-border digital trade is unlikely to weigh heavily against data protection in the EU’s fundamental rights calculus.

\textbf{2.3.4 The incompatibility of two ‘necessities’}

Now that both tests have been explicated, one can see that the risk of tension lies in the fact that neither the EU’s trade liberalisation commitments to trade in services nor a potential decision of an international trade adjudicating body requiring the EU to reduce the restrictions on cross-border transfers of personal data to comply with such commitments, are likely to survive the EU Charter’s ‘strict necessity’ assessment.

To show the polar opposition between the two tests, one could say that, because transfers of personal data outside the EEA amount to a limitation of the fundamental rights to privacy and the protection of personal data, the CJEU’s assessment of the liberalisation of data transfers starts from the question of ‘whether transfers \textit{should be allowed} and under what conditions’. In trade law, the question is the opposite, namely ‘whether transfers \textit{should be limited}'. Implementing a decision by an international trade adjudicating body requiring the EU to lower the standard of ‘essential equivalence,’ which all the mechanisms for systematic personal data transfers should meet based on the CJEU jurisprudence,\textsuperscript{339} would run afoul of the core of the conditions under which the CJEU considers transfers of personal data outside the EEA compliant with the EU Charter. It follows from the CJEU \textit{Schrems II} judgment that, in the context of transfers of personal data outside the EEA, the ‘essential equivalence’ requirement is an instantiation of the strict necessity test of article

\textsuperscript{336} CJEU, \textit{Schrems II}, para. 176, internal footnotes omitted. See also CJEU, \textit{Schrems I}, paras 93, 95; CJEU, \textit{Opinion on EU-Canada PNR Agreement}, paras. 140-141, 154.


\textsuperscript{338} CJEU, \textit{Opinion on EU-Canada PNR Agreement}, paras. 149, 154. (emphasis added)

Two other core conditions for the compliance of a data transfer mechanism with the EU Charter are the existence and effective functioning of an independent supervisory authority, and effective administrative and judicial remedies for individuals. All the mechanisms allowing for systematic transfers of personal data outside the EEA meet, to some extent, this condition. This component of the fundamental right to the protection of personal data alone renders infeasible, under the EU Charter, any approach to data transfers that does meet the following two criteria. First, those that do not allow for a preliminary assessment of the legal regime in the country of destination. And, second, those that do not require a commitment from a personal data recipient in a foreign country to grant EU individuals certain safeguards to exercise their rights to judicial remedy. Even if other mechanisms for data transfers are theoretically possible, those mechanisms, if applied horizontally to all types of personal data, would not be less trade restrictive than those already envisaged in the GDPR.

2.4 Ways forward

The discussion in this Chapter has shown that in prior cases concerning the trade-off between the WTO members’ autonomy to protect public interests like the environment or public health, on the one hand, and trade liberalisation commitments on the other, the trade necessity test has been interpreted restrictively. Too restrictively to accommodate the EU’s current approach to transfers of personal data outside the EEA under the EU Charter, as implemented in the GDPR. At the same time, under the strict necessity test contained in the EU Charter (as interpreted by the CJEU), the regulatory autonomy under EU law to derogate from the protection of the fundamental rights to privacy and the protection of personal data may be insufficient to comply with the EU’s international trade obligations when it comes to cross-border flows of personal data. The sequential application of the two ‘necessities’ creates an overlap (see Figure 1) where there is a risk that the two ‘necessities’ may clash, putting the EU in a compliance dead-lock between the violation of trade law or unjustifiable derogation from the fundamental right to the protection of personal data, as construed by the CJEU.

---

340 CJEU, Schrems II, paras. 184-185.
341 For further discussion on this issue see Section 5.2.2.
342 E.g. Art. 45(2)(b) GDPR on adequacy assessment, Arts. 47(2)(e), 40(4) and 40(2)(k) GDPR, Clause 5(c) and 7(1)(b) Standard contractual clauses (Set I); Clause V(c) and para (7) of preamble to Commission Decision 2004/915/EC approving Standard contractual clauses (Set II); Clause 5(e) and 7(1)(b) of Standard contractual clauses for controller to processor transfers. In Schrems II, the CJEU explicitly confirmed that the latter SCC Decision meets the requirement to ensure an effective remedy. CJEU, Schrems II, paras. 144, 145, 148.
In the context of the ongoing digital trade negotiations that the EU is conducting with its trading partners on cross-border data flows, privacy and data protection, this state of affairs is not sustainable. As explained in Section 2.3.1 above, the EU should be able to comply with the Charter and its international trade obligations simultaneously. The path forward suggested in this thesis, and further elaborated on in Chapters 3 and 4, is guided by three principal considerations. First, from a practical perspective, it is risky to wait until the EU restrictions are struck down by – or even challenged by – an international trade adjudicating body which will force the EU’s hand. A more proactive approach seems preferable. Second, and relatedly, ongoing uncertainty surrounding the lawfulness of transfers of personal data outside the EEA, on the one hand, and compliance with the restrictions on such transfers with EU’s international trade commitments, on the other hand, may have a chilling effect on cross-border trade to the detriment of EU businesses. Third, although the approach to transfers of personal data outside the EEA that would make the most solid contribution to the ‘effective and complete’ protection of the fundamental rights to privacy and the protection of personal data is a total ban on such transfers, this rather extreme approach would undermine the very existence of digital cross-border trade with the EU and is thus unwarranted.

This thesis envisions that the problem explicated in this Chapter should be
addressed from both international trade and EU law perspectives. It elaborates on the ways this can be done in Chapters 4 and 5 respectively. From an international trade law perspective, as discussed in Chapter 4, one way out of the quandary is to negotiate a broader general exception for the protection of personal data in future trade agreements, one that would embrace the EU’s restrictions on transfers of personal data without jeopardising EU trade policy ambitions. Chapter 5 of the thesis explores, from an EU law perspective, the possibility of reforming the current framework for transfers of personal data outside the EEA in a way more conducive to international trade, whilst keeping within the constitutional boundaries of the EU charter. However before the thesis moves on to those discussions, the next Chapter uses elements of discourse analysis to explicate the role of narratives in the negotiation and interpretation of trade agreements, and how such narratives could affect the baseline between legitimate protection of data privacy, and protectionism in trade adjudication.

2.5 Conclusion

The pivotal role of personal and other data in the global digital economy intensifies the tension between trade liberalisation commitments and the individual rights to privacy and personal data protection. In the EU, where these rights are binding fundamental rights, this tension could result in a catch-22 situation where the EU would have to choose between adhering to its own constitutional framework and fulfilling its trade obligations. This risk of a compliance deadlock is due to the incompatibility of the exceptions – and, more specifically, the necessity tests lying at their core – that the EU law and international trade agreements have designed to prevent the clash between each other’s bodies of rules. This Chapter has argued that to prevent this risk from materialising, a reform of the international trade exception for privacy and data protection and/or the EU’s framework for transfers of personal data is necessary.
3. Privacy protection(ism): the latest wave of trade challenges on regulatory autonomy

3.1 Introduction

Labels and frames certainly matter in public policy discussions. So much so, in fact, that they often dictate the outcome. For example, China has spent billions of dollars a year over the past several years to strengthen its discursive power to shape specific international policy debates, especially in AI, which is an area where countries race for global technological and policy dominance. Similarly, the ‘digital protectionism’ label has been used in the last decade as a tool to gain control in the domain of ‘digital trade’ policy debate in relation to personal data protection, and specifically to influence policy outcomes in the European Union, where privacy and personal data are well protected. Perhaps even too well protected for those whose business models turn on personal data. As already mentioned in the introduction, restrictions on transfers of personal data, such as those adopted by the EU, are increasingly criticised as being protectionist in trade policy conversations.

“‘Protectionism” has become a dirty word.’ Yet, discursively, that is far from

345 Shambaugh (2015), pp. 99, 99–100. China’s diplomatic and development schemes form just one part of a much broader agenda aimed at enhancing its soft power in media, publishing, education, the arts, sports, and other domains. Nobody knows for sure how much China spends on these activities, but analysts estimate that the annual budget for ‘external propaganda’ runs in the neighborhood of $10 billion annually. By contrast, the U.S. Department of State spent $666 million on public diplomacy in fiscal year 2014.

Ibid. See Wang (2015), pp. 172, 173 fn.4. (‘Point 5 in Section 7 of ‘Decision of the Central Committee of the Communist Party of China on Major Issues Pertaining to Deeping Reform of the Cultural System and Promoting the Great Development and Flouring of Social Culture’ states that China needs to “strengthen international discourse power, and properly respond to external world concerns”; see also Turner (2019), pp. 234–235 (citing recommendation III from Chapter 6 of China’s ‘Artificial Intelligence Standardization White Paper’ of January 18, 2018, which advocates ‘promotion of international standardization work on artificial intelligence, gathering domestic resources for research and development, participating in the development of international standards, and improving international discourse power.’) (emphasis added); Lee, (2016), p. 113 (‘Since Xi took over the reins of power in 2013, there have been signs of a shift in China’s foreign policy from one that accommodates the existing international rules to a policy that makes new rules and institutions on China’s terms’).)

346 See, e.g., Dutton (2018) illustrating the global race for artificial intelligence (‘AI’) dominance by the fact that between 2016 and 2018 Canada, China, Denmark, the E.U. Commission, Finland, France, India, Italy, Japan, Mexico, the Nordic-Baltic region, Singapore, South Korea, Sweden, Taiwan, the United Arab Emirates, and the United Kingdom published their strategies on AI.

347 There is no universally-accepted definition of ‘digital trade’. See Aaronson, Leblond (2018), p., 248 (citing López González, Jouanjean (2017), p.6 (defining ‘digital trade’ as encompassing ‘digitally-enabled transactions in trade in goods and services that can be either digitally or physically delivered involving consumers, firms, and governments’.) For the purposes of this thesis, the author will use this term as defined by Aaronson, Leblond, Ibid.

348 See Section 3.3.

349 See Cadwalladr, Campbell (2019) (revealing Facebook’s lobbying around the world, particularly in the United Kingdom, against data privacy legislation).

obvious: in a broader societal context, the term ‘protection’ is often seen in a positive light, especially when it refers to shelter, safety, or harm prevention. But when it comes to protecting privacy and personal data, trade policy and fundamental rights discourses often seem to work on separate, parallel tracks. Paraphrasing Esty, while the word ‘protection’ ‘warms the hearts’ of those seeing data protection and privacy as fundamental rights, it ‘sends chills down the spines of free traders’. 349

This Chapter asks where one should draw the line between protection and (digital) protectionism. Set against a discursive backdrop where the label ‘protectionism,’ or ‘digital protectionism,’ is increasingly used in academic, societal, and political debates to refer to regulation that aims to protect privacy and personal data, 350 this Chapter considers the implications of this distinction for the autonomy afforded to domestic regulators to protect privacy and personal data by international trade rules and the rules’ interpretation. Further, it asks how the framing of the debate on privacy and data protection in terms of (digital) protectionism affects the normative foundations of domestic regulation on privacy and personal data, and the optimal level of privacy and personal data protection.

This Chapter tackles these questions by applying elements of ‘discourse analysis’ 351 methodology, in particular, insights from the work of Michel Foucault on the relationship between discourse and power. 352 According to Foucault, discourse is a ‘system that makes possible and governs’ the formation of knowledge; it predetermines the objects of knowledge, statements, concepts, and theoretical options as well as the rules of their production. 353 Discourse is not determined once and for all – it controls the very production

349 Esty (1994), p. 36 (Emphasising the ‘clash of cultures’ between environmentalists and free traders and noting that ‘the word ‘protection’ warms the hearts of environmentalists but sends chills down the spines of free traders’.)
350 See Section 3.3.
352 Discourse analysis is the study of language-in-use. There are many different approaches to discourse analysis. Some of them look only at the ‘content’ of the language being used, the themes or issues being discussed in a conversation or a newspaper article, for example. Other approaches pay more attention to the structure of language (‘grammar’) and how this structure functions to make meaning in specific contexts. These approaches are rooted in the discipline of linguistics.
Ibid.
We set out with an observation: with the unity of a discourse like that of clinical medicine, or political economy, or Natural History, we are dealing with a dispersion of elements. This dispersion itself with its gaps, its discontinuities, its entanglements, its incompatibilities, its replacements, and its substitutions can be described in its uniqueness if one is able to determine the specific rules in accordance with which its objects, statements, concepts, and theoretical options have been formed: if there really is a unity, it does not lie in the visible, horizontal coherence of the elements formed; it resides, well anterior to their formation, in the system that makes possible and governs that formation. Ibid.
of knowledge at a particular moment in history and can evolve over time. Discourse has the power to 'mediate' the dominant view of what constitutes normality or deviance and to 'produce ... behaviour that is in conformity with the dominant standard of normality or acceptability. Language, as Julia Black puts it, 'frames thought, and produces and reproduces knowledge' and is 'intimately related to power'. The use of language places the production of knowledge in a particular discourse, which defines the meaning of terms according to shared practices in line with the ideologies of the social groups controlling the discourse. In other words, control over a discourse ultimately translates into control over the production of 'truth' at a particular point in time, and allows the suppression of views outside the prevailing discourse. The power of discourse, or discursive power, is often mentioned in academic, political, and journalistic sources in the context of international relations, domestic trade policy formation and the functioning of international organisations. As noted above, states (or governments) use discursive power to advance certain narratives and to shape international discourses and rules on particular topics. In a narrower sense, discourse can also be controlled by 'disciplines,' that

According to Foucault, '[I]n every society the production of discourse is at once controlled, selected, organised and redistributed according to a certain number of procedures, whose role is to ward off its powers and its dangers, to gain mastery over its chance events, to evade its ponderous, formidable materiality'. Foucault (1971b), p. 52. See also Black (2002), p. 168.

Foucault, for example, whose influence is strong, conceptualized discourse as a group of statements that provided the rules for representing the knowledge about a particular topic at a particular historical moment. Discourse is about the production of knowledge, and itself produces the objects of our knowledge. It governs the way that a topic can and cannot be meaningfully talked and reasoned about, and influences how ideas are put into practice and used to regulate the conduct of others. Neither contends that nothing exists outside of discourse, that things do not have a real, material existence in the world, but rather that nothing has any meaning outside of discourse. Ibid.

See also Lesser (2006), p. 285 (defining discourses as 'systems of thoughts composed of ideas, attitudes, courses of actions, beliefs and practices that systematically construct the subjects and the worlds of which they speak'.)

See Foucault (1971a), p. 73.

As a group of rules for a discursive practice, the system of formation is not a stranger to time. It does not concentrate everything that may appear through an age-old series of statements into an initial point that is, at the same time, beginning, origin, foundation, system of axioms, and on the basis of which the events of real history have merely to unfold in a quite necessary way. A discursive formation, then, does not play the role of a figure that arrests time and freezes it for decades or centuries; it determines a regularity proper to temporal processes; it presents the principle of articulation between a series of discursive events and other series of events, transformations, mutations, and processes. It is not an atemporal form, but a schema of correspondence between several temporal series. Ibid.


is, by the social groups practicing such disciplines.\textsuperscript{361}

Julia Black’s work shows that discourse forms the basis of regulation in several respects: it influences regulation by, \textit{inter alia}, defining the problem and its operational categories; it determines the goals that regulation aims to achieve; and it ‘produces shared meanings as to regulatory norms and social practices which then form the basis for action (for example, the formation of regulatory interpretive communities).’\textsuperscript{362} The use of elements of discourse analysis in this Chapter, aims to show how and why the definition of ‘protectionism’ came about, and how the interpretation of the legal norms embedding this term in the body of international trade law have evolved over time. This is especially pertinent as international trade rules are often phrased in broad and ambiguous terms,\textsuperscript{363} which are operationalised through the interpretation of adjudicating bodies (in case of WTO law, by the WTO Panels and Appellate Body).

The Chapter makes two arguments. First, it argues that ‘protectionism’ is not endowed with an inherent meaning but is socially constructed by the power of the discourse controlling the negotiation, application, and interpretation of anti-protectionist international trade policy and rules. It explicates how shifts in the discourse dominating the negotiation and interpretation of trade law have, in the past, resulted in redefining protectionism as ‘new protectionism’. Such redefinition, in turn, triggered the expansion of the scope of domestic policies viewed as protectionist by international trade institutions and elites and the shrinking of domestic autonomy to regulate in the public interest. By extrapolating these historical insights to current policy conversations surrounding digital trade negotiations by the European Union and the United States (referred to in this Chapter as ‘digital trade’ discourse(s)), this Chapter shows that, despite the fact that the rhetoric of both the EU and the US on this issue are centred are around the same term, ‘digital protectionism,’ the trading partners advance different discourses based on diverging values, which translate to a different baseline between privacy and data protection, and protectionism. Second, this Chapter contends that coining the term ‘digital protectionism’ to refer to domestic information governance policies that are not yet fully covered by trade law disciplines is \textit{not a logical step} to respond to objectively changing circumstances, but a \textit{product of a certain dominant economic ‘digital trade’ discourse}, advanced, in particular, by the United States.\textsuperscript{364} This Chapter demonstrates how the shift from ‘protectionism’ to

\textsuperscript{361} Foucault (1971b), pp. 59–60. By ‘discipline,’ Foucault meant ‘a domain of objects, a set of methods, a corpus of propositions considered to be true, a play of rules and definitions, of techniques and instruments’. \textit{Ibid.} According to Foucault, a discipline controls the production of discourse by recognising true and false propositions within itself, thus pushing back ‘a whole teratology of knowledge beyond its margins’. \textit{Ibid.}

\textsuperscript{362} Black (2002), pp. 165, 178, 188.

\textsuperscript{363} See Section 3.2.

\textsuperscript{364} This discourse is discussed in more detail in Sections 3.3.1 and 3.3.2.
‘digital protectionism’ in this particular discourse has already resulted in the adoption of international trade rules further restricting domestic autonomy to protect the rights to privacy and the protection of personal data.\footnote{For a discussion, see Section 3.3.4.}

This Chapter also suggests that the discourse controlling regulatory conversations on privacy and personal data protection predetermines the baseline between data privacy protection and protectionism and, as a result, affects the level of such protection considered to be necessary and legitimate from a trade perspective. The dominant economic discourse, in particular advanced by the US, internalises an economic approach to personal data and the protection of data privacy.\footnote{By an economic approach to personal data and the protection of data privacy this thesis understands the law and economics approach, which focuses on economic costs and benefits of personal data protection, and does not take full account of protection of personal data as moral value or value in itself. For a more elaborate discussion, see Section 3.4.} From that perspective, as further discussed in Section 3.4 of this Chapter, personal data is viewed as an economic asset and the extent to which data privacy protection is economically justified is determined against the benchmarks of welfare maximisation and Pareto efficiency. Within that discourse, any protection beyond what is Pareto efficient is viewed as protectionist.\footnote{See Strange (1985), p. 235.} Therefore, conducting policy conversations on domestic regulation protecting privacy and personal data within the boundaries of a purely economic ‘digital trade’ discourse puts such regulation in an \textit{a priori} defensive position.\footnote{See, e.g., Bauer, Erixon, Krol, Lee-Makiyama (2013), pp. 4–9, 20–21.} In contrast, within a pluralist discourse, the optimal level of protection will be higher.\footnote{See, e.g., Schwartz, Peifer (2017), p. 121 (comparing the European Union’s pluralist, fundamental rights-based approach to data protection with the United States’ consumer-based approach).} For the purposes of this thesis, a pluralist discourse is understood as a discourse which accommodates a broad range of potentially conflicting perspectives, and which, in particular, internalises economic and non-economic grounds for protecting privacy and personal data as fundamental rights.\footnote{See Twining (2010), p. 494.} As a result, some of the policies viewed as protectionist in the economic digital trade discourse will be viewed as protection. Figure 2 illustrates this point:
Against this backdrop, this Chapter asserts that countries should be conscious of the value frameworks that come with a certain discourse and should ensure that their mutual values determine such discourse, as opposed to the other way around.

As already mentioned in the introduction to this thesis, on 25 January 2019, seventy-six members of the WTO launched talks on electronic commerce, which, among other things, will cover rules on cross-border flows of data.\(^{371}\) This multilateral dialogue, having emerged within the discourse(s) of digital trade, aims at ‘long-standing, high-standard trade principles to digital trade’.\(^{372}\) The parties to these negotiations include countries and regions that have different domestic policy priorities and that are situated at different levels of the ladder of economic development — Australia, China, the European Union, Japan, New Zealand, the United States, and Russia are examples.\(^{373}\) This Chapter suggests that the parties to this multilateral effort should not proceed from the dominant discourse of digital trade as a starting point. Instead, first and foremost, the parties to the effort should agree on the goals of the international trading system in the digital age and the place

---

\(^{371}\) See European Commission, 76 WTO Partners Launch Talks on E-Commerce, 25 January 2019; Botwright (2019); Foroohar (2019); See also Behsudi (2019) (indicating that e-commerce talks are likely to take a very long time).

\(^{372}\) Botwright (2019).

afforded to essential domestic policy goals in this system. Negotiations conducted within a discourse based on such a mutual understanding would have a much higher chance of producing meaningful results.

This Chapter proceeds as follows. Section 2 focuses on the most important milestones in the evolution of the notion of ‘protectionism’, from the mid-eighteenth century until the early twenty-first century, using the lens of discourse analysis. Section 3 introduces the way in which the discourse of digital trade labels restrictions on transfers of personal data (such as those adopted by the EU), as ‘(digital) protectionism’. Then it extrapolates the logic of the reconstruction of the term ‘protectionism’ in the past on the claims to redefine ‘protectionism’ as ‘digital protectionism’. Section 4 explicates how such discourse affects the baseline between data privacy protection and protectionism and influences the right normative rationale behind the regulation of privacy and personal data protection.

3.2 The expansion of the notion of ‘protectionism’

Although the notions of ‘free trade’ and ‘protectionism’ are among the oldest in economics, there is still no uniform understanding of what constitutes ‘protectionism’. This Section analyses of the notion of protectionism and shows that protectionism is not a natural phenomenon – it is a concept socially constructed within a particular discourse.

The core issue in defining protectionism is where to draw the line between regulation that is a precondition for trade (such as state intervention aimed at correcting market failures, which is economically efficient and socially productive), and protectionist regulation which creates market failures and stifles trade. As Bhagwati, one of the leading twentieth-century trade theorists, noted,

[S]ince all policies will inevitably affect (directly or indirectly) comparative advantage and (in this sense) there is therefore no purely ‘natural’ or ‘market-determined’ comparative advantage, where should one draw the line and say that autonomy in this set of policies is fine but not in others?

Eleven years later, Howse argued along similar lines that “[t]here is no natural or self-evident baseline or rule that can solve this basic dilemma.” Defining what constitutes a precondition for free trade and what is a barrier to trade is, indeed, ‘an

---

interpretive act,’ to use the terminology of Lang. As Tarullo explained, determining what constitutes a trade barrier and what does not, depends on the assumption of “normal” conditions of competitive markets’ that is used as a benchmark to identify the deviations. It is the discourse that predetermines what Lang calls ‘collective habits of interpretation’ or ‘the characteristic mindsets and ways of thinking’ and ultimately influences the definition of ‘normal’ market and protectionism. In other words, defining protectionism is an act of interpretation that occurs within a certain discourse. Using a particular theoretical construction of protectionism has two important practical implications. First, such a construction informs the design of international trade rules - an example of this would be the non-discrimination provisions found in current international trade agreements. Second, since these provisions are often phrased in broad and ambiguous terms, which are neither explained nor defined in the agreements, interpretation by adjudicating bodies plays a crucial role in recognising particular domestic policies and rules as ‘legitimate’ or ‘protectionist’. Hence, non-discrimination provisions will be interpreted in a broad or narrow sense, largely under under the influence of the discourse governing such interpretation.

Against this backdrop, this Section shows how shifts in the dominant economic discourse have affected the redefinition of the notion of protectionism. It also demonstrates

---

379 See Lang (2011), pp. 169–170. Since virtually every conceivable form of governmental action has some direct or indirect impact on trade, the selection of a particular set of measures as ‘barriers to trade’ involves the application of principles of selection and categorization. Similarly, we draw distinctions between government actions which constitute trade ‘distortions’ on the one hand, and other kinds of government actions which correct pre-existing market distortions on the other. Ibid., p. 170.

380 Tarullo (1987), p.549 (discussing trade laws of general application). These statutes are based on a regulatory model that assumes that deviations from market principles are ‘exceptional events’; they correct deviations from market principles by imposing extra duties to raise the low prices of imports to what they would (hypothetically) have been had the foreign producer been operating under ‘normal’ conditions of competitive markets and non-distortion by government. Ibid.


382 Ibid., p. 173.

383 See, e.g., Art. 1(1), GATT 1947 (non-discriminatory most-favored nation provision); Art. 301(2) NAFTA (non-discriminatory national treatment provision).

384 See Tarullo (1985), pp. 535–536 (arguing that ‘legal principles are generally indeterminate’ and that ‘[p]olitical or ideological choices are embodied in doctrines that promise a faithful implementation of the principles themselves’.) Using Article I of the GATT, which codifies the principle of non-discrimination in international trade, Tarullo illustrates that the non-discrimination principle ‘cannot be administered without political choices about legitimate national policies [and] the rule cannot be explained or justified simply by reference to the aim of increased trade or the principle of equality’. See ibid., pp. 536–541.

385 See, e.g., Howse (2016), p. 47 (‘The text of the national treatment provisions of the GATT requires that the adjudicator decide whether less favourable treatment is provided for ‘like’ imported products and/or, in the case of taxation measures only, whether dissimilar treatment is provided for directly competitive and substitutable products.’)
how such a redefinition has influenced the substance and interpretation of international trade rules, which ultimately transformed the very goal of the international trade system – from economic stability to liberalisation of trade. This transformation has led to a shrinking regulatory space left to domestic legal regimes by international trade rules. It is, however, not the purpose of this Section to provide a comprehensive account of all aspects of protectionism in a historical perspective. Instead, this Section focuses on the key milestones of the evolution of protectionism in order to illustrate how the boundaries of discourse and its underlying goals and values affect the predominant conceptualisation of protectionism and the functioning of the international trading system. It starts in the mid-eighteenth century with the birth of the classical free trade movement, moves forward to the 1940s and the formation of the first multilateral trading system, and ends with a discussion of the neoliberal discourse which originated in the late 1960s. Before moving on to a historical account of the evolution of protectionism, however, the following Section introduces the key disagreements on the notion of protectionism that weave their way throughout the discussion.

### 3.2.1 Defining protectionism: key disagreement

Historically, the main disagreement in understanding what protectionism is, lies in the determination of whether protectionism is a subjective or an objective notion. This general disagreement is apparent in the question of whether the regulatory intent underlying a domestic regulatory measure that discriminates against foreign competitors matters for the purpose of qualifying such a measure as protectionist. Related questions are how much or how little protection of domestic industries is sufficient to render regulation protectionist and who bears the burden of proof that a particular regulation is protectionist: the foreign state affected by the measure or the state that has adopted the regulation? As this Chapter shows, the answer to these questions has a profound effect on the breadth of the regulatory autonomy left to domestic regulatory regimes by international trade law in order to pursue important societal or public policy objectives, such as protection of human health, the environment, and public morals.

An objective approach to defining protectionism captures a much broader range of

---

386 Compare Sykes (1999), p. 3 (taking an objective approach to protectionism; defin[ing] ‘regulatory protectionism’ as any cost disadvantage imposed on foreign firms by a regulatory policy that discriminates against them or that otherwise disadvantages them in a manner that is unnecessary to the attainment of some genuine, nonprotectionist regulatory objective’; specifically underscoring that in order to qualify as protectionist such regulatory policy ‘need not be deliberate and may result simply from regulators’ failure to appreciate the trade impact of their policies’) (emphasis added), with Irwin (1996), p. 5 (defining a policy of protection as governmental policies discriminating against imported goods ‘in favor of those produced within the country, usually with the aim of sheltering domestic producers from foreign competition through tariffs, quantitative restrictions, or other import barriers’) (emphasis added). While the definition of Sykes puts an emphasis on the effects of a regulatory policy, that of Irwin focuses on the aim of such policy.

387 See Sections 3.3.5, 3.4.
regulatory measures, namely any measure that may de facto result in discrimination between domestic and foreign firms irrespective of its aim, even if such discrimination is incidental.\textsuperscript{388} An objective approach also tends to impose the burden of proving that regulation is not protectionist on the party that has adopted the regulation.\textsuperscript{389} The subjective approach, in contrast, only covers regulation intending to shelter domestic markets from foreign competition, and places the burden of proof of such intent on the party alleging the protectionist nature of another party’s measure.\textsuperscript{390}

3.2.2 Protectionism and the classical free trade idea

As a driver of policy, free trade dates back to the classical doctrines based on the theories of absolute and comparative advantage developed by Adam Smith and David Ricardo, who argued that, just like individuals, countries could gain from international trade by exchanging goods that each country can produce at a lower cost.\textsuperscript{391} As summarised by Irwin, ‘free trade describes a policy of the nation-state toward international commerce in which trade barriers are absent, implying no restrictions on the import of goods from other countries or restraints on the export of domestic goods to other markets.’\textsuperscript{392} While free trade is associated with efficiency gains, barriers to trade are seen as sources of lost gains from trade.\textsuperscript{393} The main benchmarks around which classical economic discourse on free

\textsuperscript{388} See Sykes (1999), pp. 3–4 (providing examples of ‘facially neutral regulation[s]’ that instituted not de jure but de facto discrimination, for example, a pharmaceutical regulation ‘requir[ing] foreign pharmaceutical manufacturers to engage in more testing and clinical trials than domestic manufacturers with no apparent health justification for this difference in treatment’.)

\textsuperscript{389} See, e.g., Lang (2011), pp. 268–269 (illustrating WTO panel cases that exemplify how the country that has adopted the challenged regulation has had to show that the regulation is not protectionist, for example, one case regarding Thailand’s ‘import restrictions and internal taxes on imported cigarettes’ and another case regarding France’s ‘ban on products containing asbestos for public health reasons’).

\textsuperscript{390} See, e.g., ibid., pp. 211–214 (illustrating WTO panel cases in which the challenging country had to argue why the other country’s measures were intentionally discriminatory and thus illegitimate, for example, one regarding a Pakistani challenge to an Indian measure that Pakistan believed intentionally discriminated against Pakistan, and another regarding a Danish and Norwegian challenge to a Belgian measure that Denmark and Norway believed intentionally discriminated against Denmark and Norway).

\textsuperscript{391} Smith (1763b), pp. 207, 209 (advocating that eighteenth-century Britain should be ‘a free port,’ government should not interfere in free trade by measures ‘of any kind,’ and ‘free commerce and liberty of exchange should be allowed with all nations, and for all things’.) See also Smith (1763a), pp. 204, 204 (Edwin Cannan ed., Clarendon Press 1869) (‘All commerce that is carried on betwixt any two countries must necessarily be advantageous to both’); Howse (2002), p. 94 (‘The Ricardian theory of comparative advantage dictated the removal of import restrictions in almost all circumstances, regardless of any commitment of one’s trading partners to liberalize their imports’).

\textsuperscript{392} Irwin (1996), p. 5 (emphasis added).

\textsuperscript{393} See Howse (2002), p. 94. Smith and Ricardo were concerned in the first instance to disprove the conventional or established mercantilist view that national wealth was reduced by (unilateral) free trade, and while they had many important reflections on the relationship of wealth to morals and justice, the basic logic of the theory of comparative advantage does not depend on any of those insights.

\textit{Ibid.}

See also Tumlir (1985), p. 4 (‘Protection imposes costs on the trading economies; when trade restrictions begin to multiply among the main markets, the costs are compounded. When restriction nears the extent
international trade revolves, are economic efficiency and welfare. However, focusing primarily on the enhancement of aggregate national wealth, the logic of comparative advantage does not take into account the concerns of distributive justice or morals.

In classical economics, the doctrines of free trade and protectionism are thus fundamentally opposed, as they offer radically different perspectives on the best way to promote a nation’s (and the world’s) welfare: free trade, by maintaining the utmost freedom of trade between the countries, and protectionism (or mercantilism), by restricting imports, promoting domestic industries, and maintaining self-sufficiency from other countries. Developed in the age of the formation of nation-states in Europe, mercantilist theory aimed to strengthen the power of the state and the accumulation of wealth by stimulating exports and limiting imports. The free trade paradigm developed by Smith and Ricardo was used to oppose and then supplant mercantilism, which dominated trade policy in the early eighteenth century. This shift in the dominant economic ideology was not purely a result of progress in economic thought, but a reflection of a “shared vision” among political economists of Britain’s economic future that represented the views of

---

indicated, these costs could be large enough to be considered a major cause of the decline in economic growth.


Debates surrounding the economics of free trade and protection all revolve around the question of efficiency: how does a particular trade policy affect a country’s ability to use its limited resources (in terms of primary factors of production, such as land, labor, and capital) to produce the greatest possible real income, which in turn enables it to procure a larger set of all goods. Ibid.

See generally ibid., pp. 40–41 (providing examples of ‘noneconomic arguments for protection that are a perennial feature of trade policy debates’). ‘Critics of the economic approach frequently contend that the criterion of wealth is too narrowly materialistic and excludes other more important societal considerations’. Ibid.

Overbeek (1999), p. viii (‘[T]he two doctrines of free trade and protectionism are fundamentally opposed.’)

Ibid., pp. 1–2 (‘The two major aims of mercantilist theory and policy were (1) the strengthening of the power of the state (political) and (2) the accumulation of wealth (economic) [M]any of the policy proposals of mercantilist writers consisted of recommendations as to how to stimulate exports and hamper imports’).

See Howse (2002), p. 94 (‘Smith and Ricardo were concerned in the first instance to disprove the conventional or established mercantilist view that national wealth was reduced by (unilateral) free trade’); Schmidtz (2013), p. 378 (‘Smith is remembered as a defender of free trade, but his practical goal was to repudiate mercantilism’s way of protecting domestic industry’); see also Nedzel (2014), p. 306 (‘Adam Smith, in the Wealth of Nations (1776), challenged mercantilism’).

See Nedzel (2014), p. 305 (suggesting the prevalence of mercantilism in the eighteenth century) (‘From the sixteenth to the eighteenth century, it was assumed that the amount of gold and silver amassed indicated a nation’s wealth and power, and that the world’s capital was static.’) Since the GATT was designed to be merely a multilateral treaty, it would be similar to the bilateral treaties that preceded it, but designed to operate under the umbrella of the ITO, when the ITO came into being. The general clauses of GATT were the same as those in the chapter of the draft ITO charter which was devoted to trading rules, which in turn had been heavily influenced by clauses in bilateral trade treaties. Ibid.

See also Lang (2011), p. 28 (referring to the Havana Charter, which was the draft of the ITO).
certain interest groups in Britain at that time.⁴⁰⁰ As Venzke notes,

It is not a coincidence that David Ricardo and others advocated trade liberalization and an international division of labour at a time in which Britain could become the ‘Workshop of the World,’ the centre of valuable production. Members of the British Parliament clearly saw the appeal of free trade so that ‘foreign nations would become Colonies to us, without imposing on us the responsibility of governing them.’⁴⁰¹

3.2.3 Protectionism and ‘embedded liberalism’ of GATT 1947

During the interwar period, protectionism was mostly conceptualised in its narrow form, namely as tariffs, import quotas, and exchange controls.⁴⁰² In addition, protectionism was associated with political nationalism, heavy interference by government in economic life, and the quest for increased self-sufficiency that characterised the developed countries’ domestic policies at the time.⁴⁰³

In 1947, the General Agreement on Tariffs and Trade (‘GATT 1947’)⁴⁰⁴ was signed.⁴⁰⁵ It incorporated the trade policy chapter of the charter of the International Trade Organization (‘ITO’), the treaty establishing an organisation that never saw the light of day.⁴⁰⁶ As a legal instrument, GATT 1947 codified efforts to curb protectionist policy. However, GATT 1947 had broader purposes as well. It was executed to avoid future trade wars (similar to those that occurred in the 1930s, and were, in part, seen as a cause of

⁴⁰⁰ Gomes (2003), pp. 45–46 (‘The attitude to foreign trade encapsulated in the principle of comparative costs sprang not only from developments in economic theory but reflected a ‘shared vision’ among political economists of Britain’s economic future. It so happened that this coincided with the interests of the new and rising industrial bourgeoisie’.) (emphasis added); see also Robinson (1977), p. 1336 (‘When Ricardo set out the case against protection, he was supporting British economic interests.’)


⁴⁰² See, e.g., Eichengreen, Irwin (2010), p. 871 (‘The Great Depression of the 1930s was marked by a severe outbreak of protectionist trade policies. Governments around the world imposed tariffs, import quotas, and exchange controls to restrict spending on foreign goods’.)

⁴⁰³ See Overbeek (1991), p. 633–634 (stating that up to 1939, ‘the belief in political and economic classical liberalism was broken. The prevailing climate of opinion moved increasingly towards a greater role for government, which meant more neo-mercantilism, statism and interventionism’). In the late 1920s and early 1930s, the United States adopted the interventionist New Deal; England ended its free trade policies introduced in the late nineteenth century; Russia, Germany, Italy and Japan ‘adopted totalitarian institutions, subordinating the individual to the state’. Ibid.

⁴⁰⁴ Throughout this Chapter, GATT 1947 refers to the legal text. GATT (without the year) refers to the organization that administered GATT 1947, as well as the agreements and codes that came later, until 1995 when the WTO took over.


WWII);\textsuperscript{407} to preserve international peace; and to prevent the spread of Communism.\textsuperscript{408} The newly created trade rules were not about ‘comparative advantage as such,’ but rather about the avoidance of protectionist \textit{sumnum malum} (or ‘beggar-thy-neighbour’ policies), that is, when trade barriers introduced by one country led to a chain reaction of trade barriers introduced by other states.\textsuperscript{409} In this sense, the post-war trading system only partially remained faithful to the neoclassical free trade idea.\textsuperscript{410}

The discursive foundations of the GATT 1947 were not monochromatic, they were laid as a compromise between two discourses (or ‘philosophies,’ according to Lang)\textsuperscript{411} that influenced its development.\textsuperscript{412} On the one hand, according to the discourse advanced by the United States, protectionism was to blame for the Great Depression of the 1930s and the trade wars that ‘led in a straight line to the outbreak of the Second World War,’ and that discriminatory trade undermined peace.\textsuperscript{413} On the other hand, another discourse advanced by the United Kingdom and influenced by Keynesian thinking emphasised the boundaries that the international trade regime should not cross in relation to domestic policies affecting trade: in particular, the discourse advocated that an important aspect of an international trade regime is the ability of the state to impose trade restrictions to ensure full employment

\textsuperscript{407} See Irwin, Mavroidis, Sykes (2008), pp. 5–6. To understand the origins of the GATT, one must appreciate the traumatic events of the 1920s and 1930. Although monetary and financial factors were primarily responsible for allowing the recession to turn into the Great Depression of the early 1930s, the spread of trade restrictions aggravated the problem. The commercial policies of the 1930s became characterized as ‘“beggar-thy-neighbor” policies because many countries sought to insulate their own economy from the economic downturn by raising trade barriers. \textit{Ibid.}

See also Lang (2011), pp. 196–197 (‘GATT was in part understood as a way of maintaining Western unity during the Cold War, by placing it on a firm and stable economic footing The fundamental and primary purpose of the post-war regime was international stability, in the specific sense of preventing a repeat of the disastrous trade wars of early 1930s.’); Howse (2022) pp. 94–95 (‘A paramount goal is the avoidance of a protectionist \textit{sumnum malum}—the situation where domestic social or economic pressures lead some states to increase or reinstate barriers to trade, thus triggering a competitive reaction in kind by other states, and eventually a “race to the bottom” that is disastrous for the global economy.’)


\textsuperscript{409} Howse (2002), p. 103 (‘After all . . . trade law in its original postwar form was not about comparative advantage as such, but about constraining destructive interdependence—of which a race to the bottom is one form’. See \textit{ibid.} pp. 94–95; see also Lang (2011), pp. 190–192.

\textsuperscript{410} See Howse (2002), pp. 94–95 (discussing how international trade law was not only concerned with ‘the classic insights about the gains to wealth and welfare from free trade,’ but also the ‘interdependency of different states’ trade and other economic policies …’). ‘The postwar trade and financial order was therefore mainly designed to enable states to manage their domestic economies, in a manner consistent with political and social stability and justice, without the risk of setting off a protectionist race to the bottom’. \textit{Ibid.}

\textsuperscript{411} Lang (2011), p. 192. There were, broadly speaking, two ‘philosophies’ which emerged at this time, with somewhat different interpretations of the causes and consequences of commercial policy during the 1930s, and different prescriptions for the post-war trading order \textit{[B]oth of these philosophies had an important influence on the post-war GATT regime. \textit{Ibid.}}

For further discussion, see \textit{ibid.} pp. 24–29 and 192–194.

\textsuperscript{412} See \textit{ibid.}, p. 192.

\textsuperscript{413} See \textit{ibid.}, p. 192–193.
and domestic economic stability. The delicate compromise between these two views shaped the discourse of ‘embedded liberalism’ – a term coined by Ruggie, which he described as follows:

The essence of embedded liberalism … is to devise a form of multilateralism that is compatible with the requirements of domestic stability. Presumably, then, governments so committed would seek to encourage an international division of labor which, while multilateral in form and reflecting some notion of comparative advantage (and therefore gains from trade), also promised to minimize socially disruptive domestic adjustment costs as well as any national economic and political vulnerabilities that might accrue from international functional differentiation. However, as neoclassical trade theory defines the term, the overall social profitability of this division of labor will be lower than of the one produced by laissez-faire. (emphasis in the original)

Hence, contrary to the (neo)classical case for free trade discussed above, the discourse of ‘embedded liberalism’ leaned towards the subjective – and, therefore, narrower – understanding of ‘protectionism’. This matters because ‘embedded liberalism’ was not only reflected in the characteristics and design of the GATT 1947, but it also governed the GATT 1947’s operation for at least two decades after its inception. Put another way, during that period, trade liberalisation was less important as a goal in itself, it was a component of a broader societal goal of maintaining economic

---

414 See ibid., p. 194.
415 See ibid.
416 Ruggie (1982), p. 392 (‘The liberalism that was restored after World War II differed in kind from that which had been known previously. My term for it is “embedded liberalism”’). (emphasis added).
417 Ibid., p. 399 (emphasis altered).
418 See Irwin (1996), p. 5 (defining the subjective understanding of protectionism) (defining a policy of protection as governmental policies discriminating against imported goods ‘in favor of those produced within the country, usually with the aim of sheltering domestic producers from foreign competition through tariffs, quantitative restrictions, or other import barriers’) (emphasis added).
419 See Lang (2011), p. 195 (‘Key players in the negotiations shared a common view of the legitimacy of state intervention to secure domestic stability, even if they disagreed on the precise form and depth that that intervention should take in particular circumstances’); see also Howse (2002), pp. 94–95.
420 See Lang (2011), p. 205 (‘These shared ideas were reflected in a set of characteristic institutional forms, social practices, and legal structures which more or less endured over the first two decades of the GATT’s existence’). These ‘shared ideas’, however, represented the compromise of the Global North and did not factor in the views of countries from the Global South, such as India. Instead of being normalized, Global South countries’ preferences were framed as ‘special and differential treatment’. See also Lamp (2015), pp. 745–752, 770.
stability.⁴²¹ Although the non-discrimination provisions of the GATT 1947 were formulated broadly,⁴²² in the first two decades of the GATT 1947’s existence and the dominance of the discourse of ‘embedded liberalism,’ they were interpreted narrowly.⁴²³ Only those discriminatory measures that were ‘explicitly or implicitly motivated by a protectionist intent’ were considered to violate the non-discrimination provisions and thus qualified as protectionism.⁴²⁴ In other words, the subjective view based on regulatory intent had legal significance in the assessment of the protectionist character of a domestic measure challenged under the GATT 1947.⁴²⁵

The discourse of ‘embedded liberalism’ – reflecting the broad consensus on the goals of the multilateral trading system – also governed the practice of challenging other countries’ domestic regulations.⁴²⁶ In the first decades after the GATT 1947’s formation, domestic policies that only indirectly intervened with international trade typically were not challenged as inconsistent with international trade rules.⁴²⁷ In line with this consensus, contracting parties to the GATT 1947 did not resort to trade disciplines in order to ‘reshape

---

[Although the removal of trade barriers was of course an important intermediate purpose of the regime, liberalization was in fact a less important norm during the first two decades of the trade regime’s history than is often assumed. Liberalization was pursued not through the application of a rigid principle, but only as far as states were practically able, and only as far as was consistent with the broader norm of economic stability. *Ibid.*]

⁴²² See *ibid.*, p. 208 (‘It takes only a moment’s reflection to see how broad and intrusive these disciplines had the potential to be.’); see also, e.g., Hudec (1990), p. 121 (stating that paragraph 4 of Article III GATT 1947, which contains a national treatment provision, ‘covered every internal law and regulation affecting commercial movement of goods, an area that is virtually unlimited in scope.’)

⁴²³ See Lang (2011), p. 211 (arguing that orientation towards embedded liberalism ‘produced a field of trade law and policy which was narrowly defined (relative to the present day), focused on tariffs and other kinds of trade measures understood at the time as quantitative restrictions, and unwilling to scrutinize “internal” measures except in the clearest circumstances of circumvention of liberalization commitments’.)

⁴²⁴ See *ibid.*, p. 254 (‘From this perspective, the non-discrimination norm contained in Article III of the GATT is essentially an “anti-protectionism” norm and ought to be applied solely to those internal measures which are expressly or implicitly motivated by a protectionist intent.’) (emphasis added); see also Kurtz (2016), p. 137 (‘GATT members were free to regulate domestically (behind-the-border) as they saw fit to do so. Trade law would only strike down such interventions if poisoned by protectionist animus.’); Howse (2002), p. 97 (‘The notion of “discrimination” against trading partners seems closely linked to the very idea of protectionism, though in some cases one may discriminate for non-protectionist reasons, which is why at least as a preliminary sorting or sifting mechanism, the nondiscrimination norm has a certain durability and putative legitimacy.’)


⁴²⁶ See Ruggie (1982), p. 399 (describing the ‘essence of embedded liberalism’); Lang (2011), pp. 195, 205, 211 (arguing that orientation towards embedded liberalism ‘produced a field of trade law and policy which was narrowly defined (relative to the present day), focused on tariffs and other kinds of trade measures understood at the time as quantitative restrictions, and unwilling to scrutinize “internal” measures except in the clearest circumstances of circumvention of liberalization commitments’.) (‘Key players in the negotiations shared a common view of the legitimacy of state intervention to secure domestic stability, even if they disagreed on the precise form and depth that that intervention should take in particular circumstances.’) (‘These shared ideas were reflected in a set of characteristic institutional forms, social practices, and legal structures which more or less endured over the first two decades of the GATT’s existence.’)

⁴²⁷ For a discussion, see *ibid.*, pp. 214–216.
domestic state-market relations’. 428

3.2.4 The new protectionism and the neoliberal discourse: towards an ever-broader conceptualisation of ‘protectionism’

3.2.4.1 The ‘new protectionism’

Starting in the early 1970s, the notion of protectionism has gradually become much more capacious. In trade economics literature, the term ‘new protectionism’ was coined to refer to a broader range of domestic measures restricting international trade. 429 Unlike traditional protectionism, the new version included not only the more traditional or mercantilist restrictions on trade, but also non-tariff barriers (‘NTBs,’ or ‘behind the border’ barriers) to trade, such as negotiated or ‘voluntary’ export restraining arrangements, and measures allegedly abusing the GATT 1947 non-discrimination provisions, such as anti-dumping measures. 430

Trade economists also viewed the ‘new protectionism’ as different in another important respect. 431 While the old protectionism of the 1930s was characterised as ‘unsystematic, improvised, and at the end, a result of panic,’ the ‘new protectionism’ was seen to be driven by strong politically organised forces representing the interests of domestic industries. 432 This approach, as this Chapter shows in greater detail below, had a major impact on the acceptability (under trade law) of key domestic policy measures.

Authoritative trade economists often attributed the rise of non-tariff barriers as a form of circumvention of GATT 1947 disciplines, 433 linked to the tendency of the United States to palliate the decline of its economic dominance (a ‘diminished giant syndrome,’ in the

428 Ibid., pp. 215–216 (‘[T]oo intrusive an application of GATT disciplines on internal regulation would undermine that purpose, as it would run the risk of itself upsetting the delicate balance of concessions embodied in the original agreement, and undermining support for the trading system as a whole.’)
429 See Salvatore (1993), p.1 (Dominick Salvatore ed., 1993) (‘This phrase, coined in the mid 1970s, refers to the revival of ‘mercantilism’ whereby nations, particularly the industrial nations, attempt to solve or alleviate their problems of unemployment, lagging growth, and declining industries by imposing restrictions on imports and subsidizing exports.’)
430 See Bhagwati (1988), pp. 43–53 (conceptualising NTBs in the form of domestic regulation on countervailing duties and anti-dumping provisions that was seen as being restrictively used against foreign suppliers); see also Bhagwati (1991), p. 239 (distinguishing between two classes of non-tariff barriers: 1) barriers bypassing the GATT’s rules, which include visibly and politically negotiated voluntary export restraints and other export restraining arrangements (e.g. import quotas, nonautomatic licensing, and variable levies); and 2) protectionist ‘captured’ provisions that have a legitimate role in a free trade regime (e.g. countervailing duties and anti-dumping provisions) but are used to ‘harass unfairly their successful foreign rivals and thus to deter fair competition and free trade’); Overbeek (1999), p. 555.
432 See ibid. (‘Protectionism in the 1930’s was unsystematic, improvised, and at the end, a result of panic. The new protectionism is a very different animal. It has been growing gradually. Industries have used intelligent, long-term planning in creating an expanded system of protection. [T]he new protectionism is politically stronger because it accommodates a broader range of interests’.)
433 Baldwin (1986), p. 1 (‘The international trading economy is in the anomalous condition of diminishing tariff protection but the increasing use of nontariff trade-distorting measures.’)
words of Bhagwati), and to suppress increasing competition from less developed, newly industrialising countries. A number of those countries imposed barriers to US exports in areas where the United States had a comparative advantage, especially knowledge-intensive industries and services. In addition, new protectionism was viewed as a means of alleviating domestic stability issues, such as growing unemployment and inability, due to economic decline, to deliver on the social obligations of the expanded welfare states. Recall from Section 3.2.3 of this Chapter that it was precisely these measures that were seen as legitimate and not, therefore, protectionist in the ‘embedded liberalism’ discourse.

In the new protectionism, free trade theorists saw a threat to the legitimacy and to the very existence of the multilateral trading system associated with post-war prosperity and economic growth. Recalling the disastrous consequences of protectionism in the 1930s, Bhagwati, one of the most influential trade theorists of the time, warned that the new protectionism would, just like its predecessor, trigger beggar-thy-neighbour policies and result in new trade wars.

3.2.4.2 ‘Fair trade

---

See, e.g., Bhagwati (1993a), p. 22 (‘America has been struck by a “diminished giant syndrome”—reinforced by the slippage in the growth of its living standards in the 1980s. This affliction has caused a loss of confidence in America’s inherited postwar trade policies’); see also Bhagwati (1993b), p. 39 (‘Many of my examples [of demands for fair trade] come from the United States where the diminished giant syndrome has prompted an acute search for unfair trade by others.’)

Baldwin (1986), p. 1, 20 (‘[N]ew nontariff protectionism [is related] to significant structural changes in world industrial production that have brought about a decline in the dominant economic position of the United States, a concomitant rise to international economic prominence of the European Economic Community and Japan, and the emergence of a group of newly industrializing developing countries (NICs)’.)

See Howse (2016), p. 17

Many barriers worldwide hampered America in exploiting its apparent contemporary comparative advantage in knowledge-intensive industries and services. In some, intellectual property was largely unprotected; in most, competition in network services, such as in telecommunications and finance, was severely restricted or limited, while many others still imposed byzantine and archaic regulatory requirements on products, both imported and domestic. In many cases, a business presence in the other country was necessary for the full exploitation of comparative advantage, and here American firms faced severe foreign investment restrictions.


Baldwin (1986), p. 1 (‘[N]ew protectionism is taking place largely outside the framework of GATT and threatens to undermine the liberal international trading regime established after World War II.’) For further discussion, see Bhagwati (1991), pp. 238–244.


The next few years will show whether world trade can continue to survive despite the deadlock in the GATT and despite a certain amount of increased protectionism. My contention is that a combination of political and economic interests, reinforced by structural change in the international division of labor brought about by the mobility of capital and technology, is preventing a world depression from seriously arresting or reversing the steady growth in world trade.

86
The ‘New Protectionism’ in ‘Fair Trade’ Clothing

Alongside the new protectionism discourse within US business and governmental circles during the 1970s, measures characterised as new protectionism were increasingly re-framed as means to curtail ‘unfair trade practices’ from (primarily) developing countries.\textsuperscript{1} From this perspective, trade-restricting practices, such as import controls and voluntary export restraints, labelled as new protectionism by trade economists, were presented as responses to unfair trade.\textsuperscript{2} Implicitly using its domestic market as a primary reference point, the United States used the ‘fair trade’ discourse to argue that any commercially significant institutional or regulatory difference between its domestic regime and that of other countries distorted the conditions of competition and constituted barriers to US exports.\textsuperscript{3} Bhagwati, in contrast, viewed these claims as nothing more than a different rhetoric of protectionist demands in order to make lobbying efforts more successful.\textsuperscript{4}

Guided by the new fair trade narrative, the US government saw the changing mission of international trade law as the elimination of unfair trade practices through, in particular, the harmonisation (or ‘globalisation’) of a broad range of domestic regulatory frameworks

\textsuperscript{1} Subsidies, dumping practices, and other discriminatory rules disfavoring U.S. (and other) imports are examples of such ‘unfair trade practices’. See Baldwin (1986), pp. 16–19; see also \textit{ibid.}, p. 18 (‘The emphasis on the great need for fair trade is evident in the 1974 legislation authorizing U.S. participation in the Tokyo Round of multilateral negotiations’.)(emphasis added).

\textsuperscript{2} See \textit{ibid.}, pp. 18–19

The most important protectionist action taken by the United States since the late 1960’s, namely, the gradual tightening of controls over steel imports, has also been justified mainly on the grounds of unfair trade practices by foreign producers. When a series of voluntary export restraint agreements with leading steel-exporting nations were concluded in late 1984, a spokesperson for the U.S. Trade Representative stated, ‘We are responding to unfair trade in the U.S.; defending yourself against unfair trade is not, in our opinion, protectionism’. The unfair trade argument has been used in support of most other trade-restricting or trade-promoting actions taken by the United States in recent years.

\textsuperscript{3} Lang (2011), p. 227

In practice, when one country alleges that another country’s measure is an unfair trade practice (or trade distortion), it will implicitly use the institutional form of its own domestic market as the primary reference point against which fairness and distortions are measured. . . . The result is that the notion of a ‘trade distortion’ comes to be equated in practice with the existence of a commercially significant institutional or regulatory difference between countries.

\textsuperscript{4} See e.g. Bhagwati (1991), p. 239

[I]f protectionists demand protection, they will today confront politicians who are generally hesitant to supply it because it is not comfortable to be called “protectionist.” However, if you cry “foul” and allege that the foreign rival is resorting to “unfair” trade practices and therefore you need protection, your chances of successful lobbying are much greater. Protectionists have increasingly come to appreciate this and to shift their style of complaints accordingly to “unfair trade”, opening this notion to ever more areas of concern (e.g. workers’ rights enforcement by foreign countries).

See also Bhagwati (1988), pp. 123–124 (‘The insidious growth of the “fairness” issue poses a yet more disturbing threat to freer trade’.)
that affect international trade. Demands for ‘level playing fields,’ ‘harmonisation,’ and ‘fair trade’ more generally worried trade economists, who saw in such demands a threat to the legitimacy and feasibility of free trade: not only did they consider it to be impossible to harmonise every aspect of domestic regulation, but they also argued that it was in these differences between domestic regimes that lay the source of the comparative advantages that make trade beneficial in the first place.

In sum, the ‘new protectionism’ in ‘fair trade’ clothing ‘provided the enabling conditions and leverage for a radical renegotiation of the international rules that had undergirded the profound global economic transformations of the previous era.’

‘Fair Trade’ and the Human Rights Movement

Another, non-economic, strand of the ‘fair trade’ debate dealt with background conditions affecting the cost of production in developing countries, such as environmental and labour standards. As the liberalisation of capital flows allowed multinational

445 Baldwin (1986), p. 18
In reshaping the proposal of the president [for the Tokyo Round of multilateral negotiations], the Congress stressed that the president should seek ‘to harmonize, reduce, or eliminate’ nontariff trade barriers and tighten GATT rules with respect to fair trading practices. Officials in the executive branch supported these directives not only on their merits but because they deflected attention from more patently protectionist policies.

446 See Bhagwati (1993b), p. 18
[T]he true and greater crisis that we face with regard to the theory and policy of free trade today comes . . . from the growth of demand for ‘level playing fields,’ ‘harmonization,’ ‘fair trade,’ etc., all of which are variously undermining insidiously the legitimacy and feasibility of free trade since it is virtually impossible to harmonize everything so that playing fields are truly level in every way. There will always be something that an opponent of free trade will be able to find that is different in the country of one’s successful rival and hence can be argued to make free trade unfair and therefore illegitimate and unacceptable. See also Bhagwati (1991), p. 240
If differences in national institutions and policies can affect comparative advantage, as they surely can, and if these are now increasingly cited as sources of unfair trade (as they are), then we may be seriously eroding the possibility of free trade and leading towards ‘managed trade’ or towards free trade only when a great deal of policy harmonization has occurred (as in the European Community (EC)).

447 Lang (2019), p. 3 (‘What “new protectionism” signaled above all . . . [was] an attempt by many States to rewrite the rules of global trade to establish a new international division of comparative advantage and secure their preferred places in that order . . . . In retrospect, the “new protectionism” is therefore best understood . . . as a successful attempt to transform the system from one type of open global trading order to another.’)

448 See Bhagwati (1996), pp. 10–11 (stating that non-economic fair trade arguments are based on three concerns: a sense of a ‘transborder’ obligation towards others living in nation-states with lowers standards; concerns of distributive justice that amount to the fear that freer trade with poor countries with abundant unskilled labor will immiserate working people in those countries; and concerns of fair competition that require that costs attributed to environmental and labor standards should not differ across countries in free trade.); see also Bhagwati (2007), pp. 133–134; Howse, Trebilcock (1996), p. 74 (1996)
Unlike the arguments for trade restrictions on environmental and labor rights grounds . . . which have a normative reference point external to the trading system itself, competitiveness-based ‘fair trade’ claims focus largely on the effects on domestic producers and workers of
companies from developed countries to move production to developing countries with lower environmental and labour standards, the non-economic fair trade argument raised concerns of a ‘race to the bottom’ of such standards in developed countries.\(^{449}\) To prevent this, proponents of the argument called for the creation of an international ‘level playing field’ and especially with regard to environmental and labour-rights trade measures.\(^{450}\) Just like their economic counterpart, these arguments were attacked by opponents as protectionism in disguise.\(^{451}\) Moreover, even if one views these arguments as not protectionist in nature, addressing non-economic issues through trade measures was perceived as a second-best solution, because the first-best domestic measures are those not interfering with international trade.\(^{452}\)

Although trade theorists advancing the idea of free trade were critical of the fair trade narrative, it would be inaccurate to say that this critique applied to any domestic interference with free trade.\(^{453}\) For example, Bhagwati acknowledged that objecting to any other countries’ environmental and labor policies, and not per se on the effects of those policies on the environment and on workers elsewhere.

See also Wai (2003), p. 48–49 (‘Free trade based on comparative advantage is agnostic about the production conditions in any particular jurisdiction, including its domestic regulatory standards. Fair trade theory, in contrast, is very much concerned with defining the background of those conditions under which international trade should occur. Production that violate these background conditions would constitute “unfair competition”.’) For an overview of non-trade rationales for environmental and labor protection, see Howse, Trebilcock (1996), p. 63–65.

\(^{449}\) See Howse (2002), p. 104

In the wake of the debt crisis, a range of developing countries ended up removing or modifying restrictions on foreign investment and various other domestic policies that were disincentives to the attraction of foreign capital. This led to fears of ‘social dumping’ in the developed world that would eventually cause a race to the bottom: developed countries would not be able to sustain high environmental and labor standards, or rates of taxation needed to finance the redistributive policies of the welfare state, if they had to compete with these poorer countries for the location of capital investment.


\(^{451}\) See, e.g., Bhagwati (2007), pp. 123–131, 147–150 (arguing that the ‘race to the bottom’ argument is not supported by empirical evidence; differences in environmental and labor standards are insignificant to affect the location of production; higher labor and environmental standards themselves can be a protectionist move; and finally, attributing such arguments to ‘rent seeking’.); see also Overbeek (1999), p. 557 (‘At present [(1990s)], protectionists in wealthier countries, who are always on the look-out for new reasons for trade barriers, are using labor and environment related arguments to back up demands for additional trade impediments. … [T]his type of argument is extreme protectionism in its crudest possible disguise.’); Lee (1997), p. 177. But see Ehrlich(2010), p. 1014, 1026, 1029–30 (providing empirical evidence of genuine nature of concerns with environmental and labor standards); Davies, Chaitanya Vadlamannati (2013), p. 11–12 (providing empirical evidence of the race to the bottom in labor standards).

\(^{452}\) See Howse (2002), p. 100 (‘Thus, the notion that a more effective policy instrument than trade protection is always available to achieve any legitimate public end vastly oversimplifies the problem of politics.’) Bhagwati argued that using trade distorting measures to tackle unemployment is only a second-best measure, while purely domestic measures would be the first best solution. See Bhagwati (1991), p. 238. On the theory of second best, see Bhagwati (1971).

state intervention as a departure from fair trade was ‘a wrongheaded’ approach. He also supported some of the ‘fair trade’ arguments insofar as they were focused on the importance of creating intra-sectoral level playing fields – especially in the ‘context of the few technology-intensive industries in which there are significant scale economies relative to the size of the world market. Along the same lines, he called for greater tolerance of ‘other countries’ social objectives’; regulation pursuing such objectives, he argued, should not be labelled as ‘unfair’.

3.2.4.3 Neoliberal discourse

As this Chapter has explicated above, redefining ‘protectionism’ as ‘new protectionism’ was framed as a necessary and logical step in response to new forms of trade barriers. Ruggie convincingly argues instead that the emergence of the new protectionism was not the cause of, but rather the effect of neoliberal discourse, which redefined the social purposes of the international trading system. It was, thus, a new vision of the international trading system dictated by neoliberal discourse, and not objective circumstances, which effectuated the transformation of the notion of protectionism.

This evolution of neoliberal discourse happened against the background of a shift in the economic theory of regulation. A neoliberal view that any regulation may constitute a potential barrier to trade relies to a large extent on the theory of regulatory capture that became ‘common language’ in the circles of trade economists and international lawyers associated with the GATT. These economic theories were later embraced in two official GATT reports. In contrast to public interest theory (which advanced analytical arguments that regulation is adopted in the public interest, primarily to correct market failures and pursue non-economic and societal goals), the ‘regulatory capture’ theory

454 Ibid., p. 126.
455 Ibid., p. 127.
456 Ibid.
460 Ibid., p. 438 (‘During the 1980s, Ordo-liberal and public-choice economics gained influence among trade economists and international lawyers associated with GATT, and ‘capture’ theory became the common language’.)
461 Ibid.
462 See Baldwin, Cave, Lodge (2012), pp. 39–43; Ogus (1994), pp. 58–71. The private interest theory questioned one of the core assumptions of the public interest theory, the assumption of the ‘benevolent regulator,’ in other words, that the political process creating regulation is efficient. See, e.g., Stigler (1971), p. 3 (‘The second [alternative] view of regulation is essentially that the political process defies rational explanation: “politics” is an imponderable, a constantly and unpredictably shifting mixture of forces of the most diverse nature, comprehending acts of great moral virtue (the emancipation of slaves) and of the most vulgar venality (the congressman feathering his own nest”.)
(based on the empirical foundations of the public choice theory) argued that regulation is adopted and implemented primarily in the interest of organised interest groups, and that regulatory capture is essentially unavoidable. Captured regulation leads to a reduction of social welfare because it merely leads to the transfer of wealth from one industry to another and no longer serves public interest. This explains why, from the perspective of this theory, regulation should be reduced to a minimum.

This theory was also used as a justification of the aggressive pursuit of export interests on the international level for constraining domestic protectionist trade policy making. Binding reciprocal trade rules were thus seen as a tool to contain domestic protectionism through what Baldwin calls a 'juggernaut effect,' which is using domestic export-oriented groups who profit from a reduction of trade barriers to fight the domestic protectionist lobby. The new approach to domestic regulation was reinforced by a somewhat simplified version of trade economics that 'professors dole out to journalists' (a 'market fundamentalist ideology' rather than the true economic science). Proponents of this ideology argued that trade leads to efficiency gains and enhances domestic welfare, while

464 Political economists developed sophisticated models based on empirical data that strongly suggested that not only elected political actors but also non-elected bureaucrats (especially in the case of the European Economic Community) were more prone to adopt protectionist regulation than to adhere to free market principles. See Messerlin (1981), pp. 469–71. But see Baldwin (1989), p. 131 (‘[T]he individual’s various social concerns can play an important role in shaping his or her decisions. To expand their already substantial contributions toward understanding the policymaking process, economists should integrate such social motivations into their microeconomic optimizing framework’.)
465 See e.g., Tumlir (1985), p. 4 (arguing that ‘[a]ll protection is a redistribution of income and wealth within the protecting country’); see also Overbeek (1999), p. 558 (discussing the policy of managed trade).
466 See e.g., Sunstein (1993), p. 70 (criticising the capture theory). Sunstein states that, ‘[T]he notion of rent-seeking rejects, as unproductive, nearly all of the basic workings of politics. It treats citizenship itself as an evil. Efforts to enact public aspirations, to counteract discrimination, to protect the environment—all these are seen as the diversion of productive energies into a wasteful place’. Ibid., p. 71.
467 Lang (2011), p. 234 (‘As regards the trade regime itself, public choice theory supported the view that aggressive championing of export interests through trade negotiations was generally beneficial, as it provided a counterweight to the inherent tendency of protectionist special interests to capture domestic trade policy-making processes’.)
469 See Rodrik (2011), p. 77

Free market economics was in the ascendancy, producing what has been variously called the Washington Consensus, market fundamentalism, or neoliberalism. This new vision elevated the simplistic case for trade—the one that economics professors dole out to journalists—over the appropriately qualified version. It regarded any obstacle to free trade as an abomination to be removed; caveats to be damned.

see also Driskill (2012), p. 2 (‘[I]n light of the apparent settled nature of economists’ judgement on the issue of trade liberalization, the profession has stopped thinking critically about the question and, as a consequence, makes poor-quality arguments justifying their consensus’.)
470 Stiglitz (2018), p. xl (‘Doubling down on the Washington Consensus was a policy inspired by the special interests that it served, but the belief in the efficacy of these policies was supported by “market fundamentalist” ideologies—the notion that free, unregulated markets were the best way to organize a society’.) (emphasis added).
silencing the downsides, such as the lack of consideration of social or distributional effects of free trade policy.\textsuperscript{471} Relying on the assumption that any public policy objective can be more efficiently achieved by domestic regulation not interfering with international trade, this approach judged domestic trade restrictive measures against the benchmark of an imaginary ‘toolbox of effective nontrade policy instruments’.\textsuperscript{472} This perspective was also reinforced by the predisposition that protectionism explains domestic rules that deviate from this benchmark of efficient domestic rules.\textsuperscript{473}

Taking an opposite view, Stiglitz argued, that ‘[t]he globalization which emerged at the end of the twentieth century and the beginning of the twenty-first was not based on “free trade,” but managed trade—managed for special corporate interests in the United States and other advanced countries.’\textsuperscript{474} The ‘market fundamentalist’ ideologies that created a presumption that ‘free, unregulated markets were the best way to organize a society’ reinforced the myopic focus of political economy theory on the failures of domestic regulation.\textsuperscript{475} Paradoxically, a policy of deregulation (or not adopting regulation in the first place) and of complete free trade is a type of domestic policy, which itself is prone to ‘capture’ by domestic interest groups that benefit from such policies.\textsuperscript{476} This led to questions about why international trade law regulation would be immune to such capture.\textsuperscript{477} To illustrate this line of reasoning, an argument can be made that some countries, such as the United States, set their data protection standards strategically low in order to increase their competitiveness on a global digital market.\textsuperscript{478}

3.2.4.4 The impact of neoliberal discourse on the formation and functioning of the international trading system

Neoliberal discourse had a profound impact on the further rounds of negotiations of the GATT, in particular, the Uruguay Round (1986-1994) that led to the creation, design

\textsuperscript{471} See Howse (2002), p. 99 (‘Put in this crude way, the case for trade liberalization appeared to be totally indifferent to any notion of a just distribution of benefits and burdens from the removal of trade restrictions.’)
\textsuperscript{472} Ibid., p. 100 (‘One simply assumed a certain toolbox of effective nontrade policy instruments, and the stability and viability of the social bargains within states as well, or at least the stability of institutions that construct and reconstruct such social bargains.’)
\textsuperscript{473} See ibid. (‘In its confidence in the prescription of free trade as a timeless truth, the network identified special interest groups as the evil force that explained all, or almost all, deviations from the clearly rational policy prescription to use nontrade instruments for achieving public policy goals.’)
\textsuperscript{474} Stiglitz (2018), p. 20.
\textsuperscript{475} See ibid., p. xl.
\textsuperscript{477} See ibid.
\textsuperscript{478} See, e.g., Greenleaf (2012), p. 72 (characterising the U.S. privacy standards as inherently or deliberately weak). ‘[A]ttempts by US companies and the US government to use their combined economic and political influence to limit the development of data privacy laws in other countries will continue to be important, but may now be on the wrong side of history’. Ibid.; see also Azmeh, Foster (2016), p. 12 (‘Over the last few years, the political role of ICT companies has increased substantially with some of these firms becoming key political lobbying forces’.)

92
and functioning of the WTO. The conclusion of the WTO Agreement led to a considerable expansion of the scope of the multilateral trade system.\textsuperscript{479} The WTO Agreement not only incorporated the GATT 1947,\textsuperscript{480} but also introduced new international trade law disciplines on the international trade in services in the GATS, technical standards,\textsuperscript{481} sanitary and phytosanitary measures,\textsuperscript{482} and intellectual property.\textsuperscript{483} Another important outcome of the Uruguay Round was the creation of a binding dispute settlement mechanism.\textsuperscript{484}

During the Uruguay Round, ‘a specialised policy elite’– employees of the GATT/WTO secretariat and a broad range of ‘experts’ – took over the gradual development and administration of the multilateral trading system.\textsuperscript{485} These elites were ‘insulated from, and not particularly interested in, the larger political and social conflicts of the age’\textsuperscript{486} and shared a common set of neoliberal normative values (ethos or ideology) on the nature and goals of international trade, the relationship between trade law, and politics and the boundaries of domestic regulatory autonomy.\textsuperscript{487} The main goal of the international trading

\textsuperscript{479} Howse (2002), pp. 17, 53–54 (showing that the U.S. fair trade agenda became the core of the Uruguay Round, which lead to the adoption of trade disciplines implementing the rules dictated by ‘the predominant ideology represented by the Washington consensus’: extension of disciplines on domestic regulation beyond GATT non-discrimination obligations, greater market access, expansive intellectual property protection, de-monopolization and deregulation of telecommunications and finance, and ‘scaling down’ governmental health, safety and environmental protection).

\textsuperscript{480} GATT 1994 (incorporating almost all of the provisions of GATT 1947).

\textsuperscript{481} TBT Agreement.

\textsuperscript{482} SPS Agreement. Kurtz notes in relation to the SPS that it ushered ‘in a harder positive integration edge to a member state’s commitments in the WTO. The underlying logic is that, by flattening insensible regulatory variances between states, the SPS Agreement can lower compliance costs, enhance efficiency gains and thus lead to an overall improvement in economic welfare’. Kurtz (2016), p. 138.

\textsuperscript{483} TRIPS. See also Gervais (2010), p. 3.

\textsuperscript{484} Although there was a dispute settlement mechanism under the GATT 1947, the decision of the dispute settlement body (‘Panel’) had to be adopted by a consensus, which, in practice, meant that a losing party could block the adoption of the decision against it. Jackson (1998), p. 68. Establishment of the Dispute Settlement System solved this problem. The Dispute Settlement System is embodied in the DSU; see Jackson (1998), pp. 72–73; see also Vermulst, Driessen (1995), p. 131 (providing an overview of the WTO dispute settlement system).

\textsuperscript{485} Howse (2002), p. 98

This group included some officials employed in the GATT/ WTO Secretariat . . . the larger group of ‘experts’: former or current governmental trade officials; GATT-friendly academics who often sat on GATT/WTO dispute settlement panels and were invited to various conferences and meetings of the GATT/WTO; international civil servants in other organizations (particularly the World Bank, the Organisation for Economic Co-operation and Development, and the International Monetary Fund) preoccupied with trade matters; and a few private attorneys, consultants, and former politicians.

\textsuperscript{486} Ibid. (‘A sense of pride developed that an international regime was being evolved that stood above the madhouse of politics (if one can borrow Pascal’s image), a regime grounded in the insights of economic ‘science,’ and not vulnerable to the open-ended normative controversies and conflicts that plagued most international institutions and regimes, most notably, for instance, the United Nations’.)

\textsuperscript{487} See Lang (2011), p. 181

[Trade regime’s neoliberal turn was in significant part . . . a transformation of collective ideas about the nature and purpose of the trade regime, collective ideas about the function of law in trade politics, and collective principles and techniques for evaluating the legitimacy of

93
system, as advanced by these policy elites, was no longer ‘embedded liberalism,’ but the continued, gradual liberalisation of trade.\footnote{See also Weiler (2001), p. 193 (‘The diplomatic ethos which developed in the context of the old GATT dispute settlement system tenaciously persists despite the much transformed juridified WTO.’).} International trade and globalisation became an imperative for any trade policy measure, subordinated to the domestic economic, social, and political priorities, and an ‘end in itself’.\footnote{See Rodrik (2011), p. 76 (citing Friedman (1999), pp. 61–65) [T]he WTO marks the pursuit of a new kind of globalization Domestic economic management was to become subservient to international trade and finance rather than the other way around. Economic globalization, the international integration of the markets for goods and capital (but not labor), became an end in itself, overshadowing domestic agendas. Globalization became an imperative, apparently requiring all nations to pursue a common strategy of low corporate taxation, tight fiscal policy, deregulation, and reduction of the power of unions. See also Howse (2002), p. 104 (‘[S]ome insiders] moved from free trade as an economic ideology to free trade as embedded in a broader liberal economic ideology. Trade liberalization became part of a general set of prescriptions for growth and prosperity, at odds to a large extent with the progressive welfare state vision of the embedded liberalism bargain’); WTO, Appellate Body Report, EC – Chicken Cuts, para. 243 (stating that security and predictability of ‘the reciprocal and mutually advantageous arrangements directed to the substantial reduction of tariffs and other barriers to trade is an object and purpose of the WTO Agreement, generally, as well as of the GATT 1994’).} Under the influence of these policy elites, the WTO dispute settlement system, which had exclusive competence to enforce WTO rules, became largely ‘self-referential’ and gave little weight to other international rules, such as those governing human rights.\footnote{See Rodrik (2011), p. 76.}

This shift in the dominant discourse affected the behaviour of WTO members.\footnote{Weiler (2001), p. 194 (‘A very dominant feature of the GATT was its self-referential and even communitarian ethos explicable in constructivist terms.’).} Compared to the previous system under GATT 1947, the WTO dispute settlement system was used to challenge a broader range of domestic policy issues.\footnote{See Lang (2011), p. 223.} As a result, in addition to traditional trade-related questions such as tariffs and quotas, WTO dispute settlement bodies increasingly had to evaluate compliance with the new trade rules of domestic health and environment standards, cultural policies, and regulation protecting public morals.\footnote{See ibid., p. 223–224 (‘By the end of the 1990s, however, as informal norms limiting the scope of application of the GATT regulatory disciplines were gradually reconstituted, the range of measures subject to challenge under Articles I and III of the GATT had broadened considerably. It was in part the result of a twofold imaginative change consisting of, first, a redefinition of the common sense concept of “trade barrier,” and second, a rethinking of the nature and purpose of the trade regime itself.’).} In addition to domestic regulation discriminating on the basis of origin (‘de jure discrimination’),\footnote{See e.g. WTO, Appellate Body Report, US-Gambling; WTO, Appellate Body Report, EC – Asbestos; WTO, Appellate Body Report, US – Shrimp; WTO, Appellate Body Report, EC – Hormones; WTO, Appellate Body Report, Canada – Periodicals.} which was a primary matter of concern in the GATT 1947, from the
late 1980s onwards, an increasing number of disputes focused on de facto discrimination. These were the domestic measures that did not specifically aim to discriminate against foreign goods in favour of domestic ones based on their origin, but rather, on a domestic regulatory purpose (e.g. health or environmental protection).495

The WTO caselaw that emerged from these disputes demonstrates a neoliberal shift in the trade adjudicators’ interpretative techniques.496 The WTO adjudicating bodies increasingly refrained from considering regulatory intent when assessing whether a particular domestic measure resulting in discrimination between domestic and foreign goods or services violated the relevant trade agreement and was, therefore, protectionist.497 Instead, the focus shifted towards the economic impact on the competitive opportunities of foreign goods and the effects on competition between products or services.498 These developments led to an equivalence between trade-distorting measures, discrimination, and protectionism.499

This equivalence between discrimination and protectionism had two practical implications. First, it altered the baseline between legitimate regulation and protectionism,

495 See Hudec (1998), p. 620 (defining ‘de facto discrimination’ as ‘regulatory measures that make no explicit distinction between foreign and domestic goods (called “origin-neutral”), but which have a disproportionate impact on foreign goods or services that is for some reason viewed as wrong or illegitimate’). ‘Historically, GATT has been principally occupied with border measures and explicitly discriminatory measures, with de facto discrimination only becoming a major concern relatively recently’. Ibid., p. 622. Hudec clarifies that ‘[o]f the first 207 legal complaints filed in GATT between 1948 and 1990, only a small handful involved claims of de facto discrimination by internal regulatory measures’. Ibid., p. 622 fn.8; see also Diebold (2010), pp. 37–45.
498 See, e.g., WTO, Panel Report, *Argentina – Hides and Leather*, para. 11.182; (clarifying that ‘Article III:2, first sentence, is not concerned with taxes or changes as such or the policy purposes Members pursue with them, but with their economic impact on the competitive opportunities of imported and like domestic products’) (emphasis added); Lang (2011), p. 262; Howse (2016), p. 46: Consideration of regulatory intent or of evidence of purposeful discrimination plays no role in this analysis. The adjudicator makes a determination of whether the products are ‘like’ based upon objective criteria, such as physical characteristics and end uses, while consumer preferences can also be dispositive, and then undertakes a formalistic (not empirical) analysis of whether the regulatory intervention in question has detrimental impact on competitive opportunities for imported like products. In this disparate impact or de facto discrimination analysis, there is no apparent room for consideration of outside values or legitimate regulatory purposes.
499 See Lang (2011), p. 255 (‘[A]n implicit association . . . began to be made between the notion of discrimination under Articles I and III and the notion of a “market distortion” from economic analysis’.) ‘[T]he non-discrimination norm became a much more powerful tool to wield against domestic regulation, even that which was apparently “non-discriminatory” in the sense that that term had been traditionally understood. “Discrimination” began to look very much like “trade-distorting market intervention”’. Ibid., p. 264.
thus making the term protectionism much more capacious. This, in turn, left a much narrower domestic regulatory space to protect non-economic values, such as the environment, labour rights, animal welfare, and human rights. Second, by refraining from any consideration of regulatory intent in the assessment of violations of international trade commitments, the WTO adjudicating bodies transferred the centre of gravity in the consideration of regulatory purposes towards the all-important general exceptions contained in GATT 1994 Article XX and GATS Article XIV.\footnote{See WTO, Appellate Body Report, Argentina – Financial Services, para. 6.114; (‘[A] Member’s commitments under the GATS could in some cases serve to further its national policy objectives. Where measures are found to be inconsistent with a Member’s obligations or commitments under the GATS, the GATS provides for various mechanisms, such as Article XIV, which take account of policy objectives underlying such measures’.)} This shift had an important consequence for the domestic regulatory space: while the burden of proof of an alleged violation of a trade obligation is normally on the complaining party, the burden of proof that all the conditions of a necessity test have been met are on the party whose regulatory measure is contested.\footnote{See Regan (2007), p. 364.} Moreover, this is not just ‘a question of technical burden of proof,’ as Weiler argues, but ‘a question of cultural identity, the way a society wishes to understand its internal hierarchy of values.’\footnote{Weiler (2009), p. 768.} The relegation of values competing with the liberalisation of trade to exceptions, ‘establishes the WTO as a system of symbolic normative hierarchy wherein the default norm is the integrity of the market and liberalized trade.’\footnote{Weiler (2009), p. 768.} In this way, regulations in the public interest that interfered with international trade commitments were effectively put in a defensive position, facing the requirement of the necessity test and the requirements of the chapeau of the general exceptions.\footnote{See Lang (2011), p. 265 (arguing that ‘[p]art of the purpose and the effect of the reinterpretation of Article III, in other words, was to shift the centre of gravity of the legal discipline of domestic regulation under the GATT from the non-discrimination test in Article III to the necessity test in Article XX’).} Although the interpretation of the general exceptions and, in particular, the necessity test has been uneven throughout the years,\footnote{For a comprehensive overview, see Marceau, Trachtman (2014), pp. 368–377; Regan (2007), pp. 347–366; Venzke (2011), pp. 1116–1135 (detailing how various GATT panels and Appellate Bodies have analysed Article XX arguments).} one thing has remained stable: it is a particularly difficult test to meet.\footnote{Delimatis (2011), p. 266; Venzke (2011), pp. 1118–1119. For a discussion, see Section 2.3.2.} The interpretation of the general exceptions, which have become the core mechanism to distinguish between domestic measures that are legitimate and those that are protectionist,\footnote{Delimatis (2014), p. 95 (‘Since the inception of GATT, necessity tests have formed part of the contract, providing flexibility and “breathing space” to regulators. Necessity has been traditionally considered as the prevailing proxy for the identification and the discipline of protectionist or unduly burdensome regulatory behaviour’.)} has created a ‘protectionist bias’; that is, an inclination to protect the interests of trade-oriented stakeholders that ‘may be inconsistent
with the human rights interests of consumers in maximum equal liberty and open markets.\(^{508}\) For example, as discussed in Section 2.3.2 above, in the interpretation of the ‘reasonably available’ test – the benchmark for the assessment of whether a particular trade-inconsistent domestic measure meets the ‘necessity’ requirement of the general exception\(^{509}\) – WTO adjudicating bodies assess whether an alternative measure that provides the same level of protection of the public interest or objective pursued by a trade-inconsistent measure without prohibitive cost or substantial technical difficulties is available.\(^{510}\) Inconsistency in the interpretation of what ‘the same level of protection’ and ‘prohibitive’ costs entail, in some cases amounted to the consideration of an actual level of protection achieved by a contested measure (rather than a desired level of protection subjectively determined by the state and not (yet) necessarily achieved), and a disregard of high administrative and enforcement costs. Such inconsistencies left WTO members a much narrower regulatory space than the wording of the test might otherwise suggest.\(^{511}\)

The reality is that a less trade-restrictive measure is, in theory, almost always reasonably available in the imaginary ‘toolbox of effective nontrade policy instruments’ mentioned above.\(^{512}\) As argued in Section 2.3.2 above, despite the fairly consistent language in WTO case law that the less restrictive alternative should be real rather than hypothetical, this logic has not always been followed in practice.

Recently, under sharp waves of critique and public discontent with the WTO’s practice of reframing regulatory approaches protecting non-economic values as barriers to trade, the WTO attempted to restore its legitimacy by trying to give more deference to the levels

---

\(^{508}\) Petersmann (2001), p. 27.


\(^{511}\) See WTO, Appellate Body Report, Korea—Various Measures on Beef, para. 178. Based on the actual application of the contested measure, the Appellate Body held the following:

> We think it unlikely that Korea intended to establish a level of protection that totally eliminates fraud with respect to the origin of beef (domestic or foreign) sold by retailers. The total elimination of fraud would probably require a total ban of imports. Consequently, we assume that in effect Korea intended to reduce considerably the number of cases of fraud occurring with respect to the origin of beef sold by retailers. The Panel did find that the dual retail system ‘does appear to reduce the opportunities and thus the temptations for butchers to misrepresent foreign beef for domestic beef.

_Ibid._ (emphasis added). The alternative measure, which the Appellate Body said was reasonably available to Korea, involved higher administrative and enforcement costs. Korea argued that it lacked the resources necessary for this alternative, but the Appellate Body still concluded that the contested measure did not pass the ‘necessity’ assessment. _Ibid._, paras. 175, 180. But see WTO, Appellate Body Report, US-Gambling, paras. 308, 317 (The Appellate Body dismissed the alternative measure proposed by a claiming party as ‘not an appropriate alternative’, and stated, ‘[A] “reasonably available” alternative measure must be a measure that would preserve for the responding Member its right to achieve its desired level of protection with respect to the objective pursued under paragraph (a) of Article XIV’) (emphasis added).

\(^{512}\) Howse (2002), p. 100.
of protection of domestic societal interests.\textsuperscript{513} It does not seem to be working. As Andrew Lang neatly put it,

\begin{quote}
[i]n the lingua franca of trade professionals, ‘the toothpaste was out of the tube,’ and it was simply not possible to return to a trade regime which was narrowly focused on (say) border barriers, and only a small subset of domestic regulations which had direct and immediate impacts on trade flows.\textsuperscript{514}
\end{quote}

However, this does not mean that restoring such legitimacy is insurmountable in the future.

After the Uruguay Round, WTO multilateral negotiations have not made any significant progress in the further liberalisation of international trade beyond what could be achieved through a neoliberal interpretation of existing rules.\textsuperscript{515} Instead, international trade law-making moved to bilateral and regional fora where multiple bilateral and plurilateral preferential trade and investment agreements have been concluded around the world (some 2300 bilateral investment treaties and 306 regional trade agreements are in force).\textsuperscript{516} These agreements have structured and furthered the integration of national economies into a single world economic order.\textsuperscript{517} As opposed to WTO negotiations, where consensus of all parties is required, bilateral and regional negotiations make it easier for certain states to advance a new form of the neoliberal discourse – that of global digital trade – to achieve an ever-deeper trade liberalisation.\textsuperscript{518} Drawing a parallel with the redefinition of protectionism as ‘new protectionism’ in 1970s, the next Section discusses how the redefinition of protectionism as ‘digital protectionism’ may have contributed to such a transition.

\section*{3.3 Digital protectionism: the latest wave of trade constraints on regulatory autonomy}

As noted in the Introduction to this thesis, the last decade has witnessed a trend towards regulating electronic commerce and digital trade in bilateral and regional trade

\textsuperscript{513} For a detailed account see Howse (2016), pp. 13, 45–75.
\textsuperscript{515} Burri (2013), p. 3 (‘As the Doha negotiations continue to make little progress, the multilateral venue of rule-making is being seriously undermined, and this triggers forum-shopping—bilaterally, regionally, and through new plurilateral initiatives within clubs of countries, unaffiliated to any international organization, such as the Anti-Counterfeiting Trade Agreement (ACTA)’.)
\textsuperscript{516} UNCTAD. (2016), p. 101. According to Wolfe, of the 275 regional/bilateral trade agreements (‘RTAs’) that had been notified to the WTO by May 2017, seventy-five have e-commerce provisions, and such provisions are included in more than 60\% of the RTAs that entered into force between 2014 and 2016. Wolfe (2019), p. s63.
\textsuperscript{518} See Pauwelyn (2012).
agreements. These changes have occurred against a background comprised of the idea that globalisation is a net positive, on the one hand, and the development of new information technologies that allow for an almost instant exchange of information, services, and capital, on the other hand. As personal and other data became an essential component of cross-border trade, ensuring its unrestricted cross-border flow became an important yet contentious point in the negotiations of ‘new generation’ international trade agreements. These negotiations coincided with the discourse of digital trade advanced by the United States, stressing the economic benefits of digital trade and exposing the downsides of restrictions on cross-border flows of personal data – which are also sometimes referred to as data localisation requirements – labelling them as ‘digital protectionism’. This label, as the Chapter explains below, is, in particular, often attached to the EU restrictions on cross-border transfers of personal data, explained in Section 2.2.1.3 above, by those criticising the EU approach. It is that set of rules that is more often showcased as being detrimental to international trade, and described as protectionist.

In spite, or perhaps because, of this, EU politicians also regularly express their disapproval of digital protectionism. Although the EU and US discourses on digital trade are ostensibly woven with similar terminological threads of digital protectionism, such discourses are inchoate and fundamentally diverge in their views on the underlying values and policy objectives of digital trade. Although in both cases powerful economic interests may have played a role in constructing the discourse, when it comes to the interplay between digital trade and the protection of privacy and personal data, unlike the United States, the European Union is bound by internal constitutional constraints, already discussed in Chapter 2, and elaborated upon in more detail in Chapter 5 of this thesis. It is this divergence that could explain why the attempt to redefine protectionism – and narrow

520 It could be argued that ‘restrictions on cross-border data flows’ and ‘data localization’ mean different things, as data localization laws do not always restrict cross-border flows of data. See, e.g., Casalini, López González (2019), p. 5. Some authors view data localization as a form of restrictions on cross-border data flows. See, e.g., Hodson (2019). Given that there is no consensus on the meaning of these terms, and drawing a clear line between them is not the purpose of this thesis, the author uses them interchangeably.
522 See Goldfarb, Trefler (2019), pp. 479–480 (viewing restrictions on personal data transfers as a form of data localization that could favor domestic firms and have negative effects on trade); see also Ferracane, van der Marel (2018b) (‘We find that restrictions on the cross-border movement of data, as opposed to restrictions on the domestic use of data, significantly reduce imports of services’); Goldfarb, Tucker (2011), pp. 69–70 (demonstrating that European strict e-privacy rules lead to an average reduction in effectiveness of 65% of banner ads, thus proving to be damaging for the European advertising industry).
domestic regulatory space to protect personal data – has ultimately been reflected in the US-led, and not the EU-led, trade agreements. The European Union’s restrictions on cross-border transfers of personal data undoubtedly impose limitations on international trade. The key question is, however, whether such restrictions can appropriately be labelled as ‘protectionist,’ and if so, what the consequences of using this label might be in future policy decisions. This Chapter addresses this question in Section 4.

3.3.1 The digital trade discourse(s)

As shown above, in showcasing the economic benefits of free cross-border data flows, the narrative of digital trade often presents domestic privacy and data protection regimes (as well as their international divergence) as digital trade barriers. A number of economic arguments, advanced primarily by the US government, European, and US pro-trade think tanks (but also by several academics), are used to explain why restrictions on cross-border flows of personal data or data localisation requirements hamper digital trade. For instance, an influential McKinsey & Company report argued that in 2014 alone, cross-border data flows generated $2.8 trillion in value. An earlier study conducted for the US Chamber of Commerce by the pro-trade think tank, the European Centre for International Political Economy (‘ECIPE’) warned of the negative welfare effects on the EU economy if cross-border data flows were to be disrupted by the then-draft GDPR. A number of other ECIPE studies predict that the removal of restrictions on cross-border flows of information would increase imports of services, on average by five percent. These studies feed into the lobbying activities of export-oriented service industries around the world. In a similar vein, in a taxonomy of trade restricting measures prepared by the United States International Trade Commission (‘USITC’), the EU data protection framework (which, unlike US law, requires a higher level of data protection complemented by restrictions on cross-border transfers of personal data), is mentioned as restricting

528 See Ferracane, van der Marel (2018b) (‘Our analysis predicts that, if countries lifted their restrictions on the cross-border flow of data, the imports of services would rise on average by five percent across all countries, with obvious benefits for local companies and consumers who could access cheaper and better online services from abroad’.)
529 See, e.g., Global Services Coalition Statement on Digital Trade. (2017) (quoting Manyika, Lund, Bughin, Woetze, Stamenov, Dhingra (2016), and several ECIPE studies and ‘calling[ing] for negotiators of ongoing or future negotiations related to data flow including FTAs/EPAs to make their utmost efforts to agree on strong and effective provisions which guarantee free flow of data, and prohibit forced data localization and requirements for provision of software source code, while applying appropriate and effective protection and security for personal data’.)
international digital trade in several sectors. The USITC and ECIPE stress that, generally speaking, restrictions on cross-border transfers, in addition to substantive rules restricting the use of personal data and data localisation measures, increase the costs of conducting business for multinational companies. More specifically, researchers associated with the ECIPE argue that restrictions on cross-border data flows reduce (or, in other words, restrict) imports of data-intensive services.

As any user of Facebook can attest, personal data, viewed as an economic asset, also constitutes an important ingredient of AI-based systems and algorithms, an input in the production of many digital services, production processes, and logistics. In other words, it is a factor of production. Foreign providers of such services, including targeted marketing companies, are in a less favourable position than domestic providers that do not have to comply with cross-border transfer restrictions to provide the same services domestically. In addition, restrictions on flows of data are viewed not only as detrimental to ICT services, but also for trade in goods and services generally, as they may result in companies choosing a less efficient mode of production (or supply) of services. Global

---

530 United States International Trade Commission (2017), p. 273 (‘According to input from industry representatives, regulatory and policy measures focused on data protection and privacy affect all kinds of industries. These measures can inhibit global digital trade by U.S. firms due to the increased administrative costs associated with complying with stricter privacy measures that differ from U.S. standards.’)


532 See Ferracane, M.F., van der Marel, E. (2018a), p. 15 (showing that ‘more restrictive data policies, in particular with respect to the cross-border movement of data, result in lower imports in data-intensive services for countries imposing them.’)

533 See Crémer, De Montioye, Schweitzer (2019), p. 73 (‘Data is a core input factor for production processes, logistics, targeted marketing, smart products and services, as well as Artificial Intelligence (AI).’)

534 See Mueller, Grindal (2019), p. 80 (concluding that ‘information in the form of digital data flows can be considered a mobile factor of production’); see also Costa-Cabral, Lynskey (2015), p. 11 (‘Without personal data as an input some goods and services are now ostensibly impossible to produce, leading to the growth of commodity markets for personal data. Thus, personal data is a full-fledged factor of production in a modern economy.’); see also Gürses, van Hoboken (2018), p. 595 (showing that users’ data has become an integral part of production and testing of digital services and software).

535 As already explained in Section 2.2.2, under the GDPR, in order to access EEA personal data from outside the EEA foreign companies not only have to comply with legal grounds for collecting personal data under Articles 5 and 6 of the GDPR (requirements that generally apply to European companies), but also with the limitations on cross-border transfers of personal data (Chapter V GDPR). EDPB, Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, 25 May 2018, p. 3. When applying Article 49 one must bear in mind that according to Article 44 the data exporter transferring personal data to third countries or international organizations must also meet the conditions of the other provisions of the GDPR. Each processing activity must comply with the relevant data protection provisions, in particular with Articles 5 and 6. Hence, a two-step test must be applied: first, a legal basis must apply to the data processing as such together with all relevant provisions of the GDPR; and as a second step, the provisions of Chapter V must be complied with. Ibid.; see also Bergkamp (2002), p. 39.

536 See Ferracane, van der Marel (2018b) (citing Andrenelli, Cadestin, De Backer, Miroudot, Rigo, Ye (2018). (‘[A] range of data-intensive services from computer services to retail and information services are increasingly being traded over the internet rather than by other means such as foreign establishments.'
information flows allow multinational companies to operate globally without an international physical presence.\textsuperscript{537} Some academics also argue that restrictions on data flows may limit the possibilities of the world-wide aggregation of personal data and are thus threatening technological advances in such areas as cloud computing and AI.\textsuperscript{538} In a similar vein, the US Chamber of Commerce and Hunton & Williams warned that such restrictions may turn the ‘Internet’ into a ‘splinternet,’ paving the way to economic stagnation.\textsuperscript{539}

3.3.2 Framing data protection as ‘digital protectionism’ in the digital trade discourse

Discourse matters, and the discourse is changing. Political, academic, and societal debates on cross-border data flows now revolve around terms such as ‘digital protectionism,’ ‘data protectionism,’ data nationalism,’ ‘innovation mercantilism,’ ‘data colonialism’ and ‘digital colonialism’.\textsuperscript{540}

That said, the view that restrictions on cross-border flows of personal data could favour domestic industries is not new.\textsuperscript{541} As early as 1978, John Eger raised a concern that the restrictions on cross-border flows of personal data adopted by some EU countries and envisaged to be introduced on an EU level might, in practice, not only be used to protect privacy and national sovereignty, but also ‘to protect domestic economic interests’ as indirect barriers to trade.\textsuperscript{542} It is only recently, however, that the term ‘digital

Restricting data would, therefore, also inhibit companies from choosing the most efficient channel of trading many services.’)

\textsuperscript{537} See UNCTAD (2017), p. 167.

\textsuperscript{538} See Chander, Lé (2015), p. 680 (2014) (Labelling E.U. restrictions on transfers of personal data as data localization measures and stating that ‘[b]y creating national barriers to data, data localization measures break up the World Wide Web, which was designed to share information across the globe. … Data localization would dramatically alter this fundamental architecture of the Internet’.); ibid., p. 681 (arguing that data localization measures promote ‘data nationalism,’ which ‘poses a mortal threat to the new kind of international trade made possible by the Internet—information services such as those supplied by Bangalore or Silicon Valley’); see also Goldfarb, Trefler (2019), p. 29 (‘Data localization is an issue for AI because AI requires data. In other words, localization is a way to restrict the possible scale of any country in AI, but at the cost of lower quality overall’). But see Kuner (2015a), p. 2090 (offering a powerful critique of these arguments).

\textsuperscript{539} U.S. Chamber of Commerce, Hunton & Williams LLP. (2014), pp. 2–3 (‘Technological advances and an increasingly globalized economy have brought us to a policy crossroads: one path leads to a ‘splinternet’ of economic isolation, characterized by misguided attempts to safeguard data by building protectionist walls [T]his isolationist approach has repeatedly caused economic stagnation.’)


\textsuperscript{541} See Eger (1978)., p. 1066.

\textsuperscript{542} See ibid., p. 1066 (‘Many countries in Europe may have no concern other than protecting the privacy of personal data, a concern which neither the American public nor any member of a democratic society can fault. But there is the danger, of course, that these new laws will be used not only to protect just privacy but also to protect domestic economic interests.’)
protectionism’ was coined to refer to such restrictions.\textsuperscript{543} For example, in a non-paper for the discussions on electronic commerce at the WTO, Japan stressed the necessity ‘to address emerging “digital protectionism”’ as a prerequisite for ‘open, secure, and reliable global e-commerce environment that will promote and facilitate cross-border digital trade.’\textsuperscript{544} Relying on the definition of barriers to digital trade by USITC, Aaronson defined digital protectionism as ‘barriers or impediments to digital trade, including censorship, filtering, localization measures, and regulations to protect privacy.’\textsuperscript{545} Other academics, most notably Chander and Lê, argued that ‘[w]e must insist on data protection without \textit{data protectionism}. A better, safer Internet for everyone should not require breaking it apart.’\textsuperscript{546}

Similarly, Burri called upon international legal scholars to ‘stress the dangers of data protectionism, often under the disguise of legitimate objectives, such as national security or privacy protection.’\textsuperscript{547} At the same time, Burri points out that not only divergent approaches to data privacy and protection (which is arguably the crux of the cross-border data flow problem), but also standards of data protection that are \textit{too low} could be viewed as barriers or obstacles to trade.\textsuperscript{548} This is, in part, because consumer confidence and trust, she argues, are a precondition for well-functioning digital trade.\textsuperscript{549} This leads to a search for an optimal level (from a trade perspective) of protection rather than a complete absence of protection.\textsuperscript{550}

The US administration’s recent rhetoric centred on the notion of data protectionism seems to be based exactly on this logic. US trade experts and the administration have used harsh language to characterise the European Union’s privacy and data protection framework.\textsuperscript{551} Work by Aaronson demonstrates how the US administration routinely uses the terms ‘protectionism’ or ‘digital protectionism’ to refer to EU-style privacy and personal data protection regimes.\textsuperscript{552} Yet, in parallel to attaching the (negative) label ‘protectionism’ to – what it sees as too much – privacy protection, the US government has

\textsuperscript{543} See (2017), pp. 2, 8.
\textsuperscript{544} WTO, Work Programme on Electronic Commerce, Non-Paper for the Discussions on Electronic Commerce / Digital Trade from Japan, JOB/GC/100, 21 July 2016, para. 2.2.
\textsuperscript{546} Chander, Lê (2015), p. 739 (emphasis added).
\textsuperscript{547} Burri (2017c), p. 448 (emphasis added).
\textsuperscript{548} Burri (2017a), pp. 13–14.
\textsuperscript{549} \textit{Ibid.}; see also Mishra (2019), p. 503 (‘Implementing internet privacy is increasingly recognised as one of the fundamental requirements for digital trade.’)
\textsuperscript{550} \textit{Ibid.}
\textsuperscript{551} See, e.g., United States International Trade Commission (2014), p. 14 (stating that E. U. data privacy and protection requirements are ‘obstacles to international digital trade,’ among localization requirements, intellectual property rights infringement and customs measures.)
\textsuperscript{552} See, e.g., Aaronson (2017), pp. 8–10; see also Aaronson (2016a). See also Schwartz, Peifer (2017), p. 118 (‘In the United States, there has been scepticism about E.U. privacy rights and whether they are merely disguised protectionism.’)
also at times criticised situations with too little privacy protection on instrumental grounds, arguing that insufficient consumer privacy protection can stifle electronic commerce.\textsuperscript{553} It seems to agree that the protection of privacy and personal data are crucial to maintaining consumer trust in digital technologies, which is in turn indispensable for the strong and orderly development of electronic and digital commerce.\textsuperscript{554} As this Chapter argues in Section 3.4, this is not a mere ‘inconsistency in the US arguments on this issue,’\textsuperscript{555} but indeed a fundamental question of a baseline – or optimal level of protection – that delineates ‘useful’ (and possibly indispensable) protection from excessive protection (that one would then label ‘protectionist’ to try to lower it). In Section 3.4, this Chapter returns to the key role of discourse in drawing this baseline.

Authors associated with ECIPE and Baker & McKenzie, have characterised the EU data protection framework as ‘disproportionate and potentially protectionist’.\textsuperscript{556} This resonates with Beattie’s article in the \textit{Financial Times} comparing the European Union’s approach to resistance to genetically modified organisms (‘GMOs’) on public health grounds – a topic around which the battle between the European Union and United States lasted for at least two decades.\textsuperscript{557} Even the then US President Barack Obama, reacting to the antitrust and data protection enforcement actions against US tech giants Google and Facebook in the European Union, publicly insinuated the European Union was merely pursuing its own ‘commercial interests’.\textsuperscript{558}

As alluded to above, despite being criticised for pursuing potentially protectionist

\textsuperscript{553} See Aaronson (2016b), p. 87; see also Aaronson (2017), pp. 21–22.

\textsuperscript{554} \textit{Ibid.}, p. 19.

\textsuperscript{555} Aaronson (2016b), p. 87 (‘U.S. arguments against digital protectionism are often inconsistent’); see also Aaronson (2017), p. 21 (‘[T]he United States has adopted an inconsistent approach to privacy as a barrier to trade’).

\textsuperscript{556} Bauer, Erixon, Krol, Lee-Makiyama (2013), p. 4. (‘The question of whether the European regulatory model on privacy is disproportionate and potentially protectionist has become one of the most controversial political debates within the EU at this time, and perhaps rightly so.’); see also Determann (2016), pp. 247–248 (‘The USA support free global trade and have so far not retaliated against the protectionist data transfer restrictions in “Fortress Europe”’).

\textsuperscript{557} Beattie (2017) (arguing that the E.U. privacy and data protection framework is a localization requirement that acts as a form of protectionism in favour of (unnamed) interest groups, just as the E.U. prohibition on GMOs helped European farmers to protect themselves unfairly from U.S. competition.) Beattie contends that this regulatory framework will benefit European firms and, in the long term, the European Union’s ‘attitude to cross-border data flows . . . will retard European companies’ ability to maximise digital technology to full advantage’. \textit{Ibid.} From the author’s perspective, the EU-US controversy on beef treated beef would be a better parallel to the debate surrounding data protection. While mutual permeation of WTO and EU rules governing GMOs within a pluralist governance structure has eventually led – to a large extent – to reconciliation of differences between the EU and US approaches to the GMO issues, the disagreement on governance of beef hormones has never been fully reconcile. For a discussion, see Krisch (2012), pp. 205 – 216. See also European Commission, Press Release: The European Union and the United States sign an agreement on imports of hormone-free beef, 2 August 2019.

\textsuperscript{558} Ahmed, Robinson, Waters (2015) (‘We have owned the internet. Our companies have created it, expanded it, perfected it in ways that they can’t compete. And oftentimes what is portrayed as high-minded positions on issues sometimes is just designed to carve out some of their commercial interests’.)
restrictions on transfers of personal data, the EU itself is also actively seeking to remove measures it labels as digital protectionism. If one looks at the EU not as a homogenous institution but as a composition of different subsystems (primarily at the EU and member states levels) with different goals and decision-making processes that determine the European Union’s external (trade) and internal policies, then the situation is less clear.

The issue becomes even more complicated if one also takes into account that, in the European Commission, different departments (directorates general) are responsible for international trade (DG Trade) and fundamental rights (DG Just).

After the 2008 worldwide financial crisis, the European Commission changed its discourse; in its new discourse, trade liberalisation was ‘consistently presented … as a desirable and even necessary solution to the crisis and protectionism as a mistake from the past that has to be avoided.’ (emphasis in the original). This rhetoric targeted not only the European Union’s trading partners, but also the traditionally more protectionist EU member states that were opposed to the European Union’s bilateral concessions that could harm their domestic industries. Faithful to its longstanding course towards further liberalisation of trade and with an eye toward benefiting from globalisation, in its 2015 Communication ‘Trade for All,’ the European Commission contended that ‘the free flow of data across borders has become more important for European competitiveness in general.’ In November 2016, the EU trade commissioner Cecilia Malström noted that ‘in the digital age, restrictions on cross-border data flows inhibit trade of all kinds, and may amount to “digital protectionism.”’ She committed to using international trade deals as a means for setting the rules for digital trade.

559 Fioretti (2018).
560 See Young, Peterson (2014), p. 23 (2014) (‘Trade policy might be viewed as one of the most atomistic of all areas of public policy. Each policy decision—whether it is to negotiate a free trade agreement or impose anti-dumping duties on an imported product—involves different calculations, interests, and timeframes.’) Eckes, (2012), p. 233, explaining that in the EU foreign policy is ‘first and foremost a task of the executive; and the European executive is more fragmented than the average national executive. Indeed, it consists of “unseen and many layers”’.
564 Ibid. (‘This liberalisation-as-recovery-instrument discourse has been very powerful and difficult to contest by traditionally more protectionist Member States, uncompetitive industries or trade unions.’); see also Siles-Brügge (2011), p. 643 (‘How did DG Trade manage to convince the Member States to agree to the provisions of the FTA when it was facing the opposition of the powerful car industry . . . ? The answer is that, in a sense, it had already won the battle, by recasting liberalisation as necessary process, both in terms of the external constraint posed by globalisation but also, more specifically, the competitive pressure emanating from commercial rivals.’)
565 Communication from the Commission, Trade for All Towards a More Responsible Trade and Investment Policy, COM/2015/0497 final, 14 October 2015, p. 12 (emphasis added).
Where, then, one might ask, is the issue, if everyone agrees on the ills of digital protectionism? It follows from the fact that, when it comes to the rights to privacy and the protection of personal data, the European Union’s opposition to digital protectionism is now on a wholly different trajectory. The EU approach in this respect shifted in 2015 following a push-back by the European Parliament,567 EU-member states,568 academics,569 and civil society,570 to the European Union’s digital ‘free trade’ policy, which made it apparent that such a policy ‘should not undermine European levels of protection and democratic policy-making’.571 This shift is apparent, for example, in the 2017 Communication ‘Exchanging and Protecting Personal Data in a Globalised World,’ where the European Commission carefully carved out privacy protection from ‘protectionism’ by highlighting that ‘European companies operating in some third countries are increasingly faced with protectionist restrictions that cannot be justified with legitimate privacy considerations.’572

In sum, while the European Union and the United States frame their digital trade discourses in similar terms, they clearly do not agree on the right balance to be struck between the economic benefits of digital trade, on the one hand, and societal values, such as the protection of the rights to privacy and personal data, on the other.573 Both trading partners, however, do seem to agree that the term ‘protectionism’ has a negative valence. In practice, however, the European Union and the United States apply their own standards and values to measure what digital protectionism is abroad as a result of regulatory

567 See European Parliament resolution of 8 July 2015 containing the European Parliament’s recommendations to the European Commission on the negotiations for the Transatlantic Trade and Investment Partnership (TTIP) (2014/2228(INI)) (‘[T]o ensure that the EU’s Acquis on data privacy is not compromised through the liberalisation of data flows . . . while recognizing the relevance of data flows as a backbone of transatlantic trade and the digital economy’); European Parliament resolution of 3 February 2016 containing the European Parliament’s recommendations to the Commission on the negotiations for the Trade in Services Agreement (TiSA) (2015/2233(INI)). (‘[T]o acknowledge that data protection and the right to privacy are not a trade barrier, but fundamental rights, which are enshrined in Article 39 TEU and Articles 7 and 8 of the Charter of Fundamental Rights of the European Union’.)

568 See Bollen, De Ville, Orbie (2016), p. 284 (‘In the states where TTIP has become most politicised, notably Germany, Austria and the United Kingdom, the openness-protectionism dichotomy is of minor importance. Instead, the debate is dominated by arguments about sovereignty, regulatory paradigms and food safety.’)

569 See, e.g., Irion, Yakovleva, Bartl (2016), p. 54 (‘The risks for privacy and data protection stemming from the sphere of the EU are, broadly speaking, that EU international relations could place more emphasis on international trade in services relative to EU standards on privacy and data protection.’)

570 See, e.g., Järvinen (2016) (‘Discussions on forced data localisation should take place outside trade agreements. Otherwise, our fundamental rights to privacy and data protection can be undermined or challenged as trade barriers’.)


572 Communication from the Commission, Exchanging and Protecting Personal Data in a Globalised World, COM (2017) 7 final, 10 January 2017, p. 6 (emphasis added).

573 Aaronson (2015a), p. 687 (‘Unfortunately, despite their collaboration, the US and the EU do not completely agree on digital rights. In addition, the US and the EU disagree on the role of the state and business in protecting privacy’.)
divergence on a number of domestic policies that affect digital trade, including privacy and data protection.\textsuperscript{574} While both the European Union and the United States recognise, in theory, that privacy and data protection are important values, they diverge quite jarringly on what the ‘correct’ level of such protections should be.\textsuperscript{575} In other words, there is a deep disagreement on where to draw the line between protection and protectionism. This is the issue to which this Chapter returns below. The next Section, however, adds one more layer to the analytical edifice and turns to the business interests that underpin the shifts in the discourse.

3.3.3 Business interests behind the ‘digital trade’ discourse

In Section 2.2.4.3 above, this Chapter explained how a policy favouring liberalisation of trade, just as a policy favouring domestic regulation limiting free trade (which is often presented by those favouring free trade, as protectionist), can be captured. In following pages, this Chapter demonstrates that not only the economic benefits of cross-border digital trade but also certain business interests profiting from the absence of restrictions on cross-border transfers are shaping the ‘digital trade’ discourse.

The United States was one of the first WTO members to adopt a so-called ‘digital trade’ agenda back in 2002.\textsuperscript{576} Historically, the United States has a ‘strong competitive advantage in the digital economy…’.\textsuperscript{577} As Aaronson has argued, by making the campaign against digital protectionism an essential element of its international trade policy as demanded by the global US-based internet platforms, the United States is trying to promote a global internet, free of barriers to entry, while preserving its declining internet dominance.\textsuperscript{578} Some observers suspect that the United States applies the ‘digital protectionism’ label to any domestic regulation that reduces its market share abroad in this space.\textsuperscript{579} This echoes the above-mentioned ‘diminished giant syndrome,’ a term coined

\textsuperscript{574} See Aaronson (2015a), p. 682 (‘Under US law, online privacy is a consumer right, whereas in the EU (as well as in Australia and Canada), privacy is a human and consumer right that must be protected by governments’.)

\textsuperscript{575} See ibid., pp. 682–683 (‘Under US law, online privacy is a consumer right, whereas in the EU privacy is a human and consumer right that must be protected by governments. The EU strategy seemed directly at odds with US voluntary, limited, and sectoral approach’.)


\textsuperscript{577} Azmeh, Foster (2016), pp. 4–5 (‘Such policies also represent a long term threat to the US economy which has a strong comparative advantage in the digital economy and related activities which gives it a strong advantage to lead the major technological shifts in the coming decades in different economic sectors’); see also Aaronson (2017), p. 8 (noting the particular importance of digital trade to the U.S. economy).

\textsuperscript{578} See Aaronson (2016a), Digital Protectionism? (‘The United States has conflicting objectives regarding the digital economy. On one hand, it wants to encourage a vibrant global Internet with few barriers to entry. On the other, the United States wants to preserve its Internet dominance, which is clearly declining as China, India, Indonesia and others develop their digital prowess and bring more people online’.)

\textsuperscript{579} Ibid. (‘To some observers, it seems like the United States defines [digital protectionism] as policies that with or without intent reduce U.S. market share in foreign markets’.)
by Bhagwati to refer to the US trade policy in the 1970s, which used new protectionism to reshape the international trading order to its advantage. American tech companies view initiatives to control domestic data space in several countries, including through restrictions on data flows (e.g. those adopted in China, Australia, India, Russia, Thailand, Turkey, and the United Arab Emirates), as threats to their business model. As a result, the executives of these companies, often relying on the research of specialised think tanks, activated their lobbying activities with trade policy officials to ‘do a better job of limiting digital protectionism’.

A 2016 study showed that tensions around cross-border data flows have intensified due to an increase in the use of the label ‘digital protectionism’. Based on the analysis of data on political spending (lobbying, campaign contributions, and other forms of political activism), the authors of the study were able to claim convincingly that powerful US tech companies (including large corporations like Google, Facebook, Amazon, Microsoft, and Apple, as well as smaller firms such as LinkedIn, Airbnb, and Expedia) and industry associations (such as the Business Software Alliance, Information Technology Industry Council, and the Software & Information Industry Association) played a crucial role in the formation of the US’s ‘digital trade agenda,’ prioritisation of cross-border data flows in international trade policy, and increase in pressure on domestic regulations restricting such flows. These political efforts, as well as fears concerning the diminishing technological advantage of the United States in the global digital economy, made the ‘digital trade agenda’

---

580 See Bhagwati (1993a), p. 22 (‘The American mood parallels Great Britain’s at the end of the nineteenth century . . . . As was Great Britain at that time, America has been struck by a “diminished giant syndrome”—reinforced by the slippage in the growth of its living standards in the 1980s.’).
581 See, e.g., Aaronson (2015a), p. 684 ([P]olicymakers from [China, Australia, India, Russia, Thailand, Turkey, and the United Arab Emirates] were increasingly determined to control the Internet within their borders and facilitate the rise of domestic Internet firms Many US based Internet companies saw in these actions a threat to their bottom lines’).
582 Ibid. Aaronson notes, for example, that Google used the research of a Canadian think-tank to document how more than 40 governments instituted broad scale restrictions of information flows. See also Morozov (2015).
583 Azmeh, Foster (2016), p. 11 (‘[T]ensions around cross-border data flows. Such tensions have been brought to the fore by the growing use of so-called ‘digital protectionism’ in a number of countries.’)
584 Ibid., pp. 12–14 (‘In the US, political spending by these firms have increased substantially over the last few years making internet and new “tech” companies one of the strongest lobbying sectors in Washington …. This included major spending from large companies such as Google, Facebook, Amazon, Yahoo, Apple, eBay, Microsoft, and Apple, but also younger firms such as Snapchat, Rapidshare, LinkedIn, Dropbox, Twitter, Airbnb, Expedia, in addition to industry associations’). See also UNCTAD. (2019), pp. 88–89, (‘[G]lobal digital platforms’ have an interest in lobbying for international rules and regulations that allow to enable them to leverage their business models. Indeed, in the past few years, technology companies have replaced the financial sector as the biggest lobbyists, and major platforms have spent considerable resources in key locations’).
585 See Azmeh, Foster (2016), p. 19 (‘Many of the policies demanded by the industry were reflected in the US trade policy and in the ‘digital dozen’ principles adopted by the USTR. . . . Similarly, the trade promotion authority (TPA) listed digital trade and cross-border data flows as principle negotiating objectives of the United States’).
‘a key part of the US trade policy in future multilateral and bilateral agreements’.  

Due to absence of reliable granular information on lobbying at the EU institutions, no similar research seems to exist on the lobbying activities on digital trade at the EU level. The EU Transparency Register, which discloses information on interest groups affecting decision-making in the European Union, does not contain statistics on interest group spending in each particular area. The available information, however, demonstrates that not only big US tech companies, such as Google, Apple, Facebook, Amazon, and Microsoft, but also large European industry associations, such as Business Europe and Digital Europe, annually spend several million Euros on lobbying activities at EU institutions involving digital trade, cross-border data flows, and personal data protection.

---

586 Ibid., p. 30; see also Selby (2017), p. 217 (‘It is not surprising to see the US government push strongly in the next generation of international trade agreements to restrict efforts to implement data localization in other countries.’)

587 To the knowledge of the author, the EU Transparency Register is the only reliable source of information on lobbying activities and spending at the EU institutions. The problem is, however, that while registration in the Register is mandatory for lobbying at the European Commission, this is not the case for lobbying at the European Parliament and the Council. Furthermore, the lobbying spending indicated in the Register is not granular enough, as it is not possible to see the amount spent on lobbying efforts on each specific topic. In addition, there is also no control mechanism to verify that information is accurate and up-to-date. See Antypas (2018); Timmermans (2019); Nielsen (2019).


3.3.4 Measures banning ‘digital protectionism’ in recent trade agreements

Just as in the neoliberal discourse of the 1970s and 1980s, the modern digital trade discourse(s) are reflected in recent international trade agreements, which increasingly include dedicated chapters on electronic commerce and digital trade (‘digital trade chapters’). Such chapters tackle a range of domestic policies affecting cross-border digital commerce (‘digital trade provisions’), but this Chapter only focuses on those concerning cross-border data flows.

WTO members have not yet achieved a multilateral consensus on the design and scope of digital trade provisions, which have thus far only appeared in bilateral and regional trade agreements, and have somewhat overshadowed the WTO’s multilateral efforts in this area. Although the proposals on electronic commerce in the WTO increasingly focus on barriers to digital trade and digital protectionism, the WTO has not yet made any progress on this issue. It remains to be seen how the above-mentioned negotiations on electronic commerce, which started in 2019, will play out. Despite a seemingly firm consensus on the use of the terms ‘digital trade’ and ‘digital protectionism’ – the axes around which the discourses governing international negotiations revolve – the value structures underlying these discourses diverge, as the US and the EU example above illustrates. This Section explicates how the international trade provisions on cross-border data flows advanced by the United States and the European Union mirror this divergence.

In the spirit of its digital trade agenda, the United States has been a pioneer in including provisions on free cross-border data flows in international trade agreements. Although the United States has advocated regulating information flows via international

with Commissioners, Members of their Cabinet or Director-Generals since 01/12/2014 under its current ID number in the Transparency Register: 64270747023-20, http://ec.europa.eu/transparencyregister/public/consultation/displaylobbyist.do?id=64270747023-20&pdf=true (showing that Digital Europe was active on the topics of trade, data flows, artificial intelligence, and GDPR).

591 See, e.g., CPTPP.
592 See, e.g.. Art. 14.5 CPTPP (outlining the endeavors each party to the agreement must make in maintaining a legal framework governing electronic transactions domestically).
593 See Burri (2017c), p. 417 (‘As the Doha negotiations continue to make little progress, the multilateral venue of rule-making has been seriously undermined and this has triggered forum-shopping—bilaterally, regionally, or through plurilateral initiatives.’)
594 See Mitchell, Mishra (2018), p. 1111 (‘The majority of the recent proposals on electronic commerce circulated by WTO Members in recent years tend to focus on regulatory barriers to digital trade. In particular, they emphasize digital protectionism.’)
595 Aaronson (2016b), p. 59 (‘The United States is the Paul Revere of digital protectionism, using naming and shaming to condemn such policies’); see also Aaronson (2015b), p. 507; U.S. Chamber of Commerce (2014), p. 3; Geist (2018) (‘The CPTPP also includes a specific exception for financial services, ironically at the insistence of the US Treasury, which wanted to retain the right to establish restrictions on financial data flows’.)
trade rules roughly since the 1980s, the first time a non-actionable (or non-binding), horizontal provision on free cross-border data flows appeared in its trade agreement was in the electronic commerce chapter of the 2012 US-Korea free trade agreement (KORUS). The United States later proposed a binding horizontal provision – a demand of key US lobbies as explained above – in the drafts of the currently stalled TTIP and TiSA. The e-commerce chapter of the CPTPP similarly includes a legally binding horizontal obligation on the free cross-border data flow of information, including personal data, which states that '[e]ach Party shall allow the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business of a covered person.'

This provision was included in CPTPP before the US withdrawal from the agreement and remained unchanged in the final version of the agreement concluded without the United States. The USMCA – a revision of the North American Free Trade Agreement (‘NAFTA’) – includes a similar provision. Including such provisions in recent trade agreements is a US priority. The US proposal for the ongoing e-commerce talks at the WTO and the recent US-Japan Digital Trade Agreement replicates the ‘golden standard’ provisions on digital trade. This move, against the background of trade

---

596 See Aaronson (2015a), p. 672 (noting that the issue of free flow of information in trade agreements ‘is not new; in the 1980s, with the advent of faster computers, software, and satellites, officials from some states, including the US and Japan, wanted to include language governing the free flow of information in trade agreements.’). For a concise overview of earlier initiatives, see ibid., p. 679–685.

597 Ibid., p. 687 (‘[T]his provision does not forbid the use of such barriers, nor does it define necessary or unnecessary barriers. In short, the language is not actionable.’) Art. 15.8 KORUS.


599 Art 14.11(2) CPTPP.

600 The version of the agreement with the United States as a party was known simply as the Transpacific Partnership (‘TPP’). Removing the United States from this agreement was one of President Trump’s first decisions. See Executive Office of the President, Office of the U.S. Trade Representative (2017). Letter to TPP Depositary.

601 See generally CPTPP.

602 Art. 19.11(1) USMCA (‘No Party shall prohibit or restrict the cross-border transfer of information, including personal information, by electronic means if this activity is for the conduct of the business of a covered person’); see also Aaronson, Leblond (2018), p. 257 (noting that despite the fact that Trump withdrew from the TPP right after becoming President, ‘the Trump administration has built its proposals on those of the Obama administration (namely, the TPP’).

603 See, e.g., Fefer, R.F. (2019), p. 1 (‘To enable international data flows and trade, the United States has aimed to eliminate trade barriers and establish enforceable international rules and best practices that allow policymakers to achieve public policy objectives, including promoting online security and privacy.’); see also Press Release, Office of the U.S. Trade Representative, Summary of Objectives for the NAFTA Renegotiation, 17 November 2017 (outlining specific negotiation objectives for the initiation of NAFTA negotiations as it related to digital trade in goods and services and cross-border data flows).

604 Manak (2019); White House (2019); Art.11(1) US-Japan Digital Trade Agreement. (‘Neither Party shall prohibit or restrict the cross-border transfer of information, including personal information, by electronic means, if this activity is for the conduct of the business of a covered person.’)
restricting measures in traditional trade sectors,\textsuperscript{605} illustrates the strategic importance of digital trade for the US economy.

As compared to prior US-led free trade agreements, both the CPTPP and USMCA not only contain an exception from a free data flow provision for regulation pursuing important domestic public policy objectives, but also a dedicated article on the protection of personal information.\textsuperscript{606} In both cases, the structure and text of the exception strongly resemble those of Article XIV(c)(ii) of GATS. For example, Article 19.11(2) of the USMCA, states the following:

This Article does not prevent a Party from adopting or maintaining a measure inconsistent with paragraph 1 that is necessary to achieve a legitimate public policy objective, provided that the measure:

(a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and

(b) does not impose restrictions on transfers of information greater than are necessary to achieve the objective.\textsuperscript{607}

In both the USMCA and CPTPP, the exceptions do not specifically identify privacy and data protection by name, or any other particular policy objective.\textsuperscript{608} It can be reasonably argued that privacy and data protection would fall under such exceptions, as these policy interests are among the public policy goals that are most likely to be affected by the free cross-border data flow provision. The above-mentioned necessity test – the benchmark to evaluate the consistency of domestic regulation with the conditions of the exception – requires an objective assessment.\textsuperscript{609} The USMCA also clarifies that ‘[a] measure does not meet the conditions of this paragraph if it accords different treatment to data transfers solely on the basis that they are cross-border in a manner that modifies the conditions of competition to the detriment of service suppliers of another Party.’\textsuperscript{610} This ties in with the interpretation of the necessity test in the WTO general exceptions discussed in Sections

\textsuperscript{605} See Chow, Sheldon, McGuire (2019), p. 2151 (‘[T]he Trump Administration is following a path of economic nationalism and pushing back with threats of not playing by the accepted rules of international governance’); see also Handley, Limão (2017), pp. 141–143.
\textsuperscript{606} Art. 14.11(2) CPTPP and Art. 19.11(2) USMCA contain an exception for the free cross-border data flow provision; Art. 14.8 CPTPP and Art. 19.8 USMCA contain a provision on the protection of personal information.
\textsuperscript{607} Art. 19.11(2) USMCA (emphasis added).
\textsuperscript{608} See \textit{ibid}.; Art. 14.11 CPTPP.
\textsuperscript{609} Instead of the ‘necessity’ requirement, exception in Art. 14.11(2) CPTPP provides that restrictions should not be ‘greater than are \textit{required} to achieve the objective’. This difference seems, however, purely semantic, and according to the WTO Secretariat, is yet another way to convey the concept of ‘necessity’. See WTO, Note by Secretariat, ‘Necessity tests’ in the WTO, S/WPDR/W/27, 2 December 2003, para. LA.5.
\textsuperscript{610} Footnote 5 to provision of Art. 19.11(2)(b) USMCA (emphasis added).
2.3.2 and 3.2.4.3, and does not recognise regulatory intent as a factor in the necessity test assessment.

The provision for the protection of personal information in the USMCA includes not only aspirational provisions for the protection of personal information but also a number of binding obligations:

1. ‘[To] adopt or maintain a legal framework that provides for protection of personal data of users of digital trade,’ featuring the APEC Privacy Framework and the 2013 OECD Guidelines governing the Protection of Privacy and Transborder Flows of Personal data as examples of such frameworks;

2. To implement key data protection principles such as a limitation on the collection of data, data quality, purpose specification and a requirement that ‘any restrictions on cross-border flows of personal information are necessary and proportionate to the risks presented’;

3. A transparency requirement that parties publish information on how individuals can pursue a remedy in case of violation of personal information protections and on how companies can comply with the local personal information protection requirements; and

4. To cooperate with regulations towards developing mechanisms of compatibility between the parties’ data protection regimes and an endorsement of APEC Cross-Border Privacy Rules (CBPR) system as a ‘valid mechanism’ to facilitate cross-border information flows while protecting personal data.\(^61\)

This provision transplants the US approach to the protection of personal data as a consumer right. Explicit mention of the 2013 OECD Guidelines and the APEC CBPR reflects the economic approach to the protection of personal data as a precondition for digital trade.\(^61\) This way, privacy and personal data protection become normalised – or redefined – as tools of international trade and are viewed as trade values.\(^61\)

The European Union’s digital trade discourse has also produced several ‘new generation’ international trade agreements that contain, in addition to the usual chapters on trade liberalisation, specific chapters on electronic commerce that included predominantly

\(^61\) Art. 19.8 USMCA.


\(^61\) Art. 19.8 USMCA; see Yakovleva (2018), pp. 484–485.
aspirational provisions. However, so far, unlike the United States, the European Union has taken a more cautious approach to cross-border data flows in trying to defend its regulatory autonomy to protect the fundamental rights to privacy and personal data. So far, none of the EU completed trade agreements include binding provisions on cross-border data flows. As already mentioned above, in the course of the TTIP and TiSA negotiations, such provisions, especially the exceptions from them for privacy and data protection, became a contentious (and a turning) point in the European Union’s approach to regulating cross-border data flows in trade agreements, which has affected its trade negotiations with other trading partners. In the digital trade chapters of JEFTA and the revision of the EU-Mexico Free Trade Agreements, the European Union explicitly refrained from including a free cross-border data flow provision; these agreements only contain a three-year review clause, which allows parties to reconsider this issue. Cross-border flows of personal data between the European Union and Japan were eventually routed through a mutual adequacy decision granted by both parties to each other (the European Union – in accordance with the GDPR) shortly before JEFTA took effect.

As already mentioned in the Introduction, in 2018, the European Union agreed on model provisions for free cross-border data flows and respective exceptions for privacy and data protection. The European Union has already included these clauses in its proposals for currently negotiated trade agreements with New Zealand, Australia, Chile, Indonesia, Tunisia, and the UK and in its proposal for the recent WTO negotiations on electronic commerce. Unlike an open provision on cross-border data flows in Articles 14.11(2) of

614 See Bollen, De Ville, Orbie (2016), p. 282 (‘[S]ince the 2006 Global Europe communication the EU has put bilateral trade deals explicitly at the service of its commercial and wider economic interests’.); ibid., p. 287 (stating that after the 2008 crisis the European Union significantly intensified ‘the (neo)liberal pattern in the bilateral dimension’ by opening trade negotiations with the US, Canada, and Japan); see also Siles-Brügge (2011), p. 629; Orbie, De Ville (2014), pp. 95–110.
615 See Aaronson (2015a), p. 685 (‘The EU, in contrast, embraced a less combative and more internationalist strategy. The EU pushed for WTO wide data flow principles but did not name and shame other countries for digital protectionism (although it does list some countries’ policies as barriers to trade).’).
616 See ibid., pp. 685, 689–690.
618 Art. 8.81 JEFTA; Art. XX EU Proposal for a Chapter on Digital Trade of the modernised EU-Mexico FTA; see also Fortnam (2017).
620 EU model clauses on cross-border data flows.
621 See European Union, Joint Statement on Electronic Commerce. EU Proposal for WTO Disciplines and Commitments Relating to Electronic Commerce. Communication from the European Union. INF/ECOM/22, 26 April 2019; EU proposal for a Chapter on Digital Trade of the EU-New Zealand FTA; EU proposal for a Chapter on Digital Trade of the EU-Australia FTA; La proposition de l’Union européenne (UE) relative à Accord de libre-échange UE-Tunisie UE-Tunisie, Titre [ ] Commerce Numérique, 9 November 2018; Draft text of the Agreement on the New Partnership with the United Kingdom, European Commission, 18 March 2020. Digital Trade Proposals for EU- Chile and EU-Indonesia were drafted before the European Union agreed on the model provisions. Therefore, these proposals only contain a placeholder for a provision on cross-
the CPTPP and 19.11(1) of the USMCA, these model clauses, discussed in greater detail in Chapter 4 of this thesis, contain an enumerated list of restrictions on cross-border data flows. This article is formulated in a way that makes the European Union’s own restrictions on cross-border transfers of personal data a priori not subject to the prohibition to restrict cross-border data flows. Furthermore, the clauses also embody the recognition that ‘the protection of personal data and privacy is a fundamental right and that high standards in this regard contribute to trust in the digital economy and to the development of trade.’ In addition, it provides for a broad exception for domestic privacy and data protection rules, which is fundamentally different from, and sufficiently broader than, those included in the CPTPP and the USMCA in at least three ways. First, it integrates into a trade agreement a different normative approach to protecting the rights to privacy and data protection – that of fundamental rights protection as compared to the instrumental approach embedded in the CPTPP and the USMCA. Second, it recognises rules on cross-border data flows as a valid regulatory tool to protect the rights to privacy and personal data. Third, it incorporates a subjective ‘it deems appropriate’ test similar to that employed in national security exceptions in WTO agreements, as opposed to the objective necessity test in the CPTPP and the USMCA.

To sum up, in the light of the different digital trade discourses advanced by the United States and the European Union, the contrast in the design of cross-border data flow provisions and exceptions from such provisions for domestic regulation that protects privacy and personal data illustrates the practical implications of a different baseline between protection and protectionism within a particular discourse.

3.3.5 The ‘Digital protectionism’ label as a trigger to redefine ‘barriers to trade’

622 EU model clauses on cross-border data flows.
623 Ibid. (emphasis added)
624 Ibid. (emphasis added).
This Chapter argues that in the context of the expansion of ‘protectionism’ into ‘new protectionism’ in the 1970s and 1980s that led to a fundamental redefinition of ‘barriers to trade’ and the renegotiation of international trade rules, the coining of the term ‘digital protectionism’ is a new trigger for another fundamental redefinition of what constitutes a barrier to trade and, thus, deeper trade liberalisation. Simply put, by labelling certain domestic policies such as restrictions on cross-border data flows, and data localisation measures as digital protectionism, it is much easier to critique them, reject them, and put competing policy interests such as privacy, data protection, or industrial policy in a subordinate position. Moreover, in trade terms, affixing the digital protectionism label to another country’s policy decision and insisting on the efficiency gains of free trade automatically puts that measure on the defensive.

At the dawn of the multilateral trading system governed by the discourse of embedded liberalism, the term protectionism was meant to target measures intended to protect domestic industry (as applied by the GATT for two decades or more). Within the discourse of neoliberalism, the term ‘new protectionism’ led to a removal of the intent component of the test as a relevant factor in defining a protectionism measure. The increasingly frequent use of the term ‘digital protectionism’ seems to be heading in the direction of questioning any form of regulation altogether. Despite the notable differences in the scope and types of domestic policies outlawed by digital trade provisions in the EU- and US-led trade agreements discussed in the previous Section, they have one trait in common: they are not formulated as non-discrimination provisions. While a challenge to restrictions on cross-border data flows or data localisation measures would require the contesting party to prove discrimination if such measures were challenged under the MFN obligation of the GATS, or the services chapters of post-GATS trade agreements, this Chapter argues that such a challenge under the digital trade provisions would not impose such a requirement because the measures prohibit restrictions on cross-border data flows or data localisation measures irrespective of their discriminatory character. This means that a complainant need not establish discrimination. Put simply, new digital trade provisions make it easier to challenge domestic regulation that interferes with digital trade, and make the rate of successful challenges much more probable compared to challenges under non-discrimination provisions.

Aaronson puts forward several theoretical arguments about why digital

---

628 See Section 3.2.3.
630 Ibid., pp. 6, 8, 17.
631 Art. 14.11 CPTPP; Art. 19.11 USMCA.
633 See Art. 14.11 CPTPP; see also Art. 19.11 USMCA.
protectionism is unlike other forms of protectionism and calls on the United States to lead in redefining ‘protectionism’ for the digital age.634 Her arguments are based on the premise that information is different from the objects of trade that the ‘old protectionism’ is concerned with.635 The discussion above, however, shows that this redefinition has already taken place. While it seems hard to disagree with the proposition that information is different in nature from goods and services, does that difference imply ipso facto that there is a sufficient reason to redefine protectionism? This implication is not obvious, as the characteristics that delineate protectionism from protection – the discriminatory intent or effect of domestic regulation – are not related to the objects of regulation. Therefore, the rhetoric presenting the redefinition of ‘protectionism’ as ‘digital protectionism’ as a logical, necessary step to respond to changing circumstances could be self-serving. Put differently, it could be that, just as in the case of ‘new protectionism,’ that the emergence of ‘digital protectionism’ is a product of a new digital trade discourse – and not the consequence of digital transformation of trade – which serves particular business interests and not the broader public interest.

All that said, provisions aiming at curtailing digital protectionism have already been incorporated into several trade agreements.636 Given that a different conceptualisation of digital protectionism has already led to diverging and potentially mutually inconsistent digital trade provisions, a consensus on what digital protectionism means is necessary. ‘Digital protectionism’ is defined and interpreted within a particular discourse. It follows that, to be able to reach a consensus on the meaning of ‘digital protectionism,’ countries must agree on the discourse in the first place. As things stand now, though there is an agreement on the use of the terms ‘digital trade’ and ‘digital protectionism,’ the value structures underlying the discourse are vastly different. Using the example of privacy and data protection, the following Section illustrates how fundamental values on which a discourse is based affect the baseline between protection and protectionism.

3.4 The baseline between privacy protection and protectionism: the role of discourse

One variant of the digital trade discourse, advanced in particular by the United States and demonstrated in Sections 3.3.1 and 3.3.2 above, tends to equate strict privacy and data protection measures, such as restrictions on cross-border data flows, with a non-tariff trade

634 Aaronson (2016b), pp. 58, 87 (‘Scholars and policymakers alike need to rethink how we define and measure [digital protectionism] as well as reconsider the appropriate strategies to address it. … Given the stakes, the United States should take a leading role in defining protectionism at the World Trade Organization’.)
636 See, e.g., Art. 14.11 CPTPP; Art. 19.11 USMCA; see also EU model clauses on cross-border data flows, pp. 1–2.
barrier and, potentially, digital protectionism. However, even when some degree of privacy and data protection are factored into this discourse of digital trade, the protection of these interests is often presented as an economic necessity, a precondition for free trade rather than a fundamental right and societal value beyond its economic utility. It is likely to be presented as such because the use of the digital protectionism label features trade values as natural and obvious, and forces policy makers to defend the measure against a baseline of free trade, as non-protectionist. Regulatory conversations on privacy and data protection within the economic digital trade discourse about the term ‘digital protectionism’ thus implicitly bring in the normative goal of maximisation of wealth rather than a set of goals interacting with, and counterbalancing each other.

This Section unpacks the differences between economic and legal (fundamental rights) approaches to data protection, exposes the limits of the economic approach to privacy and data protection embraced by the economic ‘digital trade’ discourse, and calls for a pluralist ‘digital trade’ discourse. It argues that, in shaping policy about the protection of privacy and personal data beyond what is economically justified, it is more likely to be labelled as protectionism in an economic discourse than in a pluralist discourse in which the protectionism label loses some of its discursive power.

3.4.1 Normative approaches to privacy and data protection

There are at least two policy approaches to the protection of privacy and personal data: (1) an economic approach in which personal data is viewed as an economic asset and its protection is a precondition of data-intensive trade; and (2) a moral value approach in which personal data is a materialised form of human behaviour and its protection is directed not to data, but to an individual’s constitutional rights. While in the first case, the normative goal of protection is to generate more trade in data, as individuals tend to share more data when they believe it is protected, in the second case the aim is the

---

637 It is, however, often recognised that other legitimate concerns could also play a role. See, e.g., Mishra (2016), pp. 150–152 (‘The contentious issues with respect to data localization extend well beyond free trade versus protectionism into some delicate, complex and legitimate political concerns, such as technology transfer and IP rights, privacy, human rights, and national security, which is currently missing (and expectedly so) on most trade agendas.’) Mitchell and Hepburn similarly concede that there might be privacy and security concerns behind restrictions on cross-border data flows, but add that ‘digital protectionism may also be at play’. Mitchell, Hepburn (2017), p. 186.


639 See Driskill (2012), pp. 2–3 (‘[T]he standard argument made by economists in favour of free trade … implicitly imposes philosophical value judgements about what is good for a nation or society, or it makes leaps of empirical faith about how the world works.’)

640 See Spiekermann-Hoff, Böhme, Acquisti, Hui (2015), p. 164 (‘Interpreting personal data as a tradable good raises ethical concerns about whether people’s lives, materialized in their data traces, should be property at all, or whether in fact personal data should be considered inalienable from data subjects’.)

641 See, e.g., Acquisti, Brandimarte, Loewenstein (2015), pp. 512–513 (showing that providing users with explicit control mechanisms over their personal data may lead to sharing more sensitive data by users).
From an economic perspective, protection of privacy and personal data has several justifications, of which the creation and maintenance of consumers’ trust is most prominently featured in the economic discourse on digital trade.643 This justification is explicitly included in the text of several EU- and US-led trade agreements.644 This economic approach serves as a normative rationale for the protection of personal data as a commercial consumer right in the United States.645 By contrast, the moral value approach views the protection of personal data rights from a broad societal perspective, as contributing to the preservation of a free and democratic society, social equality, individual autonomy, integrity, and self-determination.646 In addition, preventing and correcting discriminatory harms caused by inappropriate use of personal data can (and should) be seen as a matter of social justice.647

Importantly, these two approaches are not mutually exclusive, as economically motivated protection contributes to the protection of a fundamental right, and fundamental rights protection may have positive effects on digital commerce. The European Union is a good illustration of how these two approaches can coexist, as it simultaneously advances

---


643 See Section 3.3. Looking at the digital economy as a whole, trust meets all the criteria of a public good: it is neither rivalrous nor excludable. Without regulation, the market will not produce an optimal amount of trust necessary for the digital economy to flourish. On trust as a public good, see generally Schäfer, Ott (2004), pp. 359–360; Cohen (1992), p. 976 (‘Economists too have recognized that trust is an extremely valuable and vulnerable resource, which the market alone cannot be counted on to supply.’) For a discussion on the how privacy protection contributes to building trust, see Richards, Hartzog (2016), p. 435; Richards, Hartzog (2017), pp. 1185–1186; Joinson, Reips, Buchanan, Paine Schofield (2010), p. 4. For an overview of other economic justifications of privacy protection, see, e.g., Brown (2016), pp. 248–256.

644 See, e.g., Art. 19.8(1) USMCA (‘Personal Information Protection—The Parties recognize the economic and social benefits of protecting the personal information of users of digital trade and the contribution that this makes to enhancing consumer confidence in digital trade.’); see also Art. 14.8(1) CPTPP (a similar provision stating ‘The Parties recognise the economic and social benefits of protecting the personal information of users of electronic commerce and the contribution that this makes to enhancing consumer confidence in electronic commerce.’); Art. 8.57(4) EU-Singapore FTA; Art. 16.4 CETA (entitled ‘Trust and confidence in electronic commerce,’ which requires that parties ‘should adopt or maintain laws, regulations or administrative measures for the protection of personal information of users engaged in electronic commerce.’).


647 See Bridges (2017), p. 153 (arguing that ‘denying privacy is a mechanism for social control.’); Taylor (2017), pp. 4–8 (Showing, based on examples of big data-driven discrimination, that ‘a specific articulation of social justice is now required with regard to contemporary data technologies.’); Cinnamon (2017).
both models in the domestic and international arenas.\textsuperscript{648} In the European Union, a strong economic discourse – in which personal data and its protection are presented as enablers of the digital single market – is counterbalanced by a fundamental rights discourse.\textsuperscript{649} It is for that reason Polčák and Svantesson label the intertwined nature of economic and fundamental rights considerations in data privacy a ‘Gordian knot’.\textsuperscript{650} On the one hand, the EU privacy and data protection framework is deeply rooted in a European cultural preference for strong privacy protection and is viewed as an integral part and key instance of the protection of human dignity.\textsuperscript{651} However, as explained in Section 2.2.1.1, the history of the EU data protection regime shows that the both EU legislative instruments on data protection – the 1995 Data Protection Directive and the GDPR – are underpinned by the goal of establishing a functioning internal market, of which the protection of the fundamental rights of individuals to privacy and data protection is a necessary ingredient.\textsuperscript{652} In its communication ‘Completing a Trusted Digital Single Market for All’ the European Commission noted that it is crucial to "enable the free flow of personal data within the Union, from which the critical mass of data essential for a strong data economy can be generated."\textsuperscript{653} This rhetoric is clearly linked to the neoliberal internal and external policy discourse of the European Commission discussed above. At the same time, the Commission acknowledged the following:

\begin{quote}
[r]espect for private life and the protection of personal data are \textit{fundamental rights} in the EU. …

Strong data protection, confidentiality of communications and data security are crucial to dispel individuals’ doubts about misuse of their data and to create trust.

Without this \textit{trust}, the potential of a thriving data economy will not be met.\textsuperscript{654}
\end{quote}

\textsuperscript{648} EU model clauses on cross-border data flows, Art. 1(1). For a discussion on economic and non-economic goals of the EU data protection framework, see Section 2.2.1.1.


\textsuperscript{650} Polčák, Svantesson (2017), p. 208 (‘[D]ata privacy involves multiple fundamental human rights – the right of privacy and the freedom of expression at a minimum – and significant commercial values. Indeed, maybe we are here dealing with a Gordian knot.’)


\textsuperscript{652} For a discussion, see González Fuster (2014), p. 198; van Hoboken (2014b), p. 5.


\textsuperscript{654} Communication from the Commission, \textit{Completing a Trusted Digital Single Market for All}, COM (2018) 320 final, 15 May 2018, p. 2–3 (emphasis added). Similarly, in the explanatory memorandum to the proposal for the GDPR, the European Commission notes, on the one hand, that building a stronger and more coherent data protection framework in the European Union is essential for building the pan-European digital economy, and, on the other hand, emphasises the protection of the right to protection of personal
In a similar vein, the European Union’s most recent model clause on cross-border data flows, discussed above, states that ‘the protection of personal data and privacy is a fundamental right and that high standards in this regard contribute to trust in the digital economy and to the development of trade.’655 This illustrates that the Commission does not separate the economic and moral approaches to privacy and data protection and seems to assign equal importance to each.

In contrast to the European Commission, the CJEU has grounded the EU restrictions on transfers of personal data in the international context solely on a fundamental rights basis.656 This despite the fact that Chapter V of the GDPR, which regulates such transfers, as well as the same rules in the earlier Data Protection Directive, are, in theory, guided by the exact same economic and non-economic rationales envisaged in Article 1 of the GDPR.657 As the CJEU explained in the 2015 Schrems I judgement, limitations on transfers of personal data outside the EEA constitute a part of the European Union’s ‘constitutional’ data protection framework and are necessary to avoid circumvention of such a framework.658

Although the European Union embraces both the economic and moral value approaches to the protection of privacy and personal data, the latter will always prevail because, as already explained in Chapter 2, the European Union may neither conclude nor implement through an EU legislative act, an international agreement or decision of an international adjudicating body if it does not comply with the EU Charter.659 This matters because, although the economic and moral value rationales are complementary, the crucial difference between them is, as the next Section elaborates, that the economic justification warrants a lower level of protection than the moral value justification.

3.4.2 Limitations of the economic approach to privacy and data protection

---

655 See EU model clauses on cross-border data flows, Art. 2 (emphasis added).
656 CJEU, Schrems I, paras. 38–39, 42.
657See Art. 1; Art. 1 Data Protection Directive.
658 In the Schrems I ruling, the CJEU stated that ‘[t]he adequacy requirement’ implements the express obligation laid down in Article 8(1) of the Charter to protect personal data and . . . is intended to ensure that the high level of that protection continues where personal data is transferred to a third country’. CJEU, Schrems I, para. 72 (referring to Art. 25(6) Data Protection Directive). However, this does not affect the analysis because Art. 45 GDPR preserved the essential features of the adequacy approach. Bygrave (2002), pp. 79–80. (‘The chief aim of these rules is to hinder data controllers from avoiding the requirements of data protection laws by shifting their data-processing operations to countries with more lenient requirements (so-called “data havens”).’) This approach is now explicitly incorporated in Art. 44 GDPR, which requires that the limitations on transfers of personal data outside the EEA ‘shall be applied in order to ensure that the level of protection of natural persons guaranteed by [the GDPR] is not undermined’.
There are at least two problems with fitting privacy and data protection’s non-economic value (as opposed to the economic value of ensuring consumers’ trust in digital trade) into the economic digital trade discourse. First, non-economic interests in general, are difficult to quantify for use in the wealth maximisation calculus; it is not always possible to find convincing proof justifying the economic necessity of ensuring a certain level of privacy and data protection.\(^{660}\) For example, in *Brazil – Retreaded Tyres*, the Appellate Body held that the selection of a methodology to assess a measure’s contribution to the claimed objective in the necessity assessment in the context of a general exception ‘ultimately also depends on the *nature, quantity, and quality of evidence* existing at the time the analysis is made’\(^{661}\) (emphasis added). The elaborate discussion on the discrepancy between the levels of protection claimed and actually achieved by the EU Seal Regime in addressing public moral concerns in the EU on seal welfare, demonstrates that a defending party in a WTO dispute cannot merely assert a high level of protection.\(^{662}\) While in that particular case, arguably because the justification of the EU Seal Regime was based on the public morals exception, rather than on the exceptions aimed at *protection* of other non-economic objectives, both the WTO Panel and the Appellate Body have agreed that it was not necessary to identify ‘the exact content of the public morals standard at issue.’\(^{663}\) In contrast, the Appellate Body noted that while ‘such risk-assessment methods do not appear to be of much assistance or relevance in identifying and assessing public morals,’ ‘the focus on the dangers or risks to human, animal, or plant life or health in the context of Article XX(b) may lend itself to scientific or other methods of inquiry.’\(^{664}\) One could argue that in respect to the general exception for privacy and data protection in Article XIV(c)(ii) GATS, the analogy of Article XX(b) is closer to than that of a public morals exception. The analysis of the *EC - Seals* case by Howse and Langille, already quoted in Section 2.3.2 above, illustrates that such methods of assessment ‘that employ instrumental rationality, such as means/ends reasoning, simply does not work to establish the non-pretextual character of noninstrumental moral regulation.’\(^{665}\) Although some

\(^{660}\) See Irwin (1996), p. 221 (showing that empirical evidence ‘either played virtually no role’ or ‘played a small and unproductive role . . . in evaluating the substance of an economic argument for protection’ and that, rather, the debate about these issues was a ‘conceptual debate over economic logic’).


\(^{662}\) This discrepancy, in particular, was at the core of the Appeal by Canada and Norway of the WTO Panel Decision in the case. For example, Norway contended that ‘the Panel thus erred by holding the alternative measure *up to a benchmark level of contribution that was higher than the contribution achieved by the EU Seal Regime*. This error, Norway argues, compromised the Panel’s analysis of whether the contribution of the alternative was equal to or greater than the level actually achieved by the EU Seal Regime, and of whether the alternative was reasonably available’. (emphasis added). WTO, Appellate Body Reports, *EC – Seal Products*, para. 2.78.

\(^{663}\) WTO, Appellate Body Reports, *EC – Seal Products*, para. 5.199.


empirical research exists examining the costs of insufficient privacy protection,\textsuperscript{666} the aspects of privacy protection contributing to consumers’ trust in digital ecosystems,\textsuperscript{667} and the value (or price) of privacy,\textsuperscript{668} such research has an inherent limitation: privacy and personal data protection cannot be precisely estimated because consumers’ valuation of privacy is highly context-dependent and prone to behavioural biases.\textsuperscript{669}

The second problem is that even if privacy and personal data protection can be priced, an ‘optimal’ level of protection from an economic perspective, as this Chapter argues below, will be lower than the optimal level of such protection determined from the legal (fundamental rights) approach to privacy and data protection, because the economic calculus does not factor in the intrinsic value of privacy and data protection as a fundamental right.

From an economic perspective, the line between privacy and data protection as preconditions of trade, and as trade barriers, should be drawn based on the considerations of Pareto efficiency.\textsuperscript{670} Efficiency is defined as the maximisation of social welfare,\textsuperscript{671} where social welfare is the aggregated welfare of individual members of society.\textsuperscript{672} There is no consensus on how to define welfare; money or utility are the most widely-used proxies to evaluate welfare and suggest the most optimal regulatory option.\textsuperscript{673} In their well-known \textit{Harvard Law Review} article \textit{Fairness Versus Welfare}, Kaplow and Shavell introduce one of the most comprehensive definitions of ‘welfare’ that incorporates ‘in a positive way everything that an individual might value,’ including a taste for fairness, and

\textsuperscript{666} For empirical research attempting to quantify the chilling effects of governmental surveillance see, e.g., PEN America. (2013), p. 3; Penney (2016), pp. 145–161; Mathews, Tucker (2017), pp. 2–3.
\textsuperscript{669} See Acquisti, John, Loewenstein (2013), p. 252 (challenging the premise that privacy valuations can be precisely estimated based on theories from behavioural economics and decision research); \textit{ibid.}, p. 257 (‘The dichotomy between [willingness to pay] and [willingness to accept payment] . . . suggests that ordinary studies investigating privacy valuations may not tell us much about whether, or how much, consumers will actually pay to protect their data.’); see also Acquisti, Brandimarte, Loewenstein (2015), pp. 505–510; Wasastjerna (2018), pp. 436 (stating that privacy lacks quantifiable metrics due to the subjectivity of consumer preferences about privacy).
in a negative way anything that the ‘individual might find distasteful’. However, even this inclusive understanding of welfare does not (and should not, according to Kaplow and Shavell) include the notion of fairness as a value in itself. Kaplow and Shavell emphasise that welfare, defined in this way, should be the sole concern of legal policy makers; they criticise the legal method, which views fairness as an independent evaluative principle that should be upheld even at the expense of individuals’ well-being, because it can sometimes lead to a decrease of social welfare and make society worse-off. Similarly, the economic approach is unable to fully capture the moral value of personal data protection as a fundamental right.

A privacy and data protection policy designed with both economic and non-economic considerations in mind should arguably ensure a higher level of personal data protection than one designed with only economic efficiency considerations in mind. Put differently, the goal of privacy and personal data protection predetermines, in part, both the desired optimal level of protection and the design of the regulatory framework. If the goal is economic and instrumental, then it is justified only to the extent necessary to generate and preserve consumers’ trust (‘bottom-up regulation design’). Driven by their bottom lines, companies will only invest in privacy and data protection up to the point where the marginal costs of generating more trust will equal marginal benefits. The problem is that trust is a subjective notion. The subjective level of consumer trust that is sufficient for consumers to enter into digital transactions does not always accurately reflect the actual

674 Kaplow, Shavell (2001), pp. 980–982: The notion of well-being . . . incorporates in a positive way everything that an individual might value—goods and services that the individual can consume, social and environmental amenities, personally held notions of fulfillment, sympathetic feelings for others, and so forth. Similarly, an individual’s well-being reflects in a negative way harms to his or her person and property, costs and inconveniences, and anything else that the individual might find distasteful. Well-being is not restricted to hedonistic and materialistic enjoyment or to any other named class of pleasures and pains. The only limit on what is included in well-being is to be found in the minds of individuals themselves, not in the minds of analysts . . . . We further note a particular source of well-being . . . , namely, the possibility that individuals have a taste for a notion of fairness, just as they may have a taste for art, nature, or fine wine.

675 Ibid., pp. 967–980. Kaplow and Shavell succinctly summarise the argument: ‘whenever a notion of fairness leads one to choose a different rule from that favored under welfare economics, everyone is necessarily worse off as a result’. Ibid., p. 1012.

676 Ibid., p. 967 (stating, as their central claim, that ‘the welfare-based normative approach should be exclusively employed in the evaluating legal rules. That is, legal rules should be selected entirely with respect to their effects on the well-being of individuals in society.’)

677 See Kerber (2016), p. 857 (‘[E]conomic analysis usually focusses on welfare effects alone, which might not always grasp sufficiently the normative dimension of privacy as a fundamental right.’); see also Acquisti (2010), p. 4 (arguing that not all externalities caused by the use of personal data can be captured in economic terms); Acquisti, Brandimarte, Loewenstein (2015), p. 509.


trustworthiness of digital businesses, as consumers may not have full information or understanding on how well their personal data is actually protected by the company.\textsuperscript{682} This means that by pursuing their strategic self-interest, companies may not necessarily improve the actual trustworthiness of their digital goods or services.\textsuperscript{683} In contrast, if the protection is granted \textit{for its own sake} as independent normative significance (‘top-down regulatory design’), the level of protection will tend to be higher than the level that is necessary to advance social welfare from the welfare economics perspective.\textsuperscript{684}

In sum, the protection of personal data as a fundamental right is a type of protection that is not necessarily efficiency-enhancing in an economic sense, but it can create both economic and non-economic effects beneficial for society at large. Setting the economic approach, as just discussed, as the \textit{proper realm} of the discourse (and thus economic efficiency as the proper benchmark) predetermines the outcome.\textsuperscript{685} An emphasis on efficiency brands a broader range of domestic policies as protectionist.

When it comes to cross-border transfers of personal data, economic efficiency (or maximisation gains from international digital trade) is not the only goal of protection or restrictions.\textsuperscript{686} Even if limitations on personal data transfers, such as those imposed by the European Union, do factually restrict trade, a country may well be willing to sacrifice some gains in order to protect its constitutional, cultural, or societal values.\textsuperscript{687} As Bhagwati rightly acknowledged, when non-economic objectives, such as the intrinsic value of specific policy objectives, enter the scene, ‘free trade will generally cease to be the optimal solution’.\textsuperscript{688} Moreover, a country’s international trade policy cannot be viewed in clinical

\textsuperscript{682} See Acquisti, Brandimarte, Loewenstein (2015), pp. 512–513 (showing that the perceived and the actual levels of privacy may not coincide, and that providing users with explicit control mechanisms over their personal data may lead to sharing more sensitive data by users); see also Joinson, Reips, Buchanan, Paine Schofield (2010), pp. 16–17.

\textsuperscript{683} See Rodrik (2011), p. 227 (‘Corporations, after all, are motivated by the bottom line. They may be willing to invest in social and environmental projects if doing so buys them customers’ goodwill. Yet we shouldn’t assume their motives align closely with those of society at large, nor exaggerate their willingness to advance societal agendas. The most fundamental objection to labelling and other market-based approaches is that they overlook the social dimension of standard-setting’.)

\textsuperscript{684} Shavell (2004), p. 610. Shavell illustrates the point by the following example: ‘[I]f promise-keeping is granted independent significance, more promises will be kept than would be best if the goal were to keep promises only to advance individuals’ utilities, and whatever utility-based measure of social welfare one endorses will likely be lower than it could be’. \textit{Ibid.}; Yakovleva (2018), p. 483.

\textsuperscript{685} See Acquisti, Brandimarte, Loewenstein (2015), p. 509.

\textsuperscript{686} See Kuner (2015a), p. 2097.

\textsuperscript{687} Kuner makes a similar point. See \textit{ibid.}, p. 2096 (arguing that the central question of the economic effects of data nationalism asks is: ‘[W]hat if a country has decided that it wants to sacrifice a certain amount of economic efficiency in exchange for promoting other legitimate values that it believes are furthered by data nationalism?’).

\textsuperscript{688} Bhagwati, (1993b), p. 19 (arguing that ‘[w]hen “non-economic” objectives (such as the \textit{valuation in themselves} of specific outputs such as manufactures or high-tech industry so that a dollar worth of output is valued at four, for instance) are admitted into the analysis, free trade will generally cease to be the optimal solution’.) (emphasis added).
isolation from other domestic policies and objectives. In common with all other policies, it is (or at least should be) guided by a shared set of normative values of governmental policy in general, normative goals that are typically safeguarded by domestic constitutions. For the European Union, these principles are those contained in Articles 2, 3(5) and 21 of the Treaty on European Union, and include the universality and indivisibility of human rights and fundamental freedoms, as well as respect for human dignity, for the principles of the United Nations, and for international law. Undoubtedly, societies and governments have goals other than welfare. Susan Strange argued that efficiency falls under only one of the four basic values pursued by a politically organised society – wealth, order, justice and freedom – and in all politically organised societies, these values will be combined differently and lead to different outcomes.

The EU data protection framework – the result of a difficult political compromise between, at that time, twenty-eight member states with distinct cultures and values – may not be the best regulation, but regulation can never be perfect. In a narrow effects-based definition of ‘protectionism’ generated by neoliberal discourse, the EU framework indeed may be viewed as protectionist due to its restrictive effects on international trade. However, because of the limitations of economic discourse, this framework is not appropriate when fundamental rights are at stake. The neoliberal conception of protectionism that once drove the world trading system towards globalisation has reached a turning point where it has become a victim of its own success. A new pluralist discourse is necessary in order to allow each trading party to strike the right balance between globalisation (economic gains from digital trade and the right to conduct business), democratic politics, and domestic autonomy to pursue domestic values such as fundamental

---

690 Strange (1985), p. 236 (‘The basic premise that state policy should, or even can, be based on the single criterion of maximizing efficiency in the production of goods and services for the market is demonstrably false’.)
691 Ibid., p. 237:

Efficiency, in short, is only one of four basic values that any politically organized society seeks to achieve for its members. Wealth, order, justice, and freedom; these are the basic elements of political compounds just as hydrogen, oxygen, and carbon are the essential elements of some chemical compounds. And just as chemical elements can be combined differently to produce oil, wood, or potatoes, so basic values will be combined differently in all politically organized societies to produce, for example, fast-growing authoritarian states or slow-growing democracies, or conversely, fast-growing democracies or slow-growing police states. See also Polčák, Svantesson (2017), p. 209 (‘While the Internet is often seen as borderless in nature and global in scope, the physical work and the people that inhabit that world are still divided by fundamentally different cultures and values; and even where common values are found, those values are weighted in different ways.’)
rights to privacy and data protection. 696

Yet European integration and the resulting economic power of the European Union not only directs its energies inwards, but is also, to a large extent, an outward-looking strategy: while it improves internal trade within the European Union, it also improves the European Union’s negotiating positions in external economic relations and in the negotiations of international treaties. 697 It also contributes to the expansion of European standards and values around the world, a phenomenon labelled by Anu Bradford as the ‘Brussels Effect’. 698 The presence of political and economic rationales for the unification of data protection rules in the European Union, however, does not diminish the fact that the level of data protection guaranteed by the unified rules is a projection of a European vision of governance and cultural values. 699

Schwartz and Peifer attest that ‘[t]here is no constitutional right to information privacy in the United States analogous to the EU’s right to data protection.’ 700 The Fourth Amendment 701 only applies to government searches and seizures; it does not apply to government processing of personal data in already existing data bases. 702 Neither does it apply to the processing of personal data in the commercial context. 703 In the commercial sphere, protection of information privacy tends to be anchored in the ‘marketplace discourse’. 704 It is aimed at protecting consumer welfare rather than constitutional rights. 705 The legal weight of such protection is thus lower than, for example, that of the

696 Ibid., p. 200 (pointing at a ‘fundamental political trilemma of the world economy,’ meaning that it is impossible to simultaneously pursue democracy, national self-determination, and hyper-globalization).


698 See ibid.

699 See Reidenberg (2000), pp. 1319–1320 (‘[S]pecific privacy rules in any particular country have a governance function reflecting the country’s choices regarding the roles of the state, market, and individual in the country’s democratic structure. Under this governance theory of privacy, national differences derive from distinct visions of governance, and privacy rules strive to protect a state’s norm of governance, whether it be a liberal market norm or a socially-protective, citizen’s rights norm’); see also Milberg, Smith, Burke (2000), p. 47 (based on the empirical study of samples from nineteen different countries, the authors concluded that ‘[a] country’s cultural values are associated strongly with the privacy concerns that are exhibited by its populace (Hypothesis 1) and are associated marginally with its regulatory approach (Hypothesis 2)’.)


701 Amendment IV to the US Constitution reads as follows:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.


703 Ibid., p. 132-133.

704 Ibid., p. 136.

constitutional right to freedom of expression. Recall, in addition, that a more liberal approach to data protection in the United States not only echoes US cultural values, but also factors in the US strategy of preserving global dominance in the information technology industry.

To sum up, the core of the debate between the European Union and its trading partners is not about whether the protection of privacy and personal data is legitimate as such, but rather about what level of protection is legitimate. As differences in data protection approaches (including to the issue of cross-border transfers of personal data), are fundamentally rooted in a delicate balance between the different values pursued by a politically organised society, a related question arises: whether international trade should be tasked with the mission to reduce or remove this diversity, and if so, how to determine the right level of protection and the right level of deference to domestic interests and values?

3.5 Concluding remarks: towards a new digital trade regime

This Chapter has demonstrated that it is not possible to strike the right balance between digital trade liberalisation and the protection of data privacy by simply ruling out ‘protectionism’. It has argued that the choice of the right discourse for policy conversations on domestic privacy and the protection of personal data in the context of negotiating and interpreting international trade law is crucial. The value structures attending it will ultimately predetermine where the line will be drawn between legitimate privacy and personal data protection, and illegitimate protectionism, both in the relevant provisions of international trade agreements and in the interpretation of such provisions by trade adjudicating bodies.

Deliberations on the distinction between protection and protectionism show that it is not clear-cut: drawing a line beyond which protection should be viewed as protectionism is ultimately a judgement call. On a spectrum between the two extremes, there is a grey

---

706 Schwartz, Solove (2014), pp. 880–881 (stating that the right to privacy in the United States ‘may even be secondary to other concerns, such as freedom of speech’); see also Schwartz (2013), pp. 1976–1977 (‘The First Amendment’s protections for freedom of expression . . . help define the U.S. orientation to privacy regulation’). Although in some cases the First Amendment can ‘bolster privacy,’ most of the time it is used to limit privacy: ‘statutes that limit information sharing on privacy grounds are subject to constitutional scrutiny of their impact on the speech of the data processor’. Ibid. (emphasis omitted). See also Petkova (2019); Whitman (2004).

707 See Section 3.3.3.

708 Cf. Marceau, Trachtman (2014), p. 352 (‘The distinction between a protectionist measure—condemned for imposing discriminatory or unjustifiable costs—and a non-protectionist measure restricting trade incidentally (and thus imposing some costs) is sometimes difficult to make’); see Sykes (1999), p. 33 (‘It is exceedingly difficult to devise a workable and palatable legal rule to condemn regulatory measures that are necessary to nonprotectionist regulatory goals but that are nevertheless undesirable because of their trade
area that includes domestic measures, with an element of uncertainty as to what type of regulatory goal is at stake: protectionism in disguise or genuine protection, which only incidentally benefits domestic industries. Whether measures in this grey area should fall under the label of ‘protection’ or ‘protectionism’ – in other words, whether trade adjudicating bodies should err on the side of protection or protectionism — essentially depends on the discourse. Within an economic discourse, where free trade alone is high on the value scale, such regulation should be excluded as protectionist. In contrast, in a pluralist discourse where equal value is assigned to free trade and protection of fundamental rights, letting some disguised protectionist measures slip through in order to safeguard states’ domestic autonomy to adopt socially beneficial regulation may be a preferred approach.

This Chapter contends that the distinction between privacy and personal data protection, and protectionism is in part a moral question, that is, not just a question of economic efficiency. As Romer, a Nobel Prize winning economist explains, ‘[s]cientific authority never conveys moral authority. No economist has a privileged insight into questions of right and wrong, and none deserves a special say in fundamental decisions about how society should operate.’ Therefore, when a policy conversation, such as the one on cross-border flows of personal data, involves non-economic spill-over effects to individual rights, such conversation should not be confined within the straightjacket of trade economics, but rather placed in a broader normative perspective. The economic digital trade discourse, advanced by some states (most notably the United States), and reflected in the recently concluded CPTPP, USMCA and US-Japan Digital Trade Agreement, subordinates non-economic values, such as the protection of privacy and personal data taken as moral values, to efficiency and to ill-defined welfare enhancement goals. As a result, only an economically justified – and lower – level of privacy and data protection, as compared to that warranted by a pluralist discourse, is able to qualify as not protectionist. This thesis argues that the political economy arguments against privacy and data protection beyond economic necessity should be taken with a grain of salt, precisely

impact. As a result, this task is left to case-by-case bargaining.’); see also Howse (2012), pp. 441–443 (‘Regulations serve diverse objectives and reflect compromises between different groups. In such circumstances, it is not simple to draw a line between internal policies that are legitimate exercises of domestic regulatory autonomy (even if they have some trade-restrictive effects) and those that can be considered a form of protectionism or “cheating” on the WTO bargain, in that they undermine the market access reasonably expected from commitments on liberalization of border measures in the multilateral trading system’.); Howse (2002), p. 96.

710 Romer (2020).
711 Additionally, these goals often do not reflect negative externalities of economic growth (e.g., environmental degradation) and thus take a narrow view of ‘welfare’.
712 See Section 3.3.4.
because those who are putting them forward may themselves be suffering from capture by those profiting from unrestricted cross-border data flows.

From a global perspective, the inchoate use of the terms ‘protectionism’ and ‘digital protectionism’ in different discourses by the European Union and the United States exposes a deeper challenge to the present day multilateral trade negotiations. Having chosen digital protectionism as the main stumbling block on the path of digital trade, trading partners focus more on these labels and their definition, while shying away from more fundamental questions about the goals and values of future (digital) trade. This thesis contends that this path is misguided: there exist as many definitions of (digital) protectionism as there are discourses, which the EU and US examples clearly demonstrate. Using the same terminology, these trading partners advance utterly different discourses built upon different views on where the balance between trade and privacy should be struck. Against this backdrop, this Chapter contends that countries should rethink the goals of international trade for the twenty-first century.

On the subject of restrictions on cross-border flows of personal data, this thesis argues that such restrictions are, and will remain, necessary. Unless approaches to data protection and privacy are harmonised (which, arguably, is not the route to follow due to the lack of a (political) basis for such harmonisation, differences between countries, and the danger of settling for the lowest common denominator), countries need more regulatory space to determine the design of domestic data protection regimes. It is precisely because data protection standards in other countries are low (perhaps, strategically low) that countries with higher standards need to impose restrictions on personal data transfers.

When it comes to the consequences of removing restrictions on cross-border flows of personal data in domestic privacy and data protection regimes and the ways to avert them, one could draw a parallel with restrictions on financial data flows, which are essential to ensure financial stability in a country. Rodrik has eloquently argued the following:

Financial globalization in effect neutralizes differences in national regulations. This is what is known in the trade as “regulatory arbitrage,” a race to the bottom in finance. For this reason, a commitment to regulatory

---

713 See Section 3.3.
715 See also Section 5.2.5 arguing that these restrictions constitute part of the essence of the fundamental rights to privacy and the protection of personal data.
716 On the prospects of harmonising data protection regimes, see, e.g., Milberg, Smith, Burke (2000), p. 53 (‘What will or will not meet “societal expectations” is highly contingent on a society itself. Thus, a universal regulatory approach to information privacy seems unlikely and would ignore cultural and societal differences.’); see also Kuner (2011), p. 8; Keller (2011), p. 348–351. But see Mattoo, Meltzer (2018a), p. 769 (arguing that a common privacy framework could be based on the OECD and APEC data protection frameworks).
diversity has a very important corollary: the need for restrictions on global finance . . . Governments should be able to keep banks and financial flows out—not for financial protectionism but to prevent the erosion of national regulations. Hence a new global financial order must be constructed on the back of a minimal set of international guidelines and with limited international coordination. Most important, the rules would explicitly recognize governments’ right to limit cross-border financial transactions, insofar as the intent and effect are to prevent foreign competition from less strict jurisdictions from undermining domestic regulatory standards.\textsuperscript{717}

This line of reasoning, this thesis argues, applies equally to restrictions on cross-border transfers of personal data. Deep harmonisation of domestic privacy and data protection standards would also require a more extensive form of global governance.

4. Reconciling data privacy and global data flows the EU way

4.1 Introduction

In Chapter 2 this thesis demonstrated that, if challenged under international trade law, the EU’s framework for transfers of personal data outside the EEA might run afoul of the EU’s international trade commitments, such as those under the GATS. If found incompatible with those trade commitments, the framework may not be able to be justified under the necessity test of the general exception for the protection of the privacy of individuals in relation to the processing and dissemination of personal data under Article XIV(c)(ii) GATS (for the purposes of this Chapter, referred to as the ‘general exception for privacy and data protection’). One of the main reasons for that is that the necessity test, as interpreted by the WTO adjudicating bodies, provides the EU and other WTO members insufficient autonomy – from an EU law perspective – to protect privacy and personal data as fundamental rights. Chapter 2 also shone a spotlight on the EU’s constitutional constraints on bringing the EU’s legal framework for data transfers into compliance with the current international trade rules and, in particular, with the general exception for privacy and data protection. As a result, if the EU restrictions on transfers of personal data were successfully challenged in the WTO, the EU would face a catch-22 situation, having to choose between compliance with its trade commitments, and upholding its constitutional values. A way to avoid this problem\footnote{For a discussion on why this problem has to be addressed, see Section 2.3.1.} in future trade agreements, as suggested in Chapter 2, is to reform both the general exception for privacy and data protection, and the EU’s framework for transfers of personal data. This Chapter explores the possibilities of developing the former, while the next Chapter delves into the options for reforming the latter.

As already briefly mentioned in the Introduction and Section 3.3.4 above, in 2018, to address the international trade law aspect of this issue, the EU developed horizontal provisions on cross-border data flows and the protection of privacy and personal data for its prospective digital trade agreements (for the purposes of this Chapter referred to as the ‘proposed horizontal provisions’ or the ‘proposed model clauses’).\footnote{EU model clauses on cross-border data flows.} These clauses, in particular, contain a broader exception for domestic privacy and data protection rules (for the purposes of this Chapter referred to as the ‘digital trade exception for privacy and data protection’) than warranted by the existing general exception for privacy and data protection. The EU has included these model clauses in its proposals for digital trade chapters in bi-lateral trade agreements, such as those with Australia, New Zealand, Chile,
Indonesia and Tunisia,\textsuperscript{720} and in multilateral negotiations on electronic commerce at the WTO ever since.\textsuperscript{721} The EU continued to do so after the formation of the new European Commission in 2019, as the EU proposal for the digital trade chapter in the bi-lateral trade negotiations with the UK (following Brexit)\textsuperscript{722} illustrates. In the words of the new European Commission, the horizontal provisions ‘rule out unjustified restrictions, such as forced data localisation requirements, while preserving the regulatory autonomy of the parties to protect the fundamental right to data protection.’\textsuperscript{723} They serve the goals of ‘promoting convergence of data protection standards at international level, as a way to facilitate data flows and thus trade,’ on the one hand, and ‘to tackle digital protectionism, on the other hand.\textsuperscript{724} This rhetoric is very similar to that of the previous European Commission in relation to the proposed model clauses,\textsuperscript{725} which illustrates the continuity of the European Commission’s trade policy on the issues of cross-border data flows and the protection of privacy and personal data. Beyond the above-mentioned specific goals, the proposed model clauses are a part of the EU’s broader policy to ground its external relations on the EU’s values and strengthen its technological sovereignty.\textsuperscript{726} In its recent Data Strategy, the European Commission communicated its vision to maintain an ‘open, but assertive approach to international data flows, based on European values.’\textsuperscript{727} Similarly,

\textsuperscript{720} See EU proposal for a Chapter on Digital Trade of the EU-New Zealand FTA; EU proposal for a Chapter on Digital Trade of the EU-Australia FTA; La proposition de l’Union européenne (UE) relative à l’Accord de libre-échange UE-Tunisie UE-Tunisie, Titre [ ] Commerce Numérique, 9 November 2018; Digital Trade Proposals for EU-Chile and EU-Indonesia were drafted before the European Union agreed on the model provisions. Therefore, these proposals only contain a placeholder for a provision on cross-border data flows. EU proposal for a Digital trade title in the Trade Part of a possible modernised EU-Chile Association Agreement, 5 February 2018 (containing a placeholder for provisions on data flows); EU proposal for a Chapter on Digital Trade of the EU-Indonesia FTA, 27 July 2017. The European Union tabled its model clauses at a later stage in negotiations with these two countries. See, e.g., European Commission, Report of the 5th Round of Negotiations for a Free Trade Agreement Between the European Union and Indonesia, July 2018.


\textsuperscript{722} Draft text of the Agreement on the New Partnership with the United Kingdom, European Commission, 18 March 2020.


\textsuperscript{725} In the Communication from the Commission to the European Parliament and the Council, Data Protection Rules as a Trust-Enabler in the EU and Beyond – Taking Stock, COM(2019) 374 final, 24 July 2019 the European Commission stated that the ‘horizontal provisions rule out purely protectionist measures, such as forced data localisation requirements, while preserving the regulatory autonomy of the parties to protect the fundamental right to data protection’.

\textsuperscript{726} Communication from the Commission, Strengthening the Rule of Law Within the Union. A Blueprint for Action, COM/2019/343 final, 17 July 2019.

in its recent White Paper on Artificial Intelligence (AI), the European Commission stated that it ‘will strive to export its values,’ such as the protection of privacy and personal data, ‘across the world’ in its efforts for international cooperation on AI. Simultaneously, the EU trade policy ‘champions multilateralism and a rules-based global order’.

The EU proposed horizontal provisions that consist of three components: an article on cross-border data flows (Article 1), an article on the protection of personal data and privacy (Article 2), and an article on cooperation on regulatory issues with regard to digital trade (Article X). This proposal is typically included in EU proposals for standalone chapters on digital trade. For the reader’s convenience, this Section includes the text of Articles 1 and 2 below. Article 1 of the EU’s proposal (referred to in this Chapter as the ‘cross-border data flows provision’) reads as follows:

1. The Parties are committed to ensuring cross-border data flows to facilitate trade in the digital economy. To that end, cross-border data flows shall not be restricted between the Parties by:

   a) requiring the use of computing facilities or network elements in the Party’s territory for processing, including by imposing the use of computing facilities or network elements that are certified or approved in the territory of the Party;

   b) requiring the localisation of data in the Party's territory for storage or processing;

   c) prohibiting storage or processing in the territory of the other Party;

   d) making the cross-border transfer of data contingent upon use of computing facilities or network elements in the Party’s territory or upon localisation requirements in the Party’s territory.

---

729 Borrell (2020) (stating that ‘[t]he EU has a strong stake in maintaining and developing a rules-based international order within the framework of an effective multilateralism – even if others are clearly trying to weaken it. The joint Communication on Multilateralism that we are planning for next year will set out what the EU can do to counter this trend.’) See also European Commission, A Stronger Europe in the World; Communication from the Commission, A Balanced and Progressive Trade Policy to Harness Globalisation, COM(2017) 492 final, 13 September 2017, p.3 (stating that ‘[t]he EU is committed to open trade anchored in the rules-based multilateral trading system’).
730 The document containing the model clauses does not explain why this article is numbered as ‘X’ instead of ‘3’. This Section hypothesises that the reason for that is that unlike Arts. 1 and 2 of the model clauses, which are included in Digital Trade chapters, Article ‘X’ is to be included in Chapters on Regulatory Cooperation. Given that the exact number of this article in that chapter could be different depending on the agreement, the drafters of the proposed model clauses preferred to not give this article a specific number.
731 Article X is beyond the scope of this thesis because regulatory cooperation is not relevant to the research question addressed in it.
2. The Parties shall keep the implementation of this provision under review and assess its functioning within 3 years of the entry into force of this Agreement. A Party may at any time propose to the other Party to review the list of restrictions listed in the preceding paragraph. Such request shall be accorded sympathetic consideration.

Article 2 on the protection of personal data and privacy, includes an exception from the provision on cross-border data flows. It reads as follows:

1. Each Party recognises that the protection of personal data and privacy is a fundamental right and that high standards in this regard contribute to trust in the digital economy and to the development of trade.

2. Each Party may adopt and maintain the safeguards it deems appropriate to ensure the protection of personal data and privacy, including through the adoption and application of rules for the cross-border transfer of personal data. Nothing in this agreement shall affect the protection of personal data and privacy afforded by the Parties' respective safeguards.

3. For the purposes of this agreement, "personal data" means any information relating to an identified or identifiable natural person.

4. For greater certainty, the Investment Court System does not apply to the provisions in Articles 1 and 2 (emphasis added).

Looking ahead, the digital trade exception for privacy and data protection is likely to be included in addition to the general exception for privacy and data protection, replicating almost verbatim the general exception in the GATS, as the EU proposal for general exceptions in the trade agreement with New Zealand demonstrates.

This Chapter questions whether the proposed model clauses would indeed allow the EU to overcome the potential catch-22 compliance deadlock in future trade agreements, while at the same time pursuing the goals of facilitating cross-border data flows and promoting a rules-based multilateral trading system. It argues that superficially the clauses do seem to provide the EU with the broad autonomy to protect privacy and personal data.

---

732 There is a degree of uncertainty as to whether the proposed provision of Art. 2(2) of the model clauses is actually designed as an exception or rather as a carve-out from the scope of the agreement. This uncertainty originates from the lack of any indication in the provision itself of its actual function. However, comparison of this provision with provisions in existing trade agreements, which have similar wording (e.g. the prudential exception in Art. 2(a) of the GATS Annex on Financial Services and the prudential exceptions in Art. 195(1) EU-Central America Association Agreement, Art. 7.38(1) EU-Korea FTA, and Art. 8.50 EU-Singapore FTA) and are consistently interpreted as exceptions in literature and WTO case law suggests that Art. 2(2) of the model clauses should be viewed as an exception. See WTO, Background Note by the Secretariat, Financial Services, S/C/W/312, S/FIN/W/73, 3 February 2010, para. 28; WTO, Panel Report, Argentina – Financial Services, para. 7.814; 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. For further discussion see Cantore (2014), pp. 1232, 1242; Cottier, Krajewski (2010), pp. 826-827; Leroux (2002); Marchetti (2011); Von Bogdandy, Windsor (2008); Yokoi-Arai (2008); Mitchell, Hawkins Mishra (2016), p. 807.

733 Art. X.1(2) EU proposal for Chapter X Exceptions of the EU-New Zealand FTA.
as fundamental rights while outlawing a number of measures restricting cross-border data flows. Compared to the US model, already discussed in Chapter 3 – which is the only wording so far incorporated in actual trade agreements, such as the CPTPP, USMCA and the US-Japan Digital Trade Agreement\(^{734}\) – the prohibition of restrictions on cross-border data flows in Article 1 of the proposed model clauses is formulated more narrowly. While the above-mentioned US-led agreements contain a general obligation to allow cross-border data flows, Article 1 of the EU proposed model clauses contains an exhaustive list of restrictions on cross-border data flows that are outlawed by this provision. Article 2(1) of the proposed model clauses asserts that the normative rationale for the protection of personal data and privacy is the protection of fundamental rights. As demonstrated in Section 3.4.2, this rationale safeguards a higher level of privacy and data protection than that afforded by economic reasons for protecting privacy and personal data, and therefore arguably safeguards a broader autonomy to regulate vis-à-vis international trade commitments. This provision is likely to be interpreted as a part of the digital trade exception for privacy and data protection in Article 2(2) of the proposal. In addition, the breadth of this digital trade exception, modelled after the national security exceptions in the WTO Agreements, secures the EU’s ability to maintain restrictions on transfers of personal data outside the EEA under the GDPR. In particular, the ‘it deems appropriate’ threshold of the proposed exception establishes a significantly lower threshold than the necessity test of the general exception (this issue is discussed in more detail in Section 4.2.3 below). In addition, the proposed exception explicitly recognises the rules for cross-border transfers of personal data as an example of the types of measures that would be allowed under the exception. Incorporating the recognition of privacy and personal data protection as fundamental rights in trade agreements, coupled with the possibility of maintaining the above-mentioned GDPR restrictions, serves the goal of exporting EU data protection framework worldwide.\(^{735}\)

However, the proposed model clauses suffer from at least three essential flaws that could make them unable to safeguard the fundamental rights to privacy and the protection of personal data, and undermine the goals of the EU digital trade policy, as identified above. First, the unclear relationship of the proposed digital trade exception for privacy and data protection with the general exception, creates legal uncertainty as to the material scope of the proposed exception.

Second, the breadth of the proposed digital trade exception for privacy and data protection may nullify the impact of the provision of Article 1, which outlaws what the EU frames as ‘digital protectionism’. More generally, this Chapter contends that using the

\(^{734}\) See Section 3.3.4.

\(^{735}\) See Section 5.3.2.
extremely low threshold of national security exceptions as a model for a digital trade exception for privacy and data protection, could further undermine the stability of the rules-based international trading order. This essentially creates an almost unconditional escape valve from virtually any trade commitment as long as there is at least a remote nexus to the protection of privacy and personal data. Using this threshold outside the national security context creates a de facto hierarchy between privacy and data protection, on the one hand, and other public policy objectives, such as protection of the environment or public health (which are still subject to the stricter necessity test of the general exception), on the other hand. This could lead to the replication of the same threshold in exceptions for such other policy objectives. Such replication could, on the one hand, lead to the weakening of the trading system. On the other hand, it could also lead to a more restrictive interpretation of the ‘it considers necessary’ threshold of the national security exception. This, in turn, would reduce the broad autonomy of states to protect their national security in spite of their international trade commitments – the goal for which this low threshold was introduced into international trade law in the first place.

Third, the proposed model clauses are overly EU-centric in the sense that they require a recognition of the protection of privacy and personal data as fundamental rights – a commitment that not all EU trading partners may be willing to accept.

Based on the analysis of the proposed model clauses, this Chapter argues that these clauses could be improved in at least three ways. First, as a minimum, the future trade agreements should include a provision clarifying the relationship between the general and the digital trade exceptions for privacy and data protection. As a maximum, although this could be problematic to implement in practice, future trade agreements should contain a single exception for privacy and data protection, which would apply throughout the agreement. Second, in the course of negotiations, the EU should consider replacing the ‘it deems appropriate’ threshold of the digital trade exception for privacy and data protection with a threshold which is higher than the ‘it deems appropriate’ standard but lower than the necessity test standard of the general exception. Third, the provision requiring the recognition of the parties that the protection of personal data and privacy is a fundamental right should be rephrased in a way, which, on the one hand, safeguards the EU’s autonomy to maintain its fundamental rights protection of these rights but, on the other hand, allows other trading partners to adopt a lower level of protection, if they so choose, within international human rights law bounds.

Considering that the proposed digital trade exception for privacy and data protection is only a starting point in negotiations, Section 3 of this Chapter considers alternative thresholds for this exception that the EU could fall back on without compromising on the fundamental rights to privacy and data protection. It looks at other alternatives found in
WTO agreements and bi-lateral and regional trade agreements, which are on the continuum between the ‘necessity’ in the general exception, which is the current test for privacy and data protection, and the ‘it deems appropriate’ test proposed for a digital trade exception for privacy and data protection by the EU. Those alternatives are non-circumvention; non-avoidance; reasonableness; and the prohibition of arbitrary or unjustified restriction on trade. Relying on the interpretation of these thresholds in WTO case law and academic literature, Section 3 of this Chapter demonstrates that the principles of good faith and the prohibition of abuse of rights are the common denominators of all these thresholds. The flexibility of these principles is both a blessing and a curse. On the one hand, it gives adjudicating bodies wiggle-room to adjust the application of these thresholds to specific circumstances, but, on the other, it vests adjudicating bodies with broad discretionary powers, which can only be performed responsibly in the presence of appropriate checks and balances. The Chapter then argues that the issue in designing a digital trade exception for privacy and data protection is not only about the wording of the threshold for domestic autonomy to protect these policy interests, but also, and most importantly, about the amount of discretion afforded to the adjudicating bodies. As Chapter 3 has demonstrated, by using their discretion, the adjudicating bodies can — under the influence of a particular discourse — change the breadth of the exception by means of interpretation. Therefore, to ensure more predictability and control for the parties to a trade agreement over the interpretation of the threshold of the digital trade exception, restrictive mechanisms are necessary. In sum, this Chapter argues that the standards of non-circumvention, non-avoidance and reasonableness could be viable alternatives to the ‘it deems appropriate’ standard, provided that they are accompanied by appropriate restrictive mechanisms constraining the discretion of trade adjudicators, and are applied in a nuanced manner. The use of the ‘prohibition of arbitrary or unjustified restriction on trade’ standard, however, is undesirable due to the risks of importation of existing WTO case law on the chapeau of the general exceptions, which, as this Chapter shows, has at times been interpreted in an overly restrictive manner for domestic regulatory autonomy.

This Chapter proceeds as follows. Section 2 explicates the background of the proposed horizontal provisions, exposes the weaknesses of those provisions against the benchmark of their aims as outlined by the European Commission and in light of the broader goal of the preservation of the rules-based international trading system, and outlines ways for remedying those weaknesses. Section 3 discusses possible alternatives for the threshold of the future digital trade exception for privacy and data protection, instead of the proposed ‘it deems appropriate threshold’. Based on their interpretation in WTO case law and academic literature, Section 3 evaluates which of them could be more apt in the light of the above-mentioned goals. Section 4 sums up the main conclusions of the Chapter.
4.2 EU horizontal provisions: a critical evaluation

4.2.1 Background

The proposed model clauses represent a political compromise between what can be seen as the offensive and defensive strategies coexisting in EU trade policy on cross-border data flows and the protection of privacy and personal data. The offensive strategy is the product of the European ‘digital trade’ discourse, grounded in the economic benefits of the absence of restrictions on cross-border data flows abroad for European businesses. In contrast, the defensive strategy is the product of the fundamental rights discourse, grounded in the moral value of the fundamental rights to privacy and the protection of personal data at home, and geared towards protecting EU data protection legislation, most specifically GDPR’s restrictions on transfers of personal data outside the EEA from being challenged in a trade forum.

Developed under a strong political pressure from the European Parliament, DG Justice, civil society organisations, and academics, the proposed model clauses are not only a set of legal provisions delineating the EU’s starting point in international trade negotiations, but also largely an inward-looking political statement. In terms of regulatory autonomy for domestic privacy and personal data protection rules, the proposed model clauses go a step further than their predecessor - the 2017 EU Council concept paper on data flows in trade agreements, discussed in Section 4.3.1 below. Unable to reach an internal consensus on the EU Council’s proposal, the EU ultimately refrained, as mentioned elsewhere, from including any commitments on cross-border data flows and the protection of privacy and personal data into the E-Commerce chapter of JEFTA, which was in the final stages of negotiations at that time. In its 2018 statement outlining the key elements of this agreement, the European Commission clearly laid out the EU’s position on this matter: ‘[d]ata protection is a fundamental right in the European Union and is therefore not up for negotiation. Privacy is not a commodity to be traded.’ This statement, however, as Kanetake and de Vries argue, was largely a narrative maintained by the EU for its own constituencies. Although the final version of JEFTA did not cover cross-border data flows or privacy and data protection, these issues were negotiated within the framework of adequacy assessments under the GDPR which unfolded in parallel with trade negotiations. The EU and Japan agreed to recognise the ‘essential equivalence’ of each other’s data protection frameworks – the key benchmark of adequacy under the GDPR.

---

736 See also Section 3.3.2.
739 As explained in Section 2.2.1.3, adequacy decisions adopted by the European Commission constitute a primary mechanism for transfers of personal data outside the EEA under the GDPR.
— on the day when both parties signed the trade agreement. Kanetake and de Vries contend that the fact that the EU awarded an adequacy decision to Japan, despite the gaps between the GDPR and the Japanese data protection framework, demonstrates that contrary to the mainstream narrative of the Commission, privacy and data protection were very much ‘negotiated and traded’. The weaknesses of the adequacy decision which resulted from these negotiations, in the light of the EU Charter, are addressed in more detail in Chapter 5 of this thesis. It is important to keep in mind that — unlike trade agreements — adequacy decisions, even if adopted ‘mutually’ by two trading partners, are unilateral decisions of each trading partner. This means that they can also be unilaterally revoked without the risk of adverse consequences under the trade agreement. From this perspective, an adequacy decision does not substitute for a binding provision on data flows in a trade agreement.  

4.2.2 Relationship with the general exception

Unlike most other trade law disciplines, the proposed model clauses – intended to form a part of the future digital trade chapters – apply to information flows in electronic commerce in general, irrespective of whether they are related to goods or services, or constitute part of financial or telecommunication services, and are, in this sense, horizontal. Therefore, the provisions of Articles 1 and 2 would apply in addition to other obligations under the trade agreement on trade in goods and services. For example, information flows can also be relevant in the context of trade in database services, and as such can also be captured by more traditional trade disciplines, such as MFN, national treatment and market access. As Bartl and Irion rightly concluded, removing a data flow provision from the e-commerce chapter ‘does not remove personal data from the emergent trade law institutions.’ In a similar vein, the general exception for privacy and data protection – modelled after GATS Article XIV(c)(ii) – is typically included in the EU proposals for the Exceptions chapters of the same trade agreements, where the EU includes

742 Draft digital trade chapters proposed by the EU define the scope of application of those chapters as ‘trade enabled by telecommunications and/or other information and communication technologies’ (see, e.g., Art. X.1(1) EU proposal for a Chapter on Digital Trade of the EU-Indonesia FTA; Art. I(1) EU proposal for a Digital trade title in the Trade Part of a possible modernised EU-Chile Association Agreement) or as ‘measures of a Party affecting trade enabled by electronic means’ (see, e.g., Art. I(1) EU proposal for a Chapter on Digital Trade of the EU-New Zealand FTA; or Art. 1(1) La proposition de l’Union européenne (UE) relative à Accord de libre-échange UE-Tunisie UE-Tunisie, Titre [ ] Commerce Numérique). The scope of these chapters can be limited. For example, it typically exempts audio-visual services exempting financial services. See, e.g., Art. 1(2) EU proposal for a Chapter on Digital Trade of the EU-New Zealand FTA.
743 Whether these services are captured by national treatment and market access obligations, which represent specific commitments under trade agreements, depends on whether the EU has liberalised these services in each particular trade agreement. These services are included in the EU’s schedules of specific commitments under the GATS. Sen (2018), p. 336.
the proposed model clauses in the digital trade chapter.\textsuperscript{745} Similarly, ongoing e-commerce negotiations at the WTO,\textsuperscript{746} for which the EU submitted its proposed model clauses, are unlikely to include a revision of the GATS general exceptions. This creates a situation where \textit{two exceptions must cohabit in the same trade agreement} (one in the digital trade chapter and the other in the general exceptions), with significantly different thresholds for justifying privacy and data protection measures inconsistent with the provisions of the agreement, as the following section illuminates.

Despite the difference in the wording of the privacy and data protection interests in the two exceptions, their scope in the context of present-day international trade is nearly identical. The proposed digital trade exception for privacy and data protection exempts domestic measures that ‘ensure the protection of personal data and privacy’. The general exception proposed for the same trade agreement exempts measures protecting ‘the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts.’\textsuperscript{747} Because of their connection to a particular person, individual records and accounts would constitute personal data under most data protection regimes.\textsuperscript{748} Similarly, confidentiality of personal data is a necessary component of most data protection frameworks.\textsuperscript{749} During the Uruguay round (1986-1994), the protection of the privacy of individuals in relation to the processing and dissemination of person data, and the protection of the confidentiality of individual records and accounts could have been different concepts, as at that time many WTO members, including the EU, did not have dedicated data protection laws. Nowadays, the second concept has become a subset of the first, and the difference in wording between the general exception, and the proposed digital trade exception for privacy and data protection is better explained by historical reasons than by the intention of the parties to exempt a different scope of privacy and data protection interests.

The EU proposals for digital trade chapters do not contain any provisions regulating the relationship between the digital trade chapter and other provisions of the trade agreements incorporating such a chapter. These EU proposals do, however, clarify that the general exception, security exception and prudential carve-out also apply to the digital trade chapter.\textsuperscript{750} The absence of a conflict of laws provision in currently proposed digital

\textsuperscript{745} Art. X.1(2) EU proposal for Chapter X Exceptions of the EU-New Zealand FTA. Proposed Chapter on exceptions in other FTAs under negotiation are not available at the time of writing.


\textsuperscript{747} See, e.g., Art. XIV(c)(ii) GATS.

\textsuperscript{748} See DLA Piper (2020).

\textsuperscript{749} Ibid.

\textsuperscript{750} See also Art. 3 EU proposal for a Chapter on Digital Trade of the EU-Australia FTA; Art. 3 La proposition de l’Union européenne (UE) relative à Accord de libre-échange UE-Tunisie UE-Tunisie, Titre [
trade chapters stands in sharp contrast to the two most recently concluded trade agreements by the EU, namely the JEFTA and the CETA. The electronic commerce chapters of both of these agreements state that in case of any inconsistency between the electronic commerce chapter and other provisions of the trade agreement, those other provisions will prevail to the extent of the inconsistency.\footnote{Commerce Numérique; EU proposals for Digital Trade chapters for EU-Indonesia FTA and Digital trade title of a possible modernised EU-Chile Association Agreement only contain a placeholder for such a provision. It states that ‘such provisions will either apply to this title but be incorporated in another title or be incorporated in this title’.

\footnote{Art. 8.70(6) JEFTA; Art. 16.7 CETA.}}

If restrictions on transfers of personal data, or any other trade-restrictive privacy or data protection measure are found to be in violation of the trade in services commitments, alone, or together with a violation of Article 1 of the proposed model clauses on cross-border data flows of a digital chapter, which exception will then prevail? Article 1 is unlikely to capture any of the EU’s restrictions on cross-border transfers of personal data, as such restrictions are not included in the exhaustive list of prohibited restrictions on cross-border data flows. Therefore, if an EU trading partner moved to challenge those restrictions in an international trade forum, it would, most likely, have to invoke one of the non-discrimination provisions or a market access provision in the trade in services chapter.

Because the exception of Article 2(2) of the proposed model clauses is destined for the digital trade chapter, and thus not for the exceptions chapter, one could argue that this exception would only apply if a measure is challenged under the digital trade chapter, while the general exception would apply to measures challenged under other chapters of the same trade agreement. Following this argumentation, the exception of the digital trade chapter would only apply to information flows \textit{in abstracto}, such as flows of employment data between the subsidiaries of a multinational company, and not when such flows constitute an integral part of a digital service or good. In some cases – for example, when a provision of a service involves the application of an algorithmic system dependent on the processing of personal data – it may be impossible to disentangle the provision of the service from the data flows. The approach where the digital trade exception for privacy and data protection serves as a derogation from the obligation on cross-border data flows in the digital trade chapter (and not other chapters such as the one on trade in services) has been implemented in the recent US-led trade agreements. For example, the exception for privacy and data protection included in Article 19.11(2) of the digital trade chapter of the USMCA states that ‘[t]his Article does not prevent a Party from adopting or maintaining a measure inconsistent with paragraph 1 …’ where paragraph 1 contains a clause prohibiting restrictions on cross-border data flows. This wording suggests that this exception cannot
justify a derogation from any other obligation under the trade agreement except for the one regulating cross-border data flows.

The line of reasoning where the scope of the digital trade exception for privacy and data protection is limited to the digital trade chapter in the context of the model clauses proposed by the EU could be met, however, by a counterargument that the proposed digital trade exception should be invoked to justify any violation of the trade agreement as long as the challenged measure affects trade enabled by electronic means. There are at least two reasons that lend weight to this counterargument. First, the proposed digital trade exception is not worded as an exception solely to the provision on data flows included in Article 1 of the proposed model clauses, but as an independent provision on data protection and privacy, which applies in relation to the whole agreement. Second, since there is no explicit provision on conflict of laws in the EU proposals for the digital trade chapters or in the general exceptions, the interpretative maxim (also recognised as the general principle of law) on the relationship between general and specialised rules lex specialis derogat legi generali should apply. This principle has been applied by the WTO adjudicating bodies on several occasions. According to this maxim, the lex specialis – that is that the digital trade exception of Article 2 of the proposed model clauses – should prevail over the general exception if a challenged privacy or data protection measure affects trade enabled by electronic means or, in other words, digital trade. If this argumentation is correct, then a conflict between any provision of the trade agreement, which contains the proposed digital trade exception, and the restrictions on cross-border data flows under the GDPR, should be resolved under the digital trade exception and not the general exception. The reason for this is that the GDPR applies to the processing of personal data wholly or partly by electronic means, and thus does not apply to the analogue processing of personal data. This means that any privacy and data protection under the GDPR, if trade restrictive, would mainly affect digital trade. Hence, the digital trade exception should apply.

This outcome, however, reduces the scope of the general exception for privacy and data protection to the highly unlikely cases of conflicts between domestic measures concerning analogue processing of personal data, and international trade norms. As a result, the general exception for privacy and data protection becomes nearly redundant. In US-Gasoline, however, the WTO Appellate Body held that:

---

752 Cf. wording of Art. XX GATT, understood broadly — as exception to any other obligation.
753 Koskenniemi (2009), pp. 4-5.
755 Art. 2(1) GDPR.
One of the corollaries of the ‘general rule of interpretation’ in the Vienna Convention is that interpretation must give meaning and effect to all the terms of a treaty. An interpreter is not free to adopt a reading that would result in reducing whole clauses or paragraphs of a treaty to redundancy or inutility.\textsuperscript{756}

If a trade adjudicating body facing the dilemma of the relationship between the digital trade and the general exceptions for privacy and data protection adhered to the above approach to interpretation, there would be a risk that the \textit{lex specialis} argument would thus not be decisive and the scope of the general exception for privacy and data protection would then be broader than just described. As a result, some of the conflicts between domestic rules on transfers of personal data and international trade disciplines could be still captured by the general exception. Therefore, the question of whether the proposed digital trade exception for privacy and data protection can, in all cases, override the general exception for privacy and data protection remains at least partially open. It is for this reason that the future EU trade agreements – if they were to include both the general exception and the proposed digital trade exception for privacy and data protection – should, as a minimum, clarify the relationship between the two exceptions in a way that makes the general exception inapplicable to domestic measures on the automated processing of personal data.

One may also wonder why the EU does not propose to change the general exception for privacy and data protection instead of adding another exception overriding it. In theory, this would be the most logical way to solve the issue discussed in this Section. It could be that the answer lies in the ‘legacy clout’ of the general exceptions, which have been replicated in multiple trade agreements for decades.\textsuperscript{757} Recall that the general exceptions typically contain exceptions for other public policy interests besides privacy and data protection. Renegotiation of a general exception for privacy and data protection only, with a view of granting parties to a trade agreement a broader autonomy to regulate these interests, \textit{would bluntly put privacy and data protection above other important policy objectives such as the protection of the environment or public health}. Shifting these renegotiations to another forum – the digital trade chapter, despite this leading to the same result of preferring privacy and data protection to other policy objectives – allows this outcome to be less apparent and avoids the possible discontent of stakeholders defending those other policy objectives on the international trade policy landscape. Therefore it could

\textsuperscript{757} For example, Riffle argues that trade agreement negotiators ‘are naturally hesitant to tinker with well-established General Agreement on Tariffs and Trade (GATT) language, unless there is a cogent reason’. Riffel (2018), p. 143.
be more convenient to negotiate a separate exception for privacy and data protection during digital trade negotiations instead of reopening negotiations on the general exception. Additionally, the transaction costs of renegotiating the general exception may simply be too high.

4.2.3 An undesirable parallel with the national security exception

Let us recall that the digital trade exception for privacy and data protection proposed in Article 2(2) allows each Party to ‘adopt and maintain the safeguards it deems appropriate to ensure the protection of personal data and privacy’ (emphasis added). The threshold that a trade-inconsistent safeguard must meet is the ‘it deems appropriate’ test (emphasis added) – as opposed to the necessity test in the general exception – which is similar to that employed in national security exceptions in the WTO agreements.758 For example, under Article XIVbis(1)(b) of the GATS: [n]othing in this Agreement shall be construed:

<br/>

(b) to prevent any Member from taking any action which it considers necessary for the protection of its essential security interests:

(i) relating to fissionable materials or the materials from which they are derived;

(ii) relating to the traffic in arms, ammunition and implements of war and to such traffic in other goods and materials as is carried on directly or indirectly for the purpose of supplying a military establishment;

(iii) taken in time of war or other emergency in international relations.759

The phrase ‘it considers necessary’ in the national security exception has been remarkably consistent since the GATT 1947, not only in various WTO Agreements,760 but also in post-WTO trade agreements concluded around the world.761 The wording of the proposed digital trade exception for privacy and data protection allows any safeguards ‘it [each Party] deems appropriate’. It is not identical to the ‘it considers necessary’ phrase contained in the national security exception. Nevertheless, despite this discrepancy in the wording of the two exceptions, the analysis of the national security exception is useful because, based on the definition of ‘appropriate’ and ‘necessary’ in dictionaries and

---

758 See, e.g., Art. XIVbis GATS; Art. XXI GATT 1994.
759 (emphasis added)
760 Art. XXI GATT; Art. XIVbis GATS; Art. 73 TRIPS; Arts. 2.2, 2.10, 5.4, 5.7 and 10.8.3 TBT Agreement; Art. III:1 Revised Agreement on Government Procurement.
761 For an overview Cottier, Delimatsis (2008).
scholarly interpretations, ‘it deems appropriate’ seems to afford the same or an even broader margin of appreciation than ‘it considers necessary’.762

In the following paragraphs, this Section first considers the interpretation of the national security exception in general, and its ‘it considers necessary’ test in particular, by the WTO Panels, and then extrapolates the insights to the proposed digital trade exception for privacy and personal data and its ‘it deems appropriate’ test. Based on this analysis it explains why modelling a digital trade exception for privacy and data protection after the national security exception is undesirable in the view of the EU’s goals to liberalise cross-border data flows and, more generally, the goal of maintaining a multilateral rules-based international trading system.

4.2.3.1 Interpretation of the national security exception at the WTO

The national security exception is the broadest of all the existing exceptions in international trade law. It provides almost unlimited autonomy for states to adopt trade law-inconsistent measures to protect their essential security interests. It is for this reason that this exception has been called ‘potentially the biggest loophole’, 763 ‘an unreviewable trump card’, 764 ‘the Achilles’ heel of international law’, 765 and ‘all-embracing and seemingly omnipotent’. 766 Until recently, Article XXI GATT had been invoked very infrequently. 767 Although the openness of the security exception has not been abused before, this is changing, 768 as the national security exception is being increasingly invoked in WTO disputes. At the time of writing, there are more than twenty pending disputes at

762 From the wording of Art. 3(1) DSU it follows that in WTO law ‘necessary’ and ‘appropriate’ have different meaning. Under this provision ‘[a] Member should respond promptly and fully to any request by a panel for such information as the panel considers necessary and appropriate’. In contrast, however, Cottier and Delimatis use the words ‘necessary’ and ‘appropriate’ interchangeably in discussing the national security exception. See Cottier , Delimatis (2008), p. 335 (referring to ICJ and ECJ case law and stating that ‘[a] Member has indeed the flexibility to choose the measure that it deems appropriate to protect its essential security interests.’). In the EC–Sardines, the WTO Panel interpreted ‘inappropriate’ as referring ‘to something which is not “specially suitable”, “proper” or “fitting”’. WTO, Appellate Body Report, EC – Sardines, para. 285 citing WTO, Panel Report, EC – Sardines, para. 7.116. See also WTO, Panel Report, US – Tuna II (Mexico), para. 7.723.) Similarly, one of the definitions of ‘appropriate’ in the Oxford English Dictionary, most suitable in the present context, is ‘specially fitted or suitable’. OXFORD ENGLISH DICTIONARY ONLINE, appropriate https://www.oed.com/view/Entry/9870?rskey=uGZYsX&result=1#eid The same dictionary defines ‘necessary’ as ‘indispensable, vital, essential; requisite’. OXFORD ENGLISH DICTIONARY ONLINE, necessary, https://www.oed.com/view/Entry/125629?redirectedFrom=necessary#eid. According to the same Dictionary, ‘deem’ and ‘consider’ have synonymous meaning. The Dictionary defines the current use of the verb ‘to deem’ as ‘[t]o form the opinion, to be of opinion; to judge, conclude, think, consider, hold’. OXFORD ENGLISH DICTIONARY ONLINE, deem, https://www.oed.com/view/Entry/48614?rskey=Ujiag&result=2&isAdvanced=false#eid

768 Chen (2017), pp. 313-317. For an example of a potential abuse see WTO, Panel Report, Saudi Arabia – Protection of IPR.
the WTO involving a national security exception.\textsuperscript{769} To name just a few examples, Russia successfully invoked the exception in a GATT case brought against it by Ukraine; Saudi Arabia – successfully to some extent\textsuperscript{770} – invoked the exception contained in Article 73 of the TRIPS Agreement (almost identical to Article XXI GATT) in a case filed by Qatar to defend piracy of Qatari broadcasts as a national security matter;\textsuperscript{771} and the US adopted tariff measures against its trading partners to protect alleged national security interests.\textsuperscript{772} The weak link between the measures adopted by the US and the national security interests invoked by the US, opens the door to invoking this exception as a justification for any trade restrictive measure vaguely related to national security.

There are two key issues in the interpretation of the ‘it considers’ threshold in the national security exception: (1) whether it means the exception is self-judging, meaning the WTO adjudicating bodies have no jurisdiction to review measures that a WTO member claims to have introduced within the boundaries of the national security exception, and (2) if the exception is not self-judging, what is the margin of appreciation afforded to a WTO member to adopt measures to protect national security, and the standard of review that the WTO adjudicating bodies should exercise in assessing whether a contested measure satisfies the conditions of the exception.

The long-standing controversy on whether the national security exception is self-judging originated in a GATT-1994 dispute between the US and the European Community, regarding the US Helms-Burton Act imposing sanctions against Cuba with extraterritorial effect bound to affect European companies. In that case, the US invoked the exception not only as a substantive justification for its GATT-inconsistent measure, but also as a jurisdictional defence.\textsuperscript{773} In doing so, the US argued that the WTO, in principle, had no jurisdiction in considering the dispute once this exception has been invoked. The parties ultimately resolved the dispute by agreement and the WTO did not express an opinion on this issue.\textsuperscript{774}

In the aftermath of this case, some scholars sided with the US: based on the wording ‘it considers’, they argued that it is ‘free from any judicial review’ and is ‘self-judging’.\textsuperscript{775}

\textsuperscript{769} Vidigal (2019), p. 205.
\textsuperscript{770} Saudi Arabia managed to successfully invoke the national security exception in relation to some TRIPS-inconsistent measures, but not the others. See WTO, Panel Report, \textit{Saudi Arabia – Protection of IPR}, paras. 7.285-7.293.
\textsuperscript{771} WTO, Panel Report, \textit{Saudi Arabia – Protection of IPR}.
\textsuperscript{773} WTO, Dispute Settlement Body, Minutes of Meeting, WT/DSB/M/24, 16 October 1996. See WTO, Request for the Establishment of a Panel by the European Communities, United States – The Cuban Liberty And Democratic Solidarity Act. WT/DS38/2, 8 October 1996.
\textsuperscript{774} Vidigal (2019), p. 204.
\textsuperscript{775} Alford (2011), pp. 701-702; See also Jackson (1969); Bhala (1998); Akande, Williams (2003).
Others argued that the security exception cannot be sensibly interpreted to deny the WTO’s jurisdiction on the interpretation and application of the exception (distinguishing between the ‘authority to define’ and ‘authority to interpret’).\textsuperscript{776} In its \textit{Russia – Traffic in Transit}\textsuperscript{777} report, the WTO Panel held that the exception is not ‘totally self-judging’ and that the WTO adjudicating bodies have the power to review whether the objective requirements of the exception are met.\textsuperscript{778} The Panel Report has not been appealed by any of the parties and is final. The WTO Panel in \textit{Saudi Arabia – Measures concerning the Protection of Intellectual Property Rights} confirmed the general interpretation and the analytical framework established by the Panel in \textit{Russia – Traffic in Transit}.\textsuperscript{779}

The Panels introduced a four-step analytical framework to assess whether a contested measure falls under the national security exception.\textsuperscript{780} The discussion below will emphasise the Panels’ findings that are most relevant for the analysis of the proposed digital trade exception for privacy and data protection, leaving aside the aspects specific to the wording of the national security exceptions.\textsuperscript{781}

Prior to the Panel reports, scholars generally considered that the national security exception afforded WTO members a wide margin of appreciation in choosing an appropriate measure to protect national security in spite of their WTO commitments.\textsuperscript{782} In particular, they believed that the state invoking the exception was free to decide \textit{whether} an action was required, no matter how remote the link between the national security and the basis for invoking the exception, and \textit{which} action should be taken: this choice could not be questioned by a trade adjudicating body.\textsuperscript{783}

The WTO Panels in \textit{Russia – Traffic in Transit} and in \textit{Saudi Arabia – Measures concerning the Protection of Intellectual Property Rights} generally confirmed that the phrase ‘which it considers’ allows a WTO member \textit{itself} to determine ‘the “necessity” of

\textsuperscript{777} WTO, Panel Report, \textit{Russia – Traffic in Transit}.
\textsuperscript{780} This framework is summarised in WTO, Panel Report, \textit{Saudi Arabia – Protection of IPR}, para. 7.241.
\textsuperscript{781} For a comprehensive discussion on all the prongs of the assessment developed in \textit{Russia – Traffic in Transit}, see Vidigal (2019).
the measures for the protection of its essential security interests’. This test is therefore easier to satisfy than the necessity test of the general exception, as the WTO Panel in Russia – Traffic in Transit clarified:

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

The Panels also explained, however, that the clause ‘it considers’ does not apply to the assessment of the three sets of circumstance under paragraphs (i)-(iii) of Article XXI(b) GATT or Article 73(c) TRIPS, which are subject to objective determination by WTO adjudicators. On the contrary, these paragraphs operate as ‘limitative qualifying clauses’ that ‘qualify and limit the exercise of the discretion accorded to Members under the chapeau to these circumstances.’

Furthermore, the Panels held that both (a) the WTO member’s discretion to designate particular concerns as ‘essential security interests’ and (b) the subjective assessment of ‘necessity’ in the national security exception are limited by the obligation to interpret and apply the exception in good faith, a general principle of law and a principle of general international law envisaged in Article 31 VCLT. Whether a WTO member met the obligation of good faith is subject to the objective assessment of the WTO adjudicating bodies. This has two implications.

First, a WTO member cannot use the security exception ‘as a means to circumvent their obligations under the GATT 1994’. While each WTO member is free to define what it considers to be its essential security interests, the WTO Panels clarified that such interests ‘generally’ concern ‘those interests relating to the quintessential functions of the state, namely, the protection of its territory and its population from external threats, and

---

787 Ibid.
789 WTO, Panel Report, Russia – Traffic in Transit, para. 7.133.
the maintenance of law and public order internally.” 790 In俄罗斯—Traffic in Transit the Panel noted that a ‘glaring example’ of circumvention is when a WTO member tries to ‘release itself’ from its trade commitments by ‘re-labelling trade interests that it agreed to protect and promote … as “essential security interests”’. 791 To satisfy the good faith requirement in relation to the evaluation of ‘essential security interests’, a WTO member must articulate those interests in the manner “minimally satisfactory” in the circumstances’, ‘sufficiently to enable an assessment of whether the challenged measures are related to those interests’. 792 This requirement, however, ‘is not a particularly onerous one, and is appropriately subject to limited review by a panel’, in particular because the Panel is not well-positioned to make such an assessment. 793 For example, in Russia—Traffic in Transit, the Panel concluded that ‘there [was] nothing in Russia’s expression of [national security] interests to suggest that Russia invoked Article XXI(b)(iii) simply as a means to circumvent its obligations under GATT 1994.794

Second, the connection between the measures at issue and the ‘essential security interests’ must meet the ‘minimum requirement of plausibility in relation to the proffered essential security interests, i.e. that they are not implausible as measures protective of these interests’. 795 In Saudi Arabia—Measures concerning the Protection of Intellectual Property Rights, failure of Saudi Arabia to meet this prong of the assessment resulted, for the first time in history, in an unsuccessful invocation by a WTO member of the national security exception to justify a trade-inconsistent measure.

This reasoning of the WTO Panels is consistent with the interpretation of the ‘it considers necessary’ test found in scholarly literature preceding the issuance of the Panel reports. For example, Cottier and Delimatsis argued that the breadth of the national security exception was not unlimited as this would be incompatible with a rules-based foundation of international trade legal order. 796 Most notably, they argued that the margin of appreciation in determining necessity is limited by the doctrine of abuse of rights or good faith, which amounts to an objective assessment.797 Similarly, to Sykes ‘Article XXI does

791 WTO, Panel Report, Russia—Traffic in Transit, para. 7.133
794 WTO, Panel Report, Russia—Traffic in Transit, para. 7.137.
796 Cottier, Delimatsis (2008).
not encompass exigencies such as a member government’s financial distress or domestic economic crises that are unrelated to war and international emergencies’. The recourse to ‘good faith’ by the panels is perhaps understandable, but fails to provide a clear direction. ‘There is no single agreed-upon formulation of a “good-faith test”’, although ‘proposals generally focus on separating genuine security policies from abuse, pretext, and subversion of the treaty.’

4.2.3.2 Interpretation of the digital trade exception for privacy and data protection

Applying the interpretation of the national security exception explained in the previous Section to the proposed digital trade exception for privacy and data protection allows one to make two predictions. First, the proposed digital trade exception is unlikely to be viewed as self-judging and will be subject to the review of trade adjudicating bodies. Second, the ‘it deems appropriate’ threshold, given its similarity to ‘it considers necessary’ in the national security exception, is most likely to be interpreted as affording a wide margin of appreciation of what safeguards to protect privacy and personal data are appropriate. In other words, it would allow the defending Party to conduct a subjective assessment of the matter. The fact that the adoption and application of rules on the cross-border transfer of personal data is explicitly mentioned in the proposed exception as an example of ‘appropriate safeguards’ creates a presumption that such restrictions are covered by the exception. At the same time, a Party’s discretion to adopt and maintain such safeguards is limited by an objective assessment by a trade adjudicating body as to whether the Party’s behaviour is in good faith and does not constitute an abuse of right. This objective assessment would include (a) a limited assessment of whether particular concerns are articulated as privacy and data protection interests in a minimally satisfactory manner to allow adjudicators to assess their relationship with the contested measures, and (b) an assessment of whether the nexus between the privacy and data protection interests and the contested measure meet a ‘minimum requirement of plausibility’. The objective assessment, however, will be narrower than in the national security exception, as the proposed digital trade exception for privacy and data protection does not contain an analogue of the ‘limitative qualifying clauses’ present in the national security exception. As a result, the proposed digital trade exception affords an even broader regulatory autonomy than the national security exceptions in the WTO agreements. This, of course, could be a function of the fact that this provision is only a starting point in negotiations.

799 Cf Art. 31(1) VCLT (stating that “[a] treaty shall be interpreted in good faith in accordance with the ordinary meaning to be given to the terms of the treaty in their context and in the light of its object and purpose.”)
Applying these predictions to the EU’s framework for transfers of personal data under the GDPR, one can conclude that such a framework would pass the ‘it deems appropriate’ threshold. Although the design of the EU’s restrictions on transfers of personal data is unlikely to be the least trade restrictive (as explained in Chapter 2), and arguably no longer fit for its constitutional purpose (as explained in Chapter 5), it does aim to protect the fundamental rights to the protection of personal data and privacy. Therefore, one can argue that restrictions on transfers of personal data are formulated in a minimally satisfactory manner and meet the minimum requirement of plausibility under the ‘it deems appropriate’ test. Furthermore, the formulation of the EU restrictions cannot be considered a means to circumvent the trade interests it agreed to protect. For one thing, these restrictions were designed in 1995 (the design of the framework has not changed since the 1995 Data Protection Directive) – a time when the issue of cross-border data flows was hardly on any country’s trade policy agenda.

### 4.2.4 A different threshold for digital trade exceptions

The previous Sections have demonstrated that the ‘it deems appropriate’ test of the proposed digital trade exception for privacy and data protection is broader than the necessity test of the general exception. Putting these two thresholds on a continuum from most restrictive to least restrictive for domestic autonomy in international trade, these tests would be at the opposite ends of this continuum. That said, although the ‘it deems appropriate’ test may provide the ultimate protection to the EU’s autonomy to protect privacy and personal data as fundamental rights and maintain the design of its framework for transfers of personal data under the GDPR, there are nevertheless at least three key reasons why the digital trade exception for privacy and data protection should not use this threshold, in view of the goals that the EU pursues by introducing the model clauses and the broader goals of EU’s trade policy. First, the risk of undermining the international rules-based trading system. Second, the risk of future replication of the ‘it deems appropriate’ threshold in exceptions for other public policy objectives. Third, and finally, undermining the EU digital trade policy goal of liberalising cross-border data flows, and in particular, facilitating the inflow of personal data to the EU. This Chapter reviews each one of them below.

The GATT 1947 parties and WTO members have for many years refrained from using the national security exception and from letting the WTO deliver a report on this exception. There was a good a reason: they were wary of opening Pandora’s Box, as abuse of the exception could undermine the rules-based trading system. The reason that

---

801 Until the WTO Panel Report in Russia – Traffic in Transit, all prior references to the national security exception did not lead to a binding decision by a WTO adjudicating body.
the possibility of invoking the national security exception is limited by the ‘limitative qualifying clauses’ subject to objective assessment, as explained above, was to keep the scope of the national security exception narrow. Adding an exception for personal data and privacy with a threshold very closely resembling that of the national security exception but without any ‘limitative qualifying clauses’ broadens the potential for future departures from international trade rules.

The breadth of the possibilities for escaping trade law disciplines under the proposed exception for privacy and data protection is also explained by the broad conceptualisation of the right to the protection of personal data in the EU, as has been explained in the Introduction. The broad understanding of data protection also suggests that data protection interests could be placed on a continuum between those integral to the existence of the democratic society and human dignity, and those which are more economic in nature (akin to consumer protection) and which are routinely ‘traded’ away for online services by individuals on the basis of consent recognised as a legitimate ground for personal data processing under the EU Charter. While for some of the data protection rights a wide autonomy within the international trade regime must be warranted, for others, it would not.

This line of reasoning does not imply that measures restricting cross-border data flows cannot be a national security issue. However, in that case, they should be defended on the basis of national security – not a digital trade exception. Each trade agreement, in which the EU includes its proposed digital trade exception for privacy and data protection, also contains a separate national security exception, which (in the EU’s recent and prospective trade agreements) repeats almost verbatim the national security exception.

803 WTO, Panel Report, Russia – Traffic in Transit, para. 7.65.
804 There is a growing volume of literature highlighting the overlap between data protection and consumer law, which is, at its core, economic regulation. See, e.g., Helberger, Zuiderveen Borgesius, Reyna (2017); Van Eijk, Hoofnagle, Kannekins (2017). This research also shows that, for example, when it comes to transparency and unfair terms in privacy policies, consumer law is more effective than data protection due to its flexibility and adaptability to changing circumstances. Van Eijk, Hoofnagle, Kannekens (2017), pp. 11–12; Helberger, Zuiderveen Borgesius, Reyna (2017), pp. 1438–1439.
805 From an economic perspective, personal data in two-sided platforms is increasingly compared to a price or consideration for services. See, e.g., Eben (2018); Bataineha, Mizounib, Barachic, Bentahar (2016). The view that personal data could be viewed as consideration for a service is also represented in some EU legislation. For example, Recital 16 European Electronic Communications Code clarifies that providing personal or other data to a service supplier or allowing such supplier to access personal data without actively supplying it (an example of this would be online tracking) in exchange for a service falls under the concept of remuneration. See also Recital 24 and Art. 3(1) Digital Content Directive. But see EDPS, Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content, p. 3, sharply criticising this approach.
806 Article 8 of the Charter.
807 See, e.g. Art. 26.8 CETA; Art. 1.5 JEFTA; Art. 16.11 EU-Singapore FTA.
808 See, e.g., Art. X.2 ‘Security exceptions’ EU proposal for Chapter X Exceptions of the EU-New Zealand FTA, 25 June 2019, which incorporates a provision almost verbatim repeating that of Art. XIVbis GATS. Namely, it contains an exhaustive list of ‘essential security interests’ that could justify invocation of the exception.
of the WTO instruments. Paradoxically, because the proposed digital trade exception is broader than the WTO national security exception, defending measures restricting cross-border data flows, in case they are implemented for national security reasons, could be problematic because of the ‘limitative qualifying clauses’ of that exception.

Introducing a broad digital trade exception to ameliorate this deficiency of the national security exception, is however, not an appropriate way forward. Rather, a reform of the national security exception, which was designed in the aftermath of World War II and has remained intact ever since, could be necessary. For example, the most recent US-led trade agreements demonstrate a significant departure from the GATT 1947 and the WTO model of the national security exception. In the national security exception of the USMCA (and the CPTPP initially led by the US) the limitative qualifying clauses are no longer present. To illustrate, the respective part of the national security exception in Article 32.2(1)(b) of the USMCA reads as follows:

1. Nothing in this Agreement shall be construed to:

   (b) preclude a Party from applying measures that it considers necessary for the fulfilment of its obligations with respect to the maintenance or restoration of international peace or security, or the protection of its own essential security interests.809

Unlike the WTO national security exception, this national security exception provides a broader escape valve for any public policy interest that has a nexus to ‘essential security’. It could justify restrictions on data flows on privacy and data protection grounds framed as a national security issue. This scenario is plausible, especially given that the Committee on Foreign Investment in the United States (CFIUS) has already blocked the acquisition of several US companies by Chinese investors by invoking data privacy-related national security concerns.810 According to some experts, these concerns are primarily driven by fear of content censorship and surveillance over personal information, which can be exploited in a way threatening to national security.811 Whether the US approach to the national security exception is the right way forward is beyond the scope of this thesis. In broad terms, removing any limitations in relation to the circumstances in which national security can be invoked seems to be a dangerous step that could jeopardise the international trading system, as constraining the abuse of the national security exception was precisely

809 See also Art. 29.2(b) CPTPP. (emphasis added)
810 Williams (2019); Lippman (2020).
811 Williams (2019).
the reason why the drafters of the ITO Charter and the GATT 1947 included the limitative clauses in the exception in the first place.\textsuperscript{812}

Heath argues that an unintended consequence of the abuse of the exception is that ‘potential for good-faith but novel national security claims’ might not be allowed, as the standards that may result from overuse are likely to increase the threshold to maintain at least a semblance of order in international trade rules.\textsuperscript{813} Similarly, the broader use of this threshold for privacy and data protection and other public interests less crucial than national security could lead to the same outcome. The threshold could be narrowed in the interpretation in relation to other public interests, and then this interpretation could be extrapolated back on the national security exception.

If the EU succeeds in introducing an ‘it deems appropriate’ test for the sake of protecting privacy and personal data in its trade agreements, it will create a precedent that will open the door for other countries to introduce similarly broad exceptions for other public policy interests that fit their own cultural, societal, economic and political preferences or sensitivities. National security and defence are public interests that, unlike privacy and data protection, are of vital importance to any country’s existence and, therefore, unique in their primary importance to any party of an international trade agreement.\textsuperscript{814} They stand above trade liberalisation goals. National security and defence are also a highly political areas for the states, the ones in which any external interference is generally not tolerated.

If a privacy and data protection exception with a similar threshold were to be introduced, it would be hard to argue that other rights – recognised as fundamental by either the EU or its trading partners – do not deserve a similar level of protection. The EU Charter itself protects multiple other fundamental rights and freedoms besides privacy and the protection of personal data, such as the above-mentioned rights to freedom of expression and the freedom to conduct business.\textsuperscript{815} Furthermore, some of the EU’s partners in international negotiations, especially in the WTO setting, may value other policy interests above privacy and data protection and, therefore, may either demand to raise the threshold for privacy and data protection or lower the threshold for other public policy interests. The participation of China, Russia and several developing countries in these negotiations is likely to add several other public policy interests (such as economic security, industrial policy, public health, and information sovereignty) to the mix of sensitive issues to be balanced against the economic benefits of digital trade liberalisation.

\textsuperscript{812} Pinchis-Paulsen (2020), p. 192.
\textsuperscript{813} Heath (2020).
\textsuperscript{814} Cottier, Delimatis (2008), p. 1.
\textsuperscript{815} Arts. 11, 16 EU Charter.
Each trading partner is likely to strike a different balance between these benefits on the one hand, and other non-trade policy priorities reflecting their own constitutional traditions, the level of digital and economic development and the desire to resist ‘digital colonialism’, on the other hand.

4.2.5 Undermining the goal of liberalisation of cross-border data flows

The use of the ‘it deems appropriate’ threshold in the digital trade exception for privacy and data protection could impair the effectiveness of the prohibitions on restrictions of cross-border data flows under Article 1 of the proposed model clauses, which serve the EU’s strategic economic interests. Liberalisation of cross-border data flows is also one of the goals pursued by the proposed model clauses. Recall that Article 1 is already formulated in a way which is unlikely to implicate the EU’s privacy and data protection framework. Rather, these disciplines serve the EU’s economic interests in removing data localisation measures in other countries, such as Indonesia, or prevent their introduction in the first place. In the 2020 European strategy for data, the European Commission once again acknowledged that ‘European companies operating in some third countries are increasingly faced with unjustified barriers and digital restrictions’ and promised to address ‘these unjustified obstacles to data flows in bilateral discussions and international fora – including the World Trade Organization.’ By ‘unjustified barriers and digital restrictions’ the Commission means restrictions that cannot be justified by legitimate privacy and data protection interests, where ‘legitimate’ clearly refers to the EU-style data protection framework. A broad digital trade exception for privacy and data protection, would not only grant a broad autonomy to protect privacy and personal data as fundamental rights to the EU, but also to its trading partners who may have a different view on what measures are necessary to protect these policy objectives. For example, Russia’s data localisation measures – often criticised as protectionist data localisation – are included in Russia’s law on the protection of personal data and are, therefore, framed as data protection measures. Ultimately, the economic interests of liberalising digital trade that the EU factors in, in the balancing between trade and fundamental rights to privacy and data protection, should not only include the economic gains from liberalising personal

---

816 See, e.g., Coleman(2019); Couldry, Mejias (2019).
817 Micallef (2019), p. 866, arguing that Art. 2 ‘can be used to neutralize the advantages that the first article brings’.
818 Herbert Smith Freehills LLP (2018).
820 See, e.g., Newton (2018), arguing that Russia is ‘using data localization laws to provide capital flow to Russian companies by requiring them to pay to store Russian data on Russian servers’ and by doing so is creating barriers to entry for international companies to the Russian market.
data flows from the EU, but also – and perhaps more importantly – the economic gains from personal data flows to the EU from its trading partners.

To sum up, the risk that the EU’s restrictions will be implicated by the proposed obligation not to restrict cross-border data flows under Article 1 of the model clauses is low. As a result, the chances that the EU will have to resort to Article 2 in defence of its restrictions on transfers of personal data are equally low. Because the prohibitions on data localisation in Article 1 primarily target the EU’s trading partners, the exception of Article 2 is also most likely to be invoked by EU’s trading partners.

As Chapter 3 of this thesis has explained, exceptions can be seen as a way to distinguish between restrictions on trade that are beneficial for society at large (public interest restrictions) and restrictions on trade captured by domestic industries which create redistribution of welfare and social costs (protectionism). The challenge is to draw a correct line between the two in each particular case, as this balance ultimately affects the balance between the interests of trade liberalisation and other public policy objectives. There will always be false positives and false negatives. The necessity test in the general exception uses multiple safeguards to ensure that trade interests are protected. Putting trade liberalisation above domestic (non-economic) public interests is likely to produce false positives, i.e. to outlaw domestic regulation genuinely pursuing public policy objectives as protectionist. By doing so, the necessity test ends up overprotecting economic trade liberalisation interests. On the other hand, the ‘it deems appropriate’ test – proposed by the EU for privacy and data protection exception in digital trade chapters – is likely to produce false negatives, as it can potentially filter out only cases (if any) where a state invokes the exception in manifestly bad faith.

Figuratively speaking, if the ‘it deems appropriate’ threshold is used, as compared to the necessity test of the general exception, the pendulum between trade liberalisation and competing policy objectives would swing to the other extreme. As discussed in Section 3.2.4.3, in the last several decades of the twentieth century, under the influence of neoliberal discourse, the international trading system has suffered from a ‘protectionism bias’ that favoured trade liberalisation over competing policy objectives. Conversely, the international trading system containing broad exceptions would, in effect, make compliance with trade liberalisation commitments voluntary. The underlying question here is that of the balance between trade liberalisation and other public policy interests, which ultimately harks back to the goals of the international trading system that states want to achieve. This question should be subject to a wide political and societal debate and not buried into the arcane details of negotiations on the wording of one particular exception of a trade instrument.
To sum up, in its proposed digital trade exception for privacy and data protection, the EU should use a threshold different from ‘it deems appropriate’. Nor is the necessity test (currently used in the general exception for privacy and data protection, as Chapter 2 has demonstrated), a suitable option due to its potential incompatibility with the EU’s constitutional framework. Given that the model clauses analysed in this Section are only a starting point in international trade negotiations, the EU still has sufficient wiggle-room to adapt its negotiation strategy. In Section 4.3, this Chapter will take stock of other tests employed in international trade law that strike a balance between trade liberalisation and domestic public policy objectives, in order to find an alternative test that would provide enough autonomy for the EU to protect privacy and personal data, whilst allowing it to pursue the goal of digital trade liberalisation and uphold the rules-based international trading system. In other words, Section 4.3 looks for a standard that lies somewhere between an overly broad ‘it deems appropriate’ or ‘it considers necessary’ tests and an overly restrictive necessity test. But first, the next Section considers the last point of critique of Article 2 of the EU’s proposed model clauses.

4.2.6 Downsides of the EU-centric approach

As mentioned in the introduction to this thesis, the EU stands out for its commitment to a high level of protection of privacy and personal data as binding fundamental rights guaranteed in Articles 7 and 8 of the EU Charter. International and regional human rights law plays only a limited role in international trade law. Therefore, for the EU to safeguard its autonomy to regulate privacy and the protection of personal data as fundamental rights vis-à-vis its international trade obligations, it is essential to include in international trade agreements provisions that reflect the normative foundations of privacy and data protection in the EU and accommodate a regulatory design of domestic frameworks most adequate to this normative goal. This seems to be precisely the rationale behind the provisions in the proposed model clauses stating that, first, ‘[e]ach Party recognises that the protection of personal data and privacy is a fundamental right’ and, second, ‘[n]othing in this agreement shall affect the protection of personal data and privacy afforded by the Parties’ respective safeguards’. This Section argues, however, that the first provision is overly EU-centric and can be amended without undermining the EU’s autonomy to protect privacy and personal data as fundamental rights in domestic law.

Although privacy is fairly widely recognised as a fundamental right, a sui generis fundamental right to the protection of personal data is much less common. It is not fully

822 For a discussion, see Yakovleva (2018), pp. 487-489, 499-508.
823 Ibid.
824 Art. 2 EU model clauses on cross-border data flows.
825 The right to privacy is enshrined in Art. 12 UDHR; Art. 17 ICCPR; Art. 8 ECHR.
recognised by the UN\textsuperscript{826} and reflects to a large degree the European legal tradition. This right is recognised in the Council of Europe Convention 108+ – the only binding international legal instrument on data protection – and the EU legal system.\textsuperscript{827} Although almost 60\% of countries in the world have a data protection law,\textsuperscript{828} not many of those countries (outside the European Union and the Council of Europe member states) recognise the protection of personal data as a fundamental right. For example, among the countries currently negotiating bilateral trade agreements where the EU has included the proposed model clauses, only Chile\textsuperscript{829} and Tunisia\textsuperscript{830} recognise data protection as a fundamental right, while Australia,\textsuperscript{831} Indonesia,\textsuperscript{832} and New Zealand\textsuperscript{833} do not. Similarly, not all WTO members adhere to the fundamental rights approach to the protection of personal data. The most obvious examples of countries that do not recognise this right are China,\textsuperscript{834} Russia\textsuperscript{835} and the United States. Although many countries are currently reviewing their data protection framework and are strengthening the protection of personal data, it is unclear whether the protection of this right as a fundamental right will become widely recognised. For example, although the US has recently intensified efforts to adopt a federal privacy law, which would increase the level of protection of personal data in the business context, such protection is still viewed as a consumer – and not a constitutional – right.\textsuperscript{836} As

\textsuperscript{826} The UN framework was developed long before the rise of personal data protection frameworks. The UN Guidelines for the Regulation of Computerized Personal Data Files, adopted by General Assembly resolution 45/95 of 14 December 1990 only refer to the human right to privacy. The UN has recently been also working on harmonising the data protection standards of the UN members. See, e.g., Personal Data Protection and Privacy Principles, Adopted by the UN High-Level Committee on Management (HLCM) at its 36th Meeting on 11 October 2018, which, however, also do not mention specifically the right to the protection of personal data, but only the right to privacy.


\textsuperscript{834} See, e.g., Aaronson, Leblond (2018), p. 263 (showing that China's governance over data is primarily driven by national security and sensorship concerns). At the time of writing, China is in the process of adopting a comprehensive law on the protection of personal data, which is said to be 'inspired' by the GDPR. Zhang, Yin (2020). It does not, however, lead to a recognition of protection of personal data as a fundamental right. See Luo, Wang (2020).

\textsuperscript{835} Russia’s constitution protects the right to privacy but does not mention the protection of personal data (Arts. 23-24 Конституция Российской Федерации от 12.12.1993 с изменениями от 01.07.2020. (Constitution of the Russian Federation of 12 December 1993 as amended on 1 July 2020)).

\textsuperscript{836} See Kerry (2019); Meyer (2018).
Chander, Kaminski and McGeveran rightly point out, the fundamental difference between the US and the European approaches to their data privacy regimes is not just the different language used in these two legal systems (‘data protection’ in Europe versus ‘privacy law in the US), but also that ‘data protection’ is universal in Europe, while most American law focuses on ‘consumer protection’. They also argue that the California Consumer Privacy Act (CCPA), despite some similarities with the GDPR, is still developed in the American tradition. It is the CCPA, in their view, not the GDPR, that is ‘catalyzing the development of U.S. data privacy law’. More broadly, as Whitman argues, Americans and continental Europeans perceive privacy differently and have two different cultures of privacy. While ‘[c]ontinental privacy protection, – he argues – are, at their core, a form of protection of a right to respect and personal dignity’, in America it ‘is much more oriented toward values of liberty, and especially liberty against the state’. In a similar vein, Schwartz and Peifer conclude that there is a ‘conceptual gulf between the data privacy systems of the EU and United States based on the different legal identities that they provide for the individual’. While the ‘EU has created a privacy culture around “rights talk” that serves to protect “data subjects” [...]’ in the United States, the focus is on “marketplace discourse” about personal information and the safeguarding of “privacy consumers.”

From this discussion it follows that recognition of the protection of personal data as a fundamental right in paragraph 1 of Article 2 of the proposed model clauses is EU-centric. It induces its foreign trading partners to adhere to the EU’s values, which are not necessarily in line with their own legal systems. Viewing privacy and data protection as a norm of governance deeply rooted in a country or region’s social, political and democratic structure suggests that, to maintain the integrity of their governance structure, countries must retain the autonomy to pursue such priority interests and values. Not every country will see the right to the protection of personal data as a similar public policy target as the EU and its member states, nor can all countries be expected to be cut from the same normative cloth. In other words, it is important to acknowledge that not all differences need to be harmonised, as long as there is a mechanism to ensure that the interests of both sides are respected and taken into account.

This Section, therefore, suggests that the proposed provision requiring each Party to recognise that the protection of personal data and privacy is a fundamental right could be

---

838 Ibid., p. 19.
839 Ibid., p. 25.
842 Ibid., p. 119.
rephrased in the course of trade negotiations as requiring each Party to recognise each other’s autonomy to choose the level of protection of privacy and personal data, including their protection as fundamental rights.

4.3 Thresholds alternative to ‘necessity’, ‘it considers necessary’ and ‘it deems appropriate’ tests

This Section discusses how far the EU can go in tightening the currently proposed ‘it deems appropriate’ threshold without compromising on the fundamental rights to privacy and data protection. This identifies the potential fallback options for the EU in relation to a threshold of a digital trade exception for privacy and data protection in international trade negotiations. Moving away from the two ‘extremes’ of ‘necessity’ in the general exception and ‘it deems appropriate’ or ‘it considers necessary’ tests in the proposed digital trade exception for privacy and data protection, this Section explores whether other thresholds could be more suitable in safeguarding the EU’s autonomy to protect privacy and personal data as fundamental rights while liberalising cross-border data flows and preserving the rules-based international trading system. Considerations applied in the selection of the relevant thresholds for analysis in this section are: (1) presence of the threshold in an existing trade agreement; (2) relevance to privacy and data protection, in particular, whether the threshold is used in an existing provision for privacy and data protection; and (3) availability of case law and academic literature. Thresholds selected with these considerations in mind and analysed in this Section are: non-circumvention, non-avoidance, reasonableness, and the prohibition of arbitrary or unjustified restriction on trade from the chapeau of the general exception.

This Section makes two arguments. First, that any of the following three thresholds are a better alternative to both the ‘necessity’ and ‘it deems appropriate’ tests: non-circumvention, non-avoidance and reasonableness. Second, to ensure more predictability and control for the parties to a trade agreement over the interpretation of the chosen threshold of the digital trade exception, restrictive mechanisms are necessary.

On the first point, interpretation of these three standards in academic literature and (scarce) WTO case law is circular in the sense that the interpretation of one refers to the other. Using prohibition of arbitrary or unjustifiable discrimination or of a disguised restriction on trade as a threshold, however, is undesirable primarily because of the ‘legacy clout’ of its interpretation by the WTO adjudicating bodies in the chapeau of the general exceptions in the GATT and GATS, which has been, at times, dangerously close to ‘necessity’ in the past. Principles of good faith and the prohibition of abuse of rights, which are a common denominator in the interpretation of all of the three alternative thresholds, as well the indeterminacy of the meaning of these thresholds in case law and literature,
would allow a dispute-settlement panel to build the interpretation of any of the thresholds in relation to privacy and data protection almost from scratch. The interpretation of these principles in relation to domestic restrictions on transfers of personal data could amount to a nuanced approach where the strictness of the threshold is situated on the continuum between the necessity test of the general exception and the ‘it considers necessary’ test of the national security exception, depending on the interference of the trade rules requiring free data flows with the rights to protection of privacy and personal data under domestic law of the Party to the agreement. In the application to EU law, the strictness of the trade law threshold for domestic privacy and data protection measures would be proportionate to the magnitude of the risk of interference with the fundamental rights to privacy and the protection of personal data. In short, a more lenient test would cover situations where the risk is lower, a more stringent test when the risk is higher, thus mirroring the granular framework for data transfers in EU law proposed in Section 5.4.3 of this thesis.

On the second point, this section argues that the precise wording of the threshold used to construct the exception for privacy and data protection (just as any other exception) matters, but only up to a point. The principles of good faith and the abuse of rights that are used to determine their meaning, are open norms, the exact meaning of which is essentially determined for each situation by adjudicators. This insight harks back to the conclusions of the previous Chapter of this thesis – that the discourse governing the interpretation of international trade law norms is just as important, if not more, as their wording. The flexibility of the principles of good faith and the prohibition of the abuse of rights is not only their main advantage, but also their main drawback, as it gives broad discretion to adjudicators.

This Section proceeds as follows. Sections 4.3.1-4.3.4 provide examples of the use of each of the above-mentioned thresholds in WTO and bi-lateral and regional trade agreements, discuss the substance and interpretation of each of them, and compare each threshold to the necessity test of the general exception and the ‘it considers necessary’ test of the national security exception. Section 4.3.5 reflects on the wisdom of using any of them in a digital trade exception for privacy and data protection to replace the currently proposed ‘it deems appropriate’ test, and the possible restrictive mechanisms limiting the adjudicators’ discretion in applying those alternative tests.

4.3.1 Non-circumvention

A non-circumvention clause can be found, for example, in the exceptions from:
(1) the obligation on cross-border information flows in financial services chapters, and

(2) a horizontal provision on cross-border data flows in digital trade agreements of the 2017 EU Council proposal for a data protection exception in digital trade agreements, which preceded the 2018 proposal mentioned in Section 4.2 of this Chapter.

According to the WTO Understanding on Financial Services,

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

Similar provisions can be found in several other EU-led trade agreements, including those with Singapore and Japan.

The ‘non-circumvention’ requirement has never been applied in practice at the WTO. Moreover, it is seldom discussed in literature. According to von Bogdandy and Windsor, although the requirement ‘not to circumvent’ has not been defined, ‘it is reasonably arguable that circumvention is equivalent to avoidance.’ Similarly, on the basis of a non-scientific survey of the WTO and GATT dispute settlement records, Jarreau concluded that “to circumvent” essentially means “to avoid”.

If ‘circumvention’ and ‘avoidance’ are equivalent notions, then the threshold of the data protection exception in the Understanding

---

844 Starting from the 1994 Understanding on Commitments in Financial Services and up to recently concluded CETA, rules in EU-led trade agreements on the liberalisation of trade in financial services contain a provision that requires the parties ‘not to take measures that prevent’ or to ‘permit’ the transfer of information or the processing of financial information, including transfers of data by electronic means, where such transfers of information, processing of financial information are necessary for the conduct of the ordinary business of a financial service supplier (obligation on free flow of financial information). Art. B.8 Understanding on Commitments in Financial Services; EU Schedule of Specific Commitments Supplement 4 Revision GATS/SC/31/Suppl.4/Rev.1. Understanding on Commitments in Financial Services is not a part of the GATS, but is an appendix to the Final Act of the Uruguay Round. Understanding is not legally binding per se, it is ‘an optional and alternative approach to making specific commitments on financial services’. See WORLD TRADE ORGANIZATION, Financial Services, https://www.wto.org/english/tratop_e/serv_e/finance_e/finance_e.htm. See also Art. 13.15(1) CETA; Art. 157(1) EU-Colombia-Peru FTA; Art. 22(1) EU-Mexico Coordination and Cooperation Agreement; Art 7.43(a) EU-Korea FTA; Art. 198(1) EU-Chile Association Agreement; Art. 8.54(1) EU-Singapore FTA.

845 Council of the European Union, Concept paper on data flows in trade agreements.

846 Art. B.8 Understanding on Commitments in Financial Services, second sentence. (emphasis added)

847 Art 8.54(2) EU-Singapore FTA.

848 Art. 8.63(2) JEFTA.


is functionally the same as the threshold in the prudential exception discussed in the following section.

Another example is useful in shedding additional light on the matter. The provision proposed in the 2017 EU Council’s concept paper on data flows reads as follows:

Nothing in the Agreement restricts the right of a Party to protect personal data and privacy so long as such right is not used to circumvent paragraph 1.851

To ensure greater legal certainty, the concept paper contains a footnote setting out a legally binding interpretation of the standard of ‘non-circumvention’, which explains that:

… circumvention means the abuse of the right to protect personal data and privacy by a Party with the intention to avoid the Party’s obligations under paragraph 1.852

The concept paper explains that the purpose of the ‘non-circumvention’ clause is to prevent the intentional use of the legitimate policy objectives, such as data protection, to disguise protectionist policies.853 The concept paper also explains that the anti-circumvention clause must not allow trade adjudicating bodies to doubt the ‘necessity of data protection measures in question’.854 This suggests that the non-circumvention standard, at least in the EU Council concept paper, is envisaged as a standard lower than the ‘necessity’ test of the general exception.

Although the available tools to interpret non-circumvention do not allow one to fully explain the meaning of this standard, they do make clear that this standard does not require the party invoking the exception to prove the ‘necessity’ of the contested measure. How different the non-circumvention threshold is from ‘it considers necessary’ or ‘it deems appropriate’ tests however, remains unclear. As discussed in section 4.2.3 of this Chapter, a prohibition to intentionally circumvent international trade commitments is also a component of the ‘it considers necessary’ standard, as applied by the WTO Panels in recent cases. The interpretation of non-circumvention as the use of legitimate policy objectives to ‘disguise protectionist policies’ offered by the footnote in the EU Council concept paper has little value, therefore, in part because there is no uniform understanding of what ‘protectionism’ is, as demonstrated in Chapter 3 of this thesis. The discussion of the ‘non-avoidance’ threshold in the following Section – a standard equivalent to ‘non-

851 (emphasis added) Council of the European Union, Concept paper on data flows in trade agreements, p. 2. Para. 1 referred to in this provision reads as follows: ‘No Party may prevent a person of the other Party from transferring, processing or storing data, within or outside the Party's territory, where such activity is necessary for the conduct of that person's business’.

852 Ibid. (emphasis added)

853 Ibid.

854 Council of the European Union, Concept paper on data flows in trade agreements, p. 3.
circumvention — brings the investigation of the relationship between non-circumvention standard and ‘it considers necessary’ test a step further.

4.3.2 Non-avoidance

The most well-known ‘non-avoidance’ clause appears in the prudential exception (also known as prudential carve-out\textsuperscript{855}) of Article 2(a) ‘Domestic Regulation’ of the GATS Annex on Financial Services. It reads as follows:

Notwithstanding any other provisions of the Agreement, a Member shall not be prevented from taking measures for prudential reasons <…>. Where such measures do not conform with the provisions of the Agreement, they shall not be used as a means of avoiding the Member’s commitments or obligations under the Agreement.\textsuperscript{856}

This clause was later reproduced in the prudential exceptions of other trade agreements, for example, in the KORUS trade agreement\textsuperscript{857} and the CPTPP.\textsuperscript{858} This demonstrates that the prudential exception provides a widely accepted example of an exception in trade law not based on the necessity test.

In addition to the prudential exception, the non-avoidance clause also appears in the exception for privacy and data protection in a cross-border data flow provision in the financial services chapter of the CPTPP. That exception reads as follows:

Nothing in this Section restricts the right of a Party to adopt or maintain measures to:

(a) protect personal data, personal privacy and the confidentiality of individual records and accounts; <…>

\textsuperscript{855} As already mentioned above, there is a scholarly debate on whether Art. 2(a) GATS Annex on Financial Services has a function of an exception or, alternatively, carves-out prudential measures from the scope of the agreement. Although the article is entitled ‘Domestic Regulation’ and – according to Cantore’s research into \textit{Travaux Preparatoire} - was intended to work as a ‘provision that excludes the application of other provisions,’ and not an ‘exception,’ this provision is predominantly seen, both by the WTO adjudicative bodies and scholars, as an exception rather than a carve out. Cantore (2014), p. 1242; WTO, Background Note by the Secretariat. \textit{Financial Services, S/C/W/312, S/FIN/W/73}, 3 February 2010, para. 28; WTO, Panel Report, \textit{Argentina – Financial Services}; para. 7.814; WTO, 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. For further discussion see Cantore (2014), pp. 1232, 1242; Cottier, Krajewski (2010), pp. 826-827; Leroux (2002); Marchetti (2011); Von Bogdandy, Windsor (2008); Yokoi-Arai (2008); Mitchell, Hawkins, Mishra (2016), p. 807.

\textsuperscript{856} (emphasis added)

\textsuperscript{857} Art. 13.10(1) KORUS, footnote omitted.

\textsuperscript{858} Art. 11.11(1) CPTPP, footnotes omitted.
provided that this right is not used as a means of avoiding the Party’s commitments or obligations under this Section.  

The ‘non-avoidance’ standard has never been interpreted by the WTO adjudicating bodies. In the only WTO case addressing the prudential exception, neither the Panel nor the Appellate Body reached the second sentence of the provision (which contains the non-avoidance clause). However, the meaning of this threshold is discussed in a WTO Background Note and in academic literature. There seems to be a consensus that the ‘non-avoidance’ standard in the prudential exception provides broad autonomy for WTO Members to adopt financial regulatory measures, that is, unless those measures are ‘purely or primarily protectionist in effect’. As explained in the WTO Background Note, the prudential exception is broader than the general exception:

In contrast to health and safety, for example, where only ‘necessary’ measures are excepted [under the general exception], all prudential measures are excepted. As a result, a prudential measure may not be challenged on the grounds of whether it is ‘necessary’ or ‘least trade restrictive’.

The main factors cited as the rationale behind safeguarding such broad regulatory space for domestic financial measures are: first, financial services are crucial for the functioning of today’s economies; second, as problems in the financial sector often emerge ex post, it is difficult to foresee which measures will be required to address those problems; and third, there is a lack of both coordination and international standards on prudential measures.

Commenting on the meaning of the ‘non-avoidance’ threshold, the WTO Background Note endorses the approach adopted by Leroux and by von Bogdandy and

---

859 Section B Annex 11-B to Chapter on Financial services CPTPP. It should be recalled that this exception differs from Art. 14.11 CPTPP. (emphasis added) Financial services are explicitly excluded from the scope of the CPTPP e-commerce chapter, thus the general obligation on cross-border transfers as well as the exception from it under Article 14.11 do not apply to financial data flows. Art. 14.2(4) and (5) CPTPP. Fefer claims that those were US financial regulators who ‘advocated for the explicit ability to restrict cross-border data flows in TPP, in addition to the flexibility provided by the prudential exception’. Fefer (2017), p. 12. Although the US later withdrew from the TPP, the provision has remained unchanged in the final version of the CPTPP.


861 WTO, Background Note by the Secretariat, Financial Services, S/C/W/312, S/FIN/W/73, 3 February 2010, para. 31. Background notes of the WTO Secretariat are of limited interpretative value and can at most be used as supplementary means of interpretation. See WTO, Panel Report, Mexico-Telecoms, para. 7.43.


863 WTO, Background Note by the Secretariat, Financial Services, S/C/W/312, S/FIN/W/73, 3 February 2010, para. 31. (emphasis added) Referring to Key (2003).

Windsor. The WTO secretariat seconds their opinion that the ‘non-avoidance’ requirement is ‘clearly intended to avoid abuse in the use of the exception’.\(^865\) For Leroux, the purpose of this requirement is ‘to prevent the abuse of the exception for prudential measures’ and, as a minimum, to impose ‘an obligation of good faith with respect to the adoption and application of prudential measures’.\(^866\) This interpretation creates a parallel between the ‘non-avoidance’ standard and the chapeau of the general exception and prompts several scholars to argue that the term ‘avoiding’ should take into account the rich case law on the chapeau of Article XX GATT 1994, as it performs a similar function.\(^867\) Scholars also note that the provision can be read ‘as requiring some level of intent to circumvent duties under GATS’.\(^868\)

Cantore criticises the interpretation of ‘non-avoidance’ through the principle of good faith as circular. In his view, ‘good faith is not a self-interpretive concept and depends on the time, context and situations in which it is invoked. As such, this approach leaves considerable discretion for panels to make evaluations on a case-by-case basis.’\(^869\) This thesis will come back to this interesting argument in Section 4.3.5 below, where it analyses and compares the alternative thresholds. Furthermore, Cantore rightly warns of the dangers of importing the WTO case law on *chapeau* in the interpretation of the prudential exception due to the absence of similarity in the wording of both provisions, taking into account also the difference in the function they perform, and the practice of the WTO adjudicating bodies of conducting an analysis of domestic policy strategies. As a result, he argues, this would shrink the regulatory autonomy safeguarded under the prudential exception.\(^870\)

As the WTO Appellate Body confirmed in its 2020 *Australia — Tobacco Plain Packaging (Honduras)* report, ‘it is well established that different words in a treaty are generally intended to convey a different meaning’.\(^871\) Despite the difference in structure and wording, however, several scholars argue that the non-avoidance standard does not substantially differ from the ‘reasonableness’ requirement in other prudential exceptions (the reasonableness requirement is discussed in the following Section).\(^872\) For example,

---

870 Ibid., pp. 71-72, 169, 180-183. For a discussion on the importation of standards of review from other provisions by WTO adjudicating bodies see, more generally, Mavroidis (2013).
871 WTO, Appellate Body Reports, *Australia – Tobacco Plain Packaging (Honduras and Dominican Republic)*, para. 6.646.
Mitchell et al contend that the non-avoidance standard implies the reasonableness requirement, which is why the interpretation of ‘reasonableness’ in WTO case law could be used to interpret ‘non-avoidance’.

Although to invoke the prudential exception the defending party need not prove its necessity or trade restrictiveness, the choice of contested prudential measures is not left to the sole discretion of the defending party but is rather subject to an objective assessment. In Argentina – Financial Services, the Panel, whose assessment was not reviewed by the Appellate Body, concluded that:

the use of the word ‘for’ in the phrase ‘measures for prudential reasons’ denotes a rational relationship of cause and effect between the measure and the prudential reason. Thus, the Member taking the measure in question must demonstrate that in its design, structure or architecture there is a rational relationship of cause and effect between the measure it seeks to justify under paragraph 2(a) and the prudential reason provided. A central aspect of this rational relationship of cause and effect is the adequacy of the measure to the prudential reason, that is, whether the measure, through its design, structure and architecture, contributes to achieving the desired effect. Whether a measure has been taken ‘for prudential reasons’, that is, whether there is a rational relationship of cause and effect between the measure and the reason, can only be determined on a case-by-case basis, taking account of the particular characteristics of each situation and each dispute.

In other words, instead of ‘necessity’ (as would be the case under the general exception), the party invoking the prudential exception must demonstrate the ‘adequacy’ of the design, structure and architecture of the measure. While this threshold, based on the interpretation above, is lower than ‘necessity’, it is sufficiently higher than that of ‘it considers necessary’ test, where the nexus between the measure and the national security interests is only subject to a ‘minimum requirement of plausibility’. It is unclear whether the same requirement of adequacy could be extrapolated to other exceptions. In particular, exceptions, which, on the one hand (unlike the national security exception), do not denote in their wording that the choice of the measures is at the discretion of the defending party, and on the other hand, do not use the preposition ‘for’ as in the prudential exception – for example, exceptions mentioned in the previous Section of this thesis. One could, however, argue that the absence of a specific wording calling for subjective choice of measures

---

874 WTO, Panel Report, Argentina – Financial Services, para. 7.891 (emphasis added)
opens the door wider for objective assessment of such choice, as compared to where there is such specific wording.

To sum up, the interpretation of the ‘non-avoidance’ threshold adds nuance to the interpretation of ‘non-circumvention’ for four main reasons. First, the interpretation favoured by the WTO Secretariat clearly sets the non-avoidance, and therefore the non-circumvention standard, apart from the necessity test of the general exception as safeguarding a broader regulatory autonomy. Second, both the WTO and scholarly interpretation further deepen the link between non-circumvention and non-avoidance, on the one hand, and the doctrines of good faith and the abuse of right, on the other. Unfortunately, besides a proposal to import case law from the chapeau of the general exception to interpret the principle of good faith – which is undesirable – there is no guidance on what good faith means in the context of the prudential exception. As a result, the interpretation of non-avoidance does not shed much more light on the relationship between this standard (and the standard of non-circumvention) with the ‘it considers necessary’ test. Third, unlike the ‘it considers necessary’ test, which clearly reserves the autonomy of the defending party to determine the appropriateness of the measures, the ‘non-avoidance’ threshold does not prevent adjudicating bodies from subjecting the appropriateness of defended measures to a fully-fledged objective assessment. Therefore, ‘non-avoidance’ affords less regulatory autonomy than the ‘it considers necessary’ test. Fourth, some interpretations use the reasonableness standard as a tool to interpret the non-avoidance standard. The following Section turns to this third alternative threshold.

4.3.3 Reasonableness

In several trade agreements, the ‘non-avoidance’ standard in the prudential exception is replaced by the ‘reasonableness’ one. For example, according to Article 13.16(1) of CETA,

This Agreement does not prevent a Party from adopting or maintaining reasonable measures for prudential reasons, including: <…>875

A similar provision is used in the prudential exception of NAFTA (Article 1410(1)).

To the knowledge of this thesis’ author, the prudential exception under NAFTA was only applied once – in an international investment case – and not actually interpreted by the panel on substance owing to judicial economy. In Fireman’s Fund v Mexico, the NAFTA investment tribunal only noted that the prudential exception ‘permits reasonable measures of a prudential character even if their effect (as contrasted with their motive or

875 Art. 13.16(1) CETA. (emphasis added)
intent) is discriminatory. The Tribunal rejected the contention that a measure discriminatory in effect is *eo ipso* unreasonable.

The tribunal referred to an authoritative interpretation of Chapter 14 of NAFTA by Wethington, the principal US negotiator:

Article 1410(1)(a) . . . carves out of the national treatment and other obligations of the financial services chapter a right to take reasonable measures even though discriminatory in application, to protect the safety and soundness of the financial system.

Analysing this award, Cantore concludes that the ‘reasonableness’ requirement only targets measures ‘that are *manifestly not linked* with a prudential objective and lead to the backhanded *avoidance* of obligations or commitments can be targeted’. Unlike the necessity test in the general exception, it does not require the assessment of costs and benefits or the evaluation of less restrictive means.

In CETA, the standard of reasonableness of the prudential carve-out is explained in the Understanding on the application of the prudential carve-out, which provides guidance on the interpretation of the carve-out in investment disputes. This guidance draws a clear parallel between reasonableness and the *chapeau* of the general exception. One of the non-exhaustive principles, outlined in the Understanding, is that ‘a measure is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between investors in like situations, or a disguised restriction on foreign investment’.

The term ‘reasonable’ actually appears more than 200 times in the text of the WTO Agreements in a variety of contexts, but never as a threshold in an exception from trade rules. For example, reasonable’ appears in Article X:3(a) of the GATT 1994. In *Dominican Republic – Import and Sales of Cigarettes*, the WTO Panel defined this term as meaning ‘in accordance with reason, not irrational or absurd, proportionate, having sound judgement’. However, as Cook explains, WTO adjudicators have also used reasonableness as an unwritten norm, even in the absence of a direct reference to it in a

---

876 ICSID, *Fireman’s Fund v. Mexico*, ICSID Case No. ARB(AF)/02/01, 17 July 2006, para 162.
877 Ibid., paras. 163-165. See also Wethington (1994), § 5.07.
878 Cantore (2018), p. 129. (emphasis added)
879 Ibid.
880 Although this thesis has used the term ‘prudential exception’ rather than ‘prudential carve-out,’ it does refer to ‘prudential carve-out’ in the context of CETA because this terminology is used in this trade agreement.
882 Ibid., para. 8(e).
883 Cook (2013), p. 3.
884 WTO, Panel Report, *Dominican Republic – Import and Sale of Cigarettes*, para. 7.385.
particular provision.\textsuperscript{885} The most relevant of such cases is the interpretation of the chapeau of the general exception, which is discussed in the following Section.

Despite the fact that, based on the scarce available literature, the reasonableness standard is very similar to both non-circumvention and non-avoidance, it is important to highlight one notable difference. While both the non-circumvention and non-avoidance requirements typically relate to how a contested measure \textit{is used or applied}, the reasonableness requirement is addressed \textit{to the measure itself}. It could be argued that, for this reason, the reasonableness requirement provides less regulatory autonomy than the other two standards. From this perspective, on the continuum between ‘necessity’ and ‘it considers necessary’ tests, the standard of reasonableness is somewhat closer to ‘necessity’. However, as is explained in the following Section, in investigating how the measure is applied, the WTO adjudicating bodies have also consistently inquired into the architecture and design of the measure.

4.3.4 \textit{Prohibition of \textquoteleft arbitrary or unjustifiable discrimination\textquoteleft or a \textquoteleft disguised restriction on international trade\textquoteleft}

The most well-known provision where the formula stated in the heading of this Section is used is the chapeau of the general exceptions contained in Articles XX GATT and XIV GATS (both of which are reproduced almost verbatim or incorporated \textit{mutatis mutandis} in most post-WTO trade agreements around the world).\textsuperscript{886} Recall from Chapter 2 that the WTO adjudicating bodies follow a two-step assessment of whether a contested measure can be justified under one of the general exceptions.\textsuperscript{887} The chapeau requirement is the second step in that assessment.\textsuperscript{888} The chapeau requires that measures justified under one of the exceptions should not be ‘applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where the same conditions prevail, or a disguised restriction on international trade’ \textsuperscript{889}

The same wording appears in article 5(d) of the GATS Annex on Telecommunications – together with the necessity test. This provision allows a WTO member to derogate from an obligation to provide access to public telecommunications infrastructure if this is \textit{necessary} to ensure the security and confidentiality of messages.

\textsuperscript{885} Cook (2013), p. 12.
\textsuperscript{886} See, e.g., Art. 28.3(2)(c)(ii) CETA; Art. 8.62(e)(ii) EU-Singapore FTA; Art. 167(1)(e)(ii) EU-Colombia–Peru FTA; Art. 7.50(e)(ii) EU-Korea FTA; Art. 203(1)(e)(ii) EU-Central America Association Agreement; Art. 135(1)(d)(ii) EU-Chile Association Agreement; Art. 23.1(2) KORUS; Art. 21.1(2) US-Singapore FTA; Art. 21.1(2) Dominican Republic–Central America-US FTA; Art. 21.1(2) US–Panama TPA; Art. 32.1(2) USMCA; Art. 29.1(3) CPTPP.
\textsuperscript{887} Section 2.3.2.
\textsuperscript{889} Art. XIV GATS, Art. XX GATT 1994.
subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade in services’. While the GATS Annex on Telecommunications does not specifically mention privacy, CETA and some of the US-led trade agreements refer to privacy in addition to the security and confidentiality of the communications.890 Some Telecommunication chapters in EU-led bi-lateral trade agreements include this wording, but without an accompanying necessity test.891 In his 2019 article, Micallef proposed complementing Article 2 of the EU model clauses discussed in Section 4.2 of this Chapter with a proviso that the right to protection personal data and privacy ‘is not to be unjustifiably used to circumvent rules for cross-border data transfers for reasons other than the protection of personal data’.892 Because the provision in the Annex on Telecommunications has not yet been interpreted in practice, however, the rest of this Section focuses solely on the chapeau.

The language of the chapeau has been criticised as unclear,893 ‘rife with ambiguity’,894 and ‘the vaguest, and therefore the most problematic’ requirement of all those found in exception clauses.895 Just like the interpretation of the necessity test, the interpretation of the chapeau in general exceptions has been uneven throughout the years. Back in 1947, during negotiations of the general exceptions in the ITO Charter, the US Executive Committee on Economic Foreign Policy (ECEFP) warned that the language of the chapeau, (which was later included verbatim in the GATT 1947 and subsequently in the GATT 1994 and the GATS), was ‘vague and diffuse, making it difficult, if not impossible, to assign specific content to it’.896 Furthermore, the ECEFP noted that the broad language of the chapeau could ‘preclude the possible application of the exceptions to meet the legitimate circumstances for which the exceptions were designed’.897 Fast forward to present day, this characterisation turned out to be not far from the truth.

890 Art. 15.3(4) CETA; Art. 9.2(4) US – Singapore FTA; Art. 13.2(4) Dominican Republic-Central America-US FTA; Art. 13.2(4) US – Panama TPA; Art. 13.2(4) US-Chile FTA; Art. 13.2(4) US-Morocco FTA, Art. 14.2(4) US-Peru TPA; Art. 14.2(4) US-Colombia TPA; Art. 18.3(4) USMCA; Art. 13.4(4) CPTPP.
891 Art. 15.3(4) CETA; Art. 192 EU-Central America Association Agreement.
893 Bartels (2015), pp. 95-125. Ibid., p. 96 (stating that although the disputes in US—Gasoline, US—Shrimp, U.S.—Gambling, Brazil—Retreaded Tyres, EC—Seal Products ‘have given the chapeau a high profile, and yet it is still not clear what it requires’.
895 Ibid., p. 176.
896 The chapeau in the New York Draft Charter, which was the subject of the critique, was formulated as follows:

Subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where the same conditions prevail, or a disguised restriction on international trade.

897 Ibid.
Reflecting on the interpretation of the chapeau in WTO case law, Riffel neatly describes the interpretative conflict of the chapeau as revolving around the two extremes:

On one end of the spectrum, the chapeau is read as a stringent threshold requirement, thus reducing the policy space of states to regulate public welfare matters. On the other end, the chapeau reaffirms the tenet of good faith, which guides the performance of every treaty in any event.\textsuperscript{898}

Just as the necessity test of the general exception, the standard of the chapeau is fairly hard to meet and has a very low success rate so far.\textsuperscript{899}

4.3.4.1 Blurring the borderline between the chapeau and necessity test of the general exception

As is apparent from its wording, the test of the chapeau is meant to address the manner in which a measure is \textit{applied}, rather than the measure itself or its content. This is how this provision was indeed interpreted in one of the earlier cases applying Article XX GATT 1994.\textsuperscript{900} In later cases, however, the Appellate Body departed from this narrow interpretation of the chapeau requirement. In contrast, it clarified that the application of a measure can also ‘most often be discerned from the design, the architecture, and the revealing structure of a measure’.\textsuperscript{901} A WTO Panel took the same approach in the interpretation of the chapeau under Article XIV GATS.\textsuperscript{902}

In \textit{US-Shrimp}, the Appellate Body underlined that the ‘standards established in the chapeau are … necessarily broad in scope and reach’. To Cantore, the Appellate Body’s ‘pervasive analyses regarding the design and structure of the measures under scrutiny’ set a high threshold for domestic measures to meet in order to satisfy the test.\textsuperscript{903} Put differently, it brings the standard of the chapeau dangerously close to the necessity test of the general exception, which, by definition should be different given that the two standards are a part of the same general exception. Similarly, Riffel argues that because of the Appellate Body’s scrutiny of substantive exceptions under the chapeau ‘the distinction between substance and administration of the measure became blurred’.\textsuperscript{904} He warns that ‘false

\textsuperscript{898} Riffel (2018), p. 143.
\textsuperscript{902} Panel Report, \textit{Argentina – Financial Services}, para. 7.748 (referring to Appellate Body Report, \textit{EC – Seal Products}, para. 5.302) and para. 7.761.
interpretation’ of the ambiguities of the chapeau ‘could lead adjudicatory bodies to seriously encroach on the Members’ regulatory autonomy’.

4.3.4.2 Chapeau as an expression of the principles of good faith and prohibition of abuse of right

The matter was not clarified much when, in relation to the legal standard set by the requirements of ‘arbitrary discrimination’, ‘unjustifiable discrimination’ and ‘disguised restriction’ on international trade of the chapeau, the Appellate Body in US-Gasoline held that, taking into consideration the object and purpose of the provision and the drafting history, their meaning overlaps. It focused on the ‘fundamental theme’ behind them rather than the exact meaning of each phrase. The Appellate Body concluded that the ‘purpose and object’ of the chapeau ‘is generally the prevention of abuse of the exceptions’ of Article XX GATT and to ensure that the exceptions are not invoked ‘as to frustrate or defeat the legal obligations of the holder of the right under the substantive rules of the General Agreement’. In US-Shrimp, the Appellate Body had explained that the chapeau is ‘a fundamental part of the balance of rights and obligations struck by the original framers of the GATT 1947’. This balancing of the rights and obligations the Appellate Body is linked to the principle of good faith:

The chapeau of Article XX is, in fact, but one expression of the principle of good faith. This principle, at once a general principle of law and a general principle of international law, controls the exercise of rights by states. One application of this general principle, the application widely known as the doctrine of abus de droit, prohibits the abusive exercise of a state's rights and enjoins that whenever the assertion of a right impinges on the field covered by [a] treaty obligation, it must be exercised bona fide, that is to say, reasonably.

---

907 Ibid.
910 Whether good faith here is applied as a general principle of international law, or is implied in the text of the chapeau, or by way of interpretation of the chapeau in good faith under Art. 31(1) VCLT, is debatable. For further discussion see Cottier, Schefer (2000), pp. 64-65; Panizzon (2006), pp. 109-110; Yoo, Ahn (2016), p. 442/ See also van den Bossche, Zdouc (2013), p. 573; Kiss (2006), para. 14.
In the same report, the Appellate Body also explained that the location of the ‘line of equilibrium’ between the rights and obligations of the Members, which the chapeau aims to achieve, ‘is not fixed and unchanging; the line moves as the kind and the shape of the measures at stake vary and as the facts making up specific cases differ’. The ‘actual contours and contents’ of ‘arbitrary or unjustifiable discrimination’ and ‘disguised restriction on trade’ themselves vary depending on the type of measure under examination and the public policy interest which that measure aims to protect. Generalising the application of the good faith and abuse of right standards to the chapeau by the WTO adjudicators, Panizzon concludes that these standards’ primary function is to control or push back ‘expansive or creationist readings of the exceptions to the liberalization obligation of GATT Article XX’, in other words, ‘to separate the “wheat” of real trade disputes from the “chaff” of non-trade disputes’. This approach at least suggests that what the standard of the chapeau means is impossible to define in general, that is, without its application to the facts of a particular dispute.

4.3.4.3 Factors in assessment of ‘arbitrary or unjustifiable discrimination’

Turning to the assessment of whether discrimination is ‘arbitrary’ or ‘unjustifiable’, the Appellate Body has primarily considered the cause or the rationale of the discrimination in light of the objectives listed in paragraphs of Article XX. In US-Tuna II the Appellate Body also considered whether ‘discrimination can be reconciled with, or is rationally related to, the policy objective with respect to which the measure has been provisionally justified under one of the subparagraphs of Article XX.’ These are, however, not the only factors that could be relevant in the assessment of ‘unjustifiable discrimination’, depending on the nature of the measure and the circumstances at hand, the effects of the discrimination as well as other factors could be relevant for the assessment.

Looking at the cause or rationale behind a contested measure, the Appellate Body considered, in particular, the following factors: (a) whether the contested measure was a ‘rigid and unbending requirement’ in that it required other countries to adopt a regulatory

---

918 WTO, Appellate Body Report, Brazil – Retreaded Tyres, para. 225 (referring to WTO, Appellate Body Report, US – Shrimp, paras. 163-166, 172, and 177). These factors were also reiterated in WTO, Appellate Body Reports, EC- Seal Products, para. 5.305.
programme that is ‘essentially the same’ as opposed to ‘comparable in effectiveness’;\(^{919}\) (b) whether the contested measure took into account different circumstances that may occur in territories of other WTO members;\(^{920}\) and (c) whether the defending party negotiated seriously with all WTO members, as opposed to doing so with some but not with others.\(^{921}\) In prior cases, the Appellate Body considered a requirement to adopt an ‘essentially the same’ regulatory framework, as failure to take into account different circumstances in other WTO members and negotiating with some but not with others as inconsistent with the chapeau requirement.\(^{922}\)

In *US-Gambling*, in applying the chapeau of Article XIV GATS, the key factor that the WTO panel considered in the assessment of ‘arbitrary and unjustifiable discrimination between countries where like conditions prevail’ and/or a ‘disguised restriction on trade’ was the *consistency* of the contested measure in which it was applied and enforced domestically.\(^{923}\) In that particular case, the Panel concluded that the contested measure did not meet the chapeau requirement because of inconsistency between the US federal measure prohibiting the remote supply of gambling and betting services and the interstate measure that permitted interstate pari-mutuel wagering over the telephone or other modes of electronic communication.\(^{924}\)

4.3.5 Towards the goldilocks exception for privacy and data protection in future EU trade agreements

Building on the discussion in Sections 4.3.1-4.3.4 above, this Section explains, first, why any of the standards of non-circumvention, non-avoidance and reasonableness are better equipped as a prototype for a new threshold in the future digital trade exception than the standard of the chapeau of the general exception; and, second, it argues that the wording of the exception matters only up to a point and that a limiting mechanism ensuring more predictability and parties’ control over the interpretation of the exception is needed.

4.3.5.1 Undesirability of replicating the standard of chapeau in digital trade exception for privacy and data protection

As explained in the previous Sections, the interpretation of the prohibition of ‘arbitrary or unjustifiable discrimination’, or of a disguised restriction on international trade’ contained in the chapeau of the general exceptions is much more elaborate and

\(^{919}\) Appellate Body Report, *US – Shrimp*, para. 177(emphasis added); see also Appellate Body Report, *Brazil – Retreaded Tyres*, para. 163.


\(^{921}\) *Ibid.*, paras. 166 and 172.


\(^{924}\) *Ibid.*, para. 6.599.
nuanced then the current understanding of the other three standards considered in Sections 4.3.1-4.3.3 above. However, it is precisely the availability of extensive WTO case law on the chapeau that presents the biggest risks in replicating the same standard in the future digital trade exception for privacy and data protection.

First, on the face of it, the standard of the chapeau appears to be less stringent than that of the necessity test of the general exception, because it aims at the assessment of the administration of a contested measure rather than its content and does not require that the measure should be the least trade restrictive. However, in practice, its interpretation was dangerously close to the necessity test. The latter, as explained in Chapter 2 of this thesis, does not leave the EU enough regulatory autonomy to protect privacy and the protection of personal data in line with its constitutional framework. Second, one of the factors in the assessment of ‘arbitrary or unjustifiable discrimination’, namely, whether the contested measure requires other countries to adopt a regulatory framework that is ‘essentially the same’ as opposed to ‘comparable in effectiveness’, is likely to be at odds with the requirement of ‘essential equivalence’ that the EU constitutional framework (as interpreted by the CJEU) imposes on other countries’ legal frameworks as a condition for unrestricted transfers of personal data from the EEA to their territory.925

In relation to these risks, one could make two objections. First, that ‘unjustifiability’, which appears in the standard of the chapeau, imposes a lower threshold for contested measures than ‘necessity’. As the Appellate Body explained in Australia — Tobacco Plain Packaging (Honduras) Report in relation to Article 20 of the TRIPS Agreement (which prohibits unjustifiable encumbrance on the use of trademarks) and the ‘necessity’ requirement in other provisions of the TRIPS Agreement:

reference to the notion of justifiability rather than necessity in Article 20 suggests that the degree of connection between the encumbrance on the use of a trademark imposed and the objective pursued reflected through the term “unjustifiably” is lower than it would have been had a term conveying the notion of “necessity” been used in this provision. Accordingly, a consideration of whether the use of a trademark has not been “unjustifiably” encumbered should not be equated with the necessity test within the meaning of Article XX of the GATT 1994 or Article 2.2 of the TBT Agreement.926

925 For a discussion about the ‘essential equivalence’ requirement in EU data protection law, see Section 5.2.2.
926 WTO, Appellate Body Report, Australia — Tobacco Plain Packaging (Honduras and Dominican Republic), para 6.647.
This insight could be used to argue that the standard of the chapeau – due to the absence of similarity with ‘necessity’ – imposes a lower threshold than ‘necessity’.

The second objection is that despite similarity of wording, even if the chapeau standard is replicated in the future digital trade exception for privacy and data protection, it will not necessarily have the same meaning. For example, in *Australia — Tobacco Plain Packaging (Honduras)*, the Appellate Body also held that ‘arbitrary or unjustifiable discrimination’ in the chapeau of Article XX of the GATT 1994 ‘does not imply that the meaning imparted to this term in other contexts can be easily transplanted to the interpretation of Article 20 of the TRIPS Agreement’.927 Similarly, the WTO Secretariat, in its Note on ‘Necessity Tests’ in the WTO, explained that ‘even if there are similar thematic issues arising in the “necessity tests” in the different provisions in the WTO agreements, an interpretation developed in the context of a specific case or specific provision is not necessarily transposable to other provisions.’928 As a result, ““necessity tests” contained in different WTO Agreements or in different provisions of the same Agreement cannot necessarily be used interchangeably’.929

In response to these objections, this thesis contends that, although the meaning of the same terms is not ‘easily’ or ‘necessarily’ transplantable or transposable, such transplantation or transposition is not impossible, especially when the same words are used in another exception. WTO practice contains several circumstances in which this has happened. For example, there has been extensive cross-pollination between the interpretation of the notion of ‘likeness’ in the MFN, and national treatment provisions in the GATT 1994 and the GATS (despite the differences between them930), as well as between the general exceptions in Article XX GATT 1994 and Article XIV GATS – irrespective of the public policy objective involved – in WTO case law.931 Even outside the WTO system, WTO case law is likely to be very influential on adjudicators appointed in the framework of bilateral and regional trade agreements. For example, the EU proposal for the Dispute Settlement Chapter for the EU-New Zealand trade agreement, explicitly states:

---

927 Ibid., para. 6.646. See also Ibid., para. 6.627.
929 Ibid., para. 83.
931 On cross-pollination between the interpretation of the general exceptions in the GATT and the GATS, see Section 2.3.2. On cross-pollination between the interpretation of ‘likeness’ in the GATT and the GATS, see, e.g., WTO, Appellate Body Report, Argentina – Financial Services, para. 6.119, referring to WTO, Appellate Body Reports, EC – Seal Products, paras. 5.90, 5.87-5.88 and 5.101 (noting that ‘[its] interpretation of Articles II:1 and XVII of the GATS chimes with the Appellate Body’s interpretation of the most-favoured-nation and national treatment obligations in the context of the GATT 1994’.) Appellate Body Report, Argentina – Financial Services,
The panel shall also take into account relevant interpretations in reports of WTO panels and the Appellate Body adopted by the Dispute Settlement Body of the WTO.\footnote{Art. X 22 EU proposal for a Chapter [XX] on Dispute Settlement of the EU-New Zealand FTA, 13 June 2018.}

Prevailing uncertainty on whether, and to what extent, trade adjudicators may import the WTO case law on the chapeau of the general exception when interpreting the digital trade exception on privacy and data protection weighs strongly against the use of the chapeau’s threshold in such exception.

\subsection*{4.3.5.2 The need for a restrictive mechanism in the digital trade exception for privacy and data protection}

As opposed to the standard of the chapeau, the non-circumvention, non-avoidance, and reasonableness standards would be more suitable than the ‘it deems appropriate’ test to achieve the EU’s goals in liberalising cross-border data flows while preserving its autonomy to protect privacy and the protection of personal data as fundamental rights, as well as the broader goal of preserving the rules-based international trading system. This thesis argues that any of these three standards are suitable, because, as illustrated above, each of them is interpreted through reference to the other. In content, each of the standards affords broader regulatory space than the necessity test of the general exception on the one hand, and and narrower regulatory space than the ‘it considers necessary’ test of the national security exception (and, therefore, the ‘it deems appropriate test’ proposed in the EU model clauses), on the other hand. The fact that the principles of good faith and the prohibition of abuse of right constitute the common denominator for the interpretation of these thresholds ensures their flexibility and the possibility of tailoring their interpretation to different situations.

This flexibility, however, also has drawbacks. For example, the WTO case law on the chapeau and the national security exceptions – the bodies of WTO jurisprudence interpreting the principles of good faith and the abuse of right in relation to exceptions from trade obligations – elucidate that the content of these principles is a moving target. Academic research on these principles confirms this conceptualisation.

Good faith is a ‘broad and value oriented concept’.\footnote{Ziegler, Baumgartner (2015), p. 31-32; Kotzur (2009), para. 26.} When interpreting good faith, the WTO adjudicators usually uncover the underlying conflict of interests, which they then balance according to the case-by-case context.\footnote{Panizzon (2006), pp. 109-110. See Ziegler, Baumgartner (2015), p. 31-34; Kiss (2006), para. 4.} The legal value that the principle of good faith has in a particular (WTO) trade dispute depends on the functions of adjudicators, and ranges between regulative (\textit{infra legem,} in particular as applied in the \textit{US-Shrimp} by the
Appellate Body), corrective or jurisdictional (*contra legem*, in particular as embodied by the principle of prohibition of the abuse of right), and gap-filling or constitutive (*praeter legem*) functions. Panizzon rightly notes in relation to the abuse of right that its “elasticity” risks giving too much power into the hands of international tribunals. Kotzur emphasises that given the abstractness of the principle of good faith ‘it may inevitably contain the risk of an all too ambitious judicial activism’. These risks are exacerbated by the absence of ‘checks and balances to guarantee that international tribunals will dispose of this power responsibly’. It is for these reasons that even the proponents of the good faith doctrine, such as Lauterpacht, call for its application with caution and restraint. Ziegler and Baumgartner likewise warn that ‘in the absence of limitations on the adjudicatory mandate, tribunals should be careful not to engage in an overly broad use of the principle of good faith, which could negatively impact the quality of the legal reasoning and thus the legitimacy of the arbitral process’. What ‘careful’ and ‘responsibly’ means in international trade context is a judgement call. For Panizzon, this means ‘in accordance with the requirements of international peace and justice and in the light of the “growing integration of the international community,” as opposed to giving in to unilateral pressure by militaries or economically superior world powers’. In practice, the normative values guiding trade adjudicators in the application of these general concepts, as Chapter 3 has demonstrated, are predetermined by the dominant discourse adopted by those adjudicators.

To sum up, the circular interpretation of ‘non-circumvention’, ‘non-avoidance’, and ‘reasonableness’ and their ultimate anchoring in the general principles of good faith and the prohibition of abuse of right, which, as interpretative tools, allow adjudicators to determine the meaning of these standards on a case-by-case basis. This also means that, after a trade agreement has been negotiated, the parties to such an agreement have little influence on the interpretation of the agreement. This thesis contends that it is to a large extent the lack of trust in international trade adjudication, as well as internal policy agenda, that has led the EU to use the broadest of trade law exceptions – the national security exception – as a prototype for the digital trade exception for privacy and data protection to

---

937 Kotzur (2009), para. 26; Ziegler, Baumgartner (2015), p. 10 (noting that ‘good faith has a firm place as both a facilitating and a restraining agent’. Yet, as ‘an inherently abstract notion,’ it leaves ‘a broad margin of discretion to the person deciding whether the principle of good faith has been respected’.)
938 Panizzon (2006), p. 34.
939 Lauterpacht (1958), p. 164 (stating that ‘[t]he doctrine of abuse of rights is therefore an instrument which, apart from other reasons calling for caution in the administration of international justice, must be wielded with studied restraint’.)
941 Panizzon (2006), p. 34.
minimise the risk that trade adjudicators will shift the meaning of the exception towards a higher threshold for domestic privacy and data protection rules than intended by the drafters. This argument ties into the broader debate on the WTO legitimacy crisis and the rule-making power of adjudicating bodies.  

To ameliorate such lack of trust, the use of ‘non-circumvention’, ‘non-avoidance’ or ‘reasonableness’ thresholds in the future digital trade exception (rather than the ‘it deems appropriate’ threshold) should be accompanied by a restrictive mechanism controlling for the adjudicators’ power of interpretation. One example of such a mechanism is the Understanding on the interpretation of the prudential carve-out in CETA, already mentioned above. On the one hand, the Understanding contains high level principles intended to guide the interpretation of the prudential carve out by investment tribunals. For example, Principle 8.a states that ‘a Party may establish and enforce measures that provide a higher level of prudential protection than those set out in common international prudential commitments’, while Principle 8.b requires investment tribunals to ‘defer to the highest degree possible to regulations and practices in the Parties’ respective jurisdictions and to the decisions and factual determinations, including risk assessments, made by financial regulatory authorities.’

On the other hand, the Understanding regulates the role of the Financial Services Committee (which includes representatives of authorities in charge of financial services policy with expertise in the field) in investment disputes concerning the prudential carve out. In particular, the Understanding determines that the Committee ‘shall decide whether and, if so, to what extent the prudential carve-out is a valid defence to a claim’. This decision, as well as the decision of the CETA Joint Committee (which is competent to make this decision if the Financial Services Committee does not provide its position within a specified term), is binding on the investment tribunal in the dispute in question. Thus, if the Financial Services Committee or the CETA Joint Committee conclude that the prudential carve-out is the valid defence to all parts of the claim in their entirety, the ‘investor is deemed to have withdrawn its claim and the proceedings are discontinued’.
Looking ahead, if the EU should decide to create a committee for privacy and data protection in a future trade agreement, further research is required to determine what the structure and composition of such a committee should be. This research is, however, beyond the scope of this thesis. What can be said at this juncture is that it is important to ensure that the conferral of certain powers on such a committee does not overstep the EU’s competence and constitutional boundaries.947

4.4 Conclusion

This Chapter has addressed the international trade aspect of the Catch-22 problem identified in Chapter 2 of this thesis, represented by a possible clash between the EU’s constitutional framework on privacy and data protection, on the one hand, and existing international trade commitments relating to cross-border data flows, on the other. It has demonstrated that the model clauses on cross-border data flows and the protection of privacy and personal data, proposed by the European Commission in 2018 are not the most optimal way to achieve the goals of the EU’s digital trade policy on data. In other words, they are unlikely to contribute to the liberalisation of cross-border data flows from other countries into Europe and may contribute to further undermining of the rules-based international trading system. This Chapter has proposed several ways to improve the model clauses with a specific focus on the threshold of the future digital trade exception for privacy and data protection. It has argued that a ‘non-circumvention’, ‘non-avoidance’ or ‘reasonableness’ threshold, anchored on the principles of good faith and prohibition of abuse of rights, and complemented by a restrictive mechanism controlling for trade adjudicators’ rule-making power, are better suited to achieve the EU’s digital trade policy goals, as compared to the ‘it deems appropriate’ threshold proposed in the EU’s model clauses.

947 For a discussion on this issue see, e.g., Weiß (2018).
5. EU framework for transfers of personal data: critique and directions for reform

5.1 Introduction

This Chapter addresses the problem of the ‘two necessities’ identified in Chapter 2 of the thesis from an EU Charter and EU data protection law perspective. The arguments in this Chapter are structured along the following three broad issues: (1) the constitutional boundaries the EU Charter imposes on EU secondary law governing transfers of personal data outside the EEA; (2) the ability of the current EU framework for transfers of personal data outside the EEA to perform its constitutional function; and (3) the reform proposal for such framework in response to changed (geo)political and economic circumstances.

The first issue on the constitutional boundaries set by the EU Charter on EU secondary law is a relatively unexplored topic in current academic debates. Relying on prevailing opinion, this Chapter approaches this issue through the prism of Article 51(2) of the Charter, which contains two layers of requirements with respect to derogations from fundamental rights: such derogations must respect the ‘essence’ of those fundamental rights and be ‘strictly necessary’ and proportionate. In other words, the essence (or the core) of fundamental rights cannot be interfered with by secondary EU law. Other derogations from fundamental rights are possible, provided that they meet the necessity and proportionality tests. This Chapter argues that there is a dynamic relationship between the GDPR (as a secondary EU law instrument) and the EU Charter (as a primary law instrument), in that EU secondary law has, to some extent, influenced the essence of the fundamental right to the protection of personal data. At the same time, only a few aspects of the current framework for transfers of personal data constitute the essence of the fundamental rights to privacy, to the protection of personal data and to effective judicial remedy (in the context of the first two rights), which cannot be changed by secondary EU legislation. The concept of ‘essential equivalence’, which, following the CJEU Schrems II judgement, can be seen as the constitutional benchmark for the secondary law framework on transfers of personal data, does not constitute a part of the essence of the above-mentioned fundamental rights. Instead, this concept is an instantiation of the strict necessity and proportionality requirements under Article 52(1) of the EU Charter in the context of transfers of personal data. It governs the balancing of the above-mentioned fundamental rights against competing policy objectives, primarily economic benefits inherent in unrestricted cross-border flows of personal data, and the national security interests of foreign countries. Building on this normative legal framework under EU law,

948 As explained in Section 2.3.3, the for derogations from the fundamental rights to privacy and data protection, the CJEU has elevated the ‘necessity’ threshold under Art. 52(1) EU Charter to ‘strict necessity’.
this Chapter contends that the EU legislator has sufficient wiggle room to change the
design of the rules currently codified in Chapter V of the GDPR.

The second issue is the ability of the current EU framework for transfers of personal
data under Chapter V of the GDPR to perform its constitutional function against the
background of circumstances that have changed since this framework was first designed.
As already mentioned elsewhere in this thesis, this framework’s main function is to prevent
circumvention of the high level of personal data protection in the EU and, ultimately, to
ensure ‘effective and complete’ protection of fundamental rights. This Chapter identifies
four weaknesses in this framework.

The first weakness is that, despite the recent Schrems II judgement, there is a
persistent qualitative gap between the adequacy decisions on the one hand, and the
appropriate safeguards under Article 46 of the GDPR on the other (both of which serve as
mechanisms for systematic transfers). In other words, the level of protection ensured by
adequacy decisions, even considering their flaws, is higher than the level of protection that
can be achieved through private law mechanisms under Article 46 of the GDPR. In the
Schrems II, the CJEU shifted the requirements of assessing the adequacy of foreign legal
frameworks towards the companies, many if not most of which lack the necessary
expertise, resources and incentives to conduct those assessments, or even to the DPAs,
which lack human and financial resources. This is unlikely to solve the problem. Instead,
this Chapter predicts that the lawfulness of transfers of personal data will ultimately be
decided by EU member state courts following private enforcement efforts, which, at least
in the short and medium term, may lead to the fragmentation of the rules for transfers of
personal data outside the EEA across Europe. Only in the long term can this fragmentation
be remedied through references for preliminary ruling to the CJEU. This Chapter argues
that the EU should address the foreign surveillance problem – which is the main reason
why issues relating to transfers of personal data land at the CJEU – on the international
level rather than through its own secondary law. The second weakness is, as this Chapter
argues, that adequacy decisions are prone to political pressures in the context of EU trade
policy. The third weakness is that adequacy decisions are unable to perform their
constitutional function due to lack of regular reviews of the assessment on which the
adequacy decisions are based (the ‘snapshot’ problem), the difficulties of enforcing
individual rights in foreign jurisdictions (the ‘heavy burden’ problem), and the inadequacy
of onward transfer mechanism embedded in the adequacy decisions (the ‘onward transfer’
problem). The fourth and last weakness is, on a more abstract level, the limited scalability
of the current regime for personal data transfers in Chapter V of the GDPR in view of the

949 CJEU, Google Spain, para. 34; CJEU, Wirtschaftsakademie, para. 28; CJEU, CJEU, Jehovan todistajat,
para. 66; CJEU, Fashion ID, paras. 66, 70.
technological developments that have occurred since the 1990s, when the core of the framework was first designed.

The third and final issue addressed in this Chapter is the reform proposal for a new EU framework for transfers of personal data outside the EEA. Relying on the analysis in this thesis and existing reform proposals in the literature, this Chapter suggests three directions or lines of thought on how to improve the framework of Chapter V of the GDPR, reflecting possible short, medium, and long term strategies for the EU in this area.

To make those points, the Chapter proceeds as follows. Section 5.2 examines the constitutional contours of the EU’s framework for transfers of personal data, including the room for manoeuvre the EU legislator has in designing such a framework. Section 5.3 of this Chapter addresses the weaknesses of the current framework in Chapter V of the GDPR. Section 5.4 elaborates on the three directions of thought on how to ameliorate these weaknesses through a reform of the GDPR’s Chapter V. Section 5 concludes.

5.2 Constitutional contours of the EU’s framework for transfers of personal data

The EU maintains a ‘multi-level protection of fundamental rights’ comprised of primary and secondary law, which applies equally to the rights to privacy and the protection of personal data.\textsuperscript{950} As already mentioned elsewhere in this thesis, Articles 7 and 8 of the EU Charter protect the rights to privacy and the protection of personal data as fundamental rights. The EU legislator’s competence underlying the adoption of the GDPR is provided for in Article 16 TFEU, namely, the competence to ‘lay down the rules relating to the protection of individuals with regard to the processing of personal data’.

This Section tackles two questions regarding the relationship between EU primary and secondary data protection rules in the context of cross-border transfers of personal data. First, whether, and to what extent, the design of the current framework for transfers of personal data in Chapter V of the GDPR is grounded in the EU Charter. Another way to approach this question is to ask which parts of the framework cannot be changed without running afoul of the EU Charter requirements for data transfers. The second, and more general, question is how much leeway, in the view of the EU Charter, the EU legislator has in designing the mechanisms for transfers of personal data in the GDPR.

5.2.1 The relationship between the EU Charter and EU secondary data protection law

In the hierarchy of EU law, secondary law is, as the name suggests, below primary law, which, in turn, has the highest legal force in the EU.\textsuperscript{951} Therefore, from a formalistic perspective, secondary law should be consistent with primary law. However, in practice –

\textsuperscript{950} Brkan (2019), p. 865.
\textsuperscript{951} Craig, De Burca (2015), pp. 105, 110.
as demonstrated by CJEU jurisprudence – this relationship is not as clear-cut as it may seem\(^{952}\) and is underexplored in academic literature, especially when it comes to the relationship between the EU Charter and the EU framework for data transfers.

Based on CJEU case law, Syrpis argues that EU secondary law may relate to EU primary law in at least three different ways. First, as just mentioned, in some cases the CJEU views primary law as hierarchically superior to secondary law, meaning that secondary law is rendered inapplicable when in conflict with primary law. Second, in other cases, the CJEU interprets primary and secondary law ‘neutrally’, meaning that interpretation of primary law affects the interpretation of secondary law and vice versa. Third, in yet other cases, secondary law has a significant impact on the CJEU’s interpretation of primary law and, to some extent, determines its content.\(^{953}\) In sum, Syrpis claims that the CJEU’s approach on this issue has been inconsistent, which gives the EU legislator the power to affect the CJEU’s interpretation of EU Treaties.\(^{954}\)

Thus, the modes of relationship between primary and secondary law that can be deduced from CJEU case law broadly represent two diverging approaches to the ‘proper’ relationship between EU primary and secondary law. The first, which this Chapter calls a static approach, puts the emphasis on the formal CJEU powers to interpret secondary law in the light of primary law and invalidate the former when contrary to the latter,\(^{955}\) and corresponds with the hierarchical relationship between EU primary and secondary law. The second, which this Chapter calls a dynamic approach, adopts a less hierarchical view of primary and secondary law, in which secondary law, although limited by the primacy of primary law (and should be annulled if the legislature has ‘manifestly’ or ‘manifestly and gravely’ exceeded the limits of its powers\(^{956}\) ), reflects the ‘(democratic) will expressed by the political [EU] institutions’ and, therefore, should able to affect the interpretation of EU primary law by the Court.\(^{957}\) This dynamic approach corresponds to the second and third ways of interaction between primary and secondary law, as identified by Syrpis.

Following the dynamic approach to the relationship between EU primary and secondary law, Muir explains that EU secondary legislation can implicate fundamental rights in three ways.\(^{958}\) First, based on the EU competence to legislate on fundamental rights, some EU secondary legislation is designed to ‘give specific expression’ to a

\(^{953}\) Ibid., pp. 465-467.
\(^{954}\) Ibid., p. 466.
\(^{955}\) Ibid., pp. 482-483.
\(^{956}\) Ibid., pp. 484.
\(^{957}\) Ibid., p. 483-485
fundamental right.\textsuperscript{959} Second, legislative instruments designed to implement an ‘ordinary’ EU competence – a competence other than fundamental rights protection – can incidentally set fundamental rights standards.\textsuperscript{960} Finally, EU secondary legislation can merely define the scope of the EU courts’ fundamental rights jurisdiction.\textsuperscript{961}

Based on the ways of thinking about the relationship between EU primary and secondary law proposed by Syripsis and Muir, this Section contends, first, that Chapter V of the GDPR (as well as Section V of the GDPR’s predecessor – the Data Protection Directive) should be viewed as secondary legislative instruments ‘giving specific expression’ to the fundamental rights, and establishing a system of checks and balances on the limitations of those fundamental rights. Second, the Chapter argues that there is a dynamic relationship between the EU framework on transfers of personal data and the EU Charter. This relationship manifests itself in the concept of ‘essential equivalence’, first introduced through the interpretation of the concept of ‘adequacy’ in Article 25 of the Data Protection Directive in the light of the EU Charter, and later injected into Chapter V of the GDPR as the central constitutional requirement for compliance of any systematic transfer of personal data outside the EEA, rather than just adequacy. The discussion below elaborates on each of these points.

The relationship between EU primary and secondary law in the area of data protection is not clear-cut. On the one hand, the limited CJEU case law concerning the fundamental right to the protection of personal data enshrined in Article 8 of the Charter leans towards a more hierarchical approach between the two. For example, in Digital Rights Ireland the CJEU invalidated the EU Data Retention Directive because by adopting it ‘the legislature exceeded the limits imposed by compliance with the principle of proportionality in the light of Articles 7, 8 and 52(1) of the Charter (of Fundamental Rights)’.\textsuperscript{962} In Schrems I, the CJEU invalidated the Commission’s implementing act approving the EU-US Safe Harbor,\textsuperscript{963} and in Schrems II, the Commission’s implementing act approving the Safe Harbor’s successor – the EU-US Privacy Shield.\textsuperscript{964} In the Opinion on EU-Canada PNR Agreement, the CJEU found the draft EU-Canada PNR agreement inconsistent with the EU Charter, treating the agreement as an ‘equivalent externally, of that which is a legislative act internally’.\textsuperscript{965} On the other hand, the origins of this fundamental right, as well as the evolution of the concept of ‘essential equivalence’ in the

\textsuperscript{959} Ibid., pp. 223-226, emphasis added.
\textsuperscript{960} Ibid., pp. 226-227.
\textsuperscript{961} Ibid., pp. 227-229.
\textsuperscript{962} CJEU, Digital Rights Ireland, para 69.
\textsuperscript{963} CJEU, Schrems I.
\textsuperscript{964} CJEU, Schrems II, paras. 150-202.
\textsuperscript{965} CJEU, Opinion on EU-Canada PNR Agreement, para. 146.
design of the EU framework for transfers of personal data, show that EU secondary law also influenced the conceptualisation of this right. This influence demonstrates a dynamic approach between the two.

The Data Protection Directive was adopted before the Lisbon Treaty and, as already mentioned above, was based on the EU internal market competence.\(^{966}\) It had a profound effect on the formation and the content of the fundamental right to the protection of personal data in the Charter.\(^{967}\) According to the Explanations relating to the Charter, one of the foundations of Article 8 of the Charter is that the Data Protection Directive contains ‘conditions and limitations for the exercise of the right to the protection of personal data’.\(^{968}\) Indeed, paragraph 2 of Article 8 can be seen as codifying the secondary law principles of fair and lawful data processing, the right of individuals to access their personal data, the right to rectification as well as the establishment of an independent supervisory authority to ensure compliance with the fundamental right – all of which were already present in the Data Protection Directive.\(^{969}\) In its 2015 Schrems I judgement, the CJEU pointed to a reverse relationship between the Data Protection Directive and the EU Charter (which was already legally binding at that time). The CJEU held that the Directive’s Article 25(6) governing the adequacy mechanism for transfers of personal data outside the EEA ‘implements the express obligation laid down in Article 8(1) of the Charter to protect personal data and … is intended to ensure that the high level of that protection continues where personal data is transferred to a third country’.\(^{970}\) This demonstrates that the relationship between the fundamental right to the protection of personal data and the EU Data Protection Directive was a two-way street.

Unlike the Data Protection Directive, the GDPR was ‘specifically adopted in order to give expression’ to the fundamental right to the protection of personal data.\(^{971}\) It constitutes secondary legislation adopted on the basis on Article 16 of the TFEU and the Charter. As rightly pointed out by Ausloos, the GDPR ‘has a primarily enabling or instrumental role’ of putting in ‘place an infrastructure of checks and balances to ensure fairness [of personal data processing]’ and setting ‘the parameters for legitimate processing

\(^{966}\) See Section 2.2.1.1.
\(^{967}\) Dalla Corte (2020), p. 45 (arguing that ‘[t]he right to data protection has been strongly shaped by the evolution of the secondary legislation’). See also Muir (2014), p. 226 (stating that ‘[a]lthough adopted in the mid–1990s as an internal market instrument on the basis of the equivalent of today’s Article 114 TFEU, in substance the Directive is specifically designed to give shape to a fundamental right’). Similar point of view is expressed by Dalla Corte (2020), pp. 44-45. But see Tzanou (2017), pp. 38-39, arguing that the meaning of Article 8 should be independent from EU secondary law.
\(^{968}\) Explanation to Art. 8, Explanations Relating to the Charter of Fundamental Rights, 2007 O.J. (C 303).
\(^{969}\) See Arts. 6, 7, 12 and 28 of the Data Protection Directive respectively. Art. 8 EU Charter is also based on Art. 8 ECHR and Convention 108, which has been ratified by all the Member States.
\(^{970}\) CJEU, Schrems I, para. 72. This goal is now explicitly incorporated in Art. 44 GDPR (emphasis added).
of personal data in the light of the Charter as a whole. This not only includes articles codifying the substantive fundamental rights, but also Article 52(1) of the EU Charter setting the boundaries for derogation from those fundamental rights. In general terms, while ‘Article 8 [of the] Charter is substantive, the GDPR is procedural’. This, however, does not mean that the right to the protection of personal data is the only fundamental right operationalised by the GDPR. In addition, just like the Data Protection Directive, the GDPR limits the fundamental rights enshrined in the EU Charter, as any processing of personal data constitutes a derogation from the fundamental right under Articles 7 and 8 of the Charter. The GDPR sets the rules for lawful processing of personal data, which must remain within the boundaries of Article 52(1) of the Charter governing derogations from the fundamental rights. This also means that the requirements of this article serve as a constitutional compass in the interpretation and application of the GDPR.

5.2.2 ‘Essential equivalence’: from EU secondary law to EU Charter and then back again

In the spirit of the dynamic relationship between EU primary and secondary law on data protection, in its Schrems I judgement the CJEU interpreted the term ‘adequate level of protection’ from Article 25(6) of the Data Protection Directive in the light of the EU Charter, ‘as requiring the third country in fact to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is “essentially equivalent” to that guaranteed within the European Union by virtue of Directive 95/46 read in the light of the Charter.’ This Article’s aim is to ensure continuity of the high level of personal data protection after personal data is transferred outside the EEA and to prevent circumvention of the EU data protection framework. Several scholars have argued that by interpreting ‘adequacy’ as ‘essential equivalence’ the CJEU has elevated the standard of data protection that a third country must meet to be afforded an adequacy decision.

In the Opinion on EU-Canada PNR Agreement, the CJEU applied the ‘essentially equivalent’ standard outside the context of the Data Protection Directive, in relation to the

---

972 Ausloos (2018), pp. 62-63. See also Clifford, Ausloos (2018), p. 147 (arguing that ‘the GDPR is a clear manifestation of a secondary framework built on checks and balances in order to respect ‘control’ as the essence of the right to data protection’), See also Dalla Corte (2020), p. 45.
973 Oostveen, Irion (2017); Ausloos (2018), pp. 62-63; Clifford, Ausloos (2018), p. 147. See also Section 1.1.3.
974 For a discussion, see Clifford, Ausloos (2018), pp. 148, 152-154.
976 CJUE, Schrems I, para. 73 (emphasis added).
977 Ibid.; CJEU, Opinion on EU-Canada PNR Agreement, para. 214; CJUE, Schrems II, para. 93.
draft EU-Canada PNR Agreement. Its compliance with the EU Charter was assessed in that case and did not fall under the scope of the Directive. Just as in Schrems I, however, the Court invoked the concept of ‘essential equivalence’ as an interpretation of the notion of ‘adequacy’ incorporated into the text of the draft Article 5 of the EU-Canada PNR Agreement. In that Opinion, the CJEU referred to the Schrems I judgement – without referring to the adequacy provision of the Directive – and stated that:

the transfer of personal data, such as PNR data, from the European Union to a non-member country is lawful only if there are rules in that country which ensure a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union.

This led Kuner to conclude that the CJEU’s reference to the standard of essential equivalence ‘leaves no doubt that this standard also applies to data transfers under international agreements’.

Although the CJEU did not explain the relationship between the concept of ‘essential equivalence’ and the assessment under Article 52(1) of the Charter, this Chapter contends that the Court used the concept of ‘essential equivalence’ as an instantiation of balancing under Article 52(1) of the EU Charter in application to the EU secondary law’s concept of ‘adequacy’. In other words, by ensuring that an adequacy decision guarantees that the level of personal data protection abroad is ‘essentially equivalent’ to that in the EU, the European Commission can strike the right balance under the strict necessity test of Article 52(1) of the EU Charter. This indirectly follows from the fact that, in Schrems I, the CJEU first conducted an assessment under Article 52(1) of the Charter (paragraphs 92 – 95) but then in paragraph 96 returned to the principle of ‘essential equivalence’ and finally in paragraph 98 concluded that the Commission’s decision was incompliant with Article 25(6) of the Directive read in the light of the Charter.

The relationship between restrictions on transfers of personal data as a component of the fundamental right under Article 8 of the Charter and its implementation in secondary law can also be illustrated by this quote from the CJEU Opinion on EU-Canada PNR Agreement:

That right to the protection of personal data requires, inter alia, that the high level of protection of fundamental rights and freedoms conferred by EU law continues

---

980 This Article states that ‘[s]ubject to compliance with this Agreement, the Canadian Competent Authority is deemed to provide an adequate level of protection, within the meaning of relevant European Union data protection law, for the processing and use of PNR data’. CJEU, Opinion on EU-Canada PNR Agreement, para. 86.

981 CJEU, Opinion on EU-Canada PNR Agreement, para. 93; see also ibid., paras. 134 and 214.

where personal data is transferred from the European Union to a non-member country. Even though the means intended to ensure such a level of protection may differ from those employed within the European Union in order to ensure that the requirements stemming from EU law are complied with, those means must nevertheless prove, in practice, effective in order to ensure protection essentially equivalent to that guaranteed within the European Union.983

This quote suggests that the principle of ‘essential equivalence’ is also a practical implementation of the constitutional requirement of continuity of protection in EU secondary law. Extrapolating the relationship between the fundamental right in Article 8 of the EU Charter and secondary data protection law, to the relationship between Article 52(1) of the EU Charter and the concept of ‘essential equivalence’, one can thus conclude that the first is substantive and the second is procedural; it is one of the tools in the toolbox of secondary law ensuring that the fundamental right is not derogated from further than is allowed under Article 52(1) of the EU Charter.

The interpretation of ‘adequacy’ as ‘essential equivalence’ later found its way to the text of the GDPR. Recital 104 of the GDPR states, in relation to the adequacy framework in Article 45 of the GDPR, that [t]he third country should offer guarantees ensuring an adequate level of protection essentially equivalent to that ensured within the Union, in particular where personal data are processed in one or several specific sectors. In particular, the third country should ensure effective independent data protection supervision and should provide for cooperation mechanisms with the Member States' data protection authorities, and the data subjects should be provided with effective and enforceable rights and effective administrative and judicial redress. (emphasis added)

The criteria to assess whether a foreign legal framework affords ‘essentially equivalent’ protection are listed in Article 45 GDPR. For systematic transfers of personal data to third countries not afforded an adequacy decision by the EU, however (such as those governed by Article 46 GDPR), the GDPR sets forth a requirement of ‘appropriate safeguards’.984 It should, therefore, be emphasised that, until Schrems II, as discussed below, the ‘essential equivalence’ requirement featured both in the CJEU case law discussed above, and in the GDPR, as the instantiation of the proportionality and strict necessity balancing under Article 52(1) of the EU Charter solely in relation to the adequacy mechanism for transfers of personal data, rather than in relation to the EU secondary law

983 CJEU, Opinion on EU-Canada PNR Agreement, para. 134. (emphasis added)
984 See also recital 107 GDPR.
framework for transfers of personal data as a whole. This created a qualitative gap – criticised in academic and policy discourse and discussed in more detail in Section 5.3.1 of this Chapter – between the level of protection that must be guaranteed to transferred personal data by an adequacy decision, on the one hand, and by appropriate safeguards under Article 46, such as the SCCs and the BCRs, on the other hand. In Schrems II, the CJEU confirmed its prior analysis of what the ‘essential equivalence’ standard requires in relation to an adequacy decision, but it also took an important step towards reinstating a consistent and holistic approach to the EU framework for transfers of personal data. In particular, the Court held that

data subjects whose personal data are transferred to a third country pursuant to standard data protection clauses are afforded, as in the context of a transfer based on an adequacy decision, a level of protection essentially equivalent to that which is guaranteed within the European Union.

The CJEU further explained that the level of protection of fundamental rights required by Article 46(1) of the GDPR ‘must be determined on the basis of the provisions of that regulation, read in the light of the fundamental rights enshrined in the Charter’. The factors that should be taken into account for such assessment in the context of Article 46 ‘correspond to those set out, in a non-exhaustive manner, in Article 45(2) of [the GDPR]’. One could, therefore, argue that not only adequacy decisions, but indeed all mechanisms for systematic transfers of personal data outside the EEA should provide an ‘essentially equivalent’ level of protection. Despite the fact that factors outlined in Article 45(2) of the GDPR – based on the textual interpretation – only apply to adequacy decisions, they should, when interpreted in the light of the EU Charter, be considered in the assessment related to any other mechanism for systematic transfer of personal data. By doing so, as explained above, the CJEU asserted the ‘essential equivalence’ standard as an instantiation of the ‘strict necessity’ and proportionality balancing under Article 52(1) of the EU Charter in the context of the whole framework for systematic transfers of personal data in EU secondary data protection law. It is no longer a constitutional interpretation of ‘adequacy’, but has acquired a meaning independent of ‘adequacy’. The factors for adequacy assessment became a part of such ‘essential equivalence’ requirement. This outcome fits with the understanding of the GDPR as a legal framework creating the system of checks and balances that enable the protection of the fundamental rights. Based on this, all provisions of the GDPR, and therefore, all mechanisms for systematic transfers of

---

985 CJEU, Schrems II, para. 176.
986 For a discussion, see Christakis (2020); Kuner (2020d).
987 CJEU, Schrems II, para. 96 (emphasis added); see also Ibid., para. 105
988 CJEU, Schrems II, para. 101.
989 CJEU, Schrems II, para. 104.
personal data, should meet the strict necessity test provided in Article 52(1) of the Charter.\footnote{Clifford, Ausloos (2018), pp. 148, 152.}

To sum up, ‘essential equivalence’ is the EU Charter requirement in relation to the level of personal data protection that any EU secondary law mechanism for transfers of personal data should ensure. Recall, in addition, that the standard of ‘essentially equivalent’ protection is not only the CJEU’s creation in the line of cases on cross-border transfers of personal data.\footnote{Azoulai, van der Sluis (2016), p. 1363.} It closely resembles the ‘essentially comparable’ standard used by the German Constitutional court in the 1986 Solange II case when assessing the level of fundamental rights protection in the EU as compared to the German legal order, and codified in Article 23 of the German Basic Law.\footnote{Ibid., p. 1363; Mayer (2015); Wünsche Handelsgesellschaft decision of 22 October 1986, BVerfGE 73, 339, case number: 2 BvR 197/83, Europäische Grundrechte-Zeitschrift, 1987, 1, [1987] 3 CMLR 225 (Solange II).} The fact that the Solange I was one of the reasons that prompted the EU transition from an economic to a constitutional union,\footnote{For a discussion, see, e.g., Perju (2017).} supports the conclusion that the standard of ‘essential equivalence’ is very likely to ‘stick’ even without adequacy being mentioned in the EU secondary law. In any event, what matters is that the CJEU determined that this standard constitutes a yardstick to gauge the permissible derogations from the fundamental rights set forth in Article 52(1) of the Charter in the context of transfers of personal data outside the EEA.

5.2.3 The concept of the ‘essence’ of fundamental rights

The previous Section has argued that the GDPR sets up a system of checks and balances for the legitimate processing of personal data in the light of the EU Charter. It has concluded that the EU primary law, and more specifically the EU Charter, set the boundaries for the legislature to regulate transfers of personal data outside the EEA in the form of the ‘essential equivalence’ requirement. This Section looks into the question of those boundaries more specifically and circumscribes the degree of discretion that the EU legislature has in designing the framework of cross-border transfers of personal data outside the EEA.

The EU law concept that seems to be most helpful in drawing a red line between the elements of a fundamental right that can and cannot be restricted is the concept of the ‘essence’ of fundamental rights, which appears in Article 52(1) of the EU Charter.\footnote{Dawson, Lynskey, Muir (2019), p. 767.} This provision requires that any limitation on the exercise of the fundamental rights must (a) be
provided for by law (first sentence), (b) respect the essence of those rights (first sentence) and (c) meet the principles of proportionality and necessity (second sentence).

The concept of the ‘essence’ of fundamental rights in general, and of the fundamental rights to privacy and the protection of personal data in particular, remains ‘elusive’ in the CJEU case law and relatively unexplored in academic literature.\(^\text{995}\) Gellert and Gutwirth even dismiss the ‘assumption that there is, eventually and behind all descriptions, such thing as an essence of privacy and data protection’.\(^\text{996}\) This Section looks into the meaning of the ‘essence’ of fundamental rights, in general and in application to the fundamental rights to privacy and the protection of personal data, with the aim to determine what – if anything – constitutes the essence of those fundamental rights in relation to transfers of personal data outside the EEA. In doing so, this Section relies on the relatively scarce literature and CJEU case law available on this topic.

Scholars generally agree that the notion of ‘essence’ is an ‘absolute limit to balancing, i.e. to underline that a certain interference actually “destroys” a certain right or strips it of any content’.\(^\text{997}\) Relying on the CJEU case law on the fundamental rights to privacy and the protection of personal data, Brkan convincingly argues that the concept of the ‘essence’ of fundamental rights contained in Article 52(1) of the EU Charter is ‘an independent constitutional concept that is not a part of the principle of proportionality’.\(^\text{998}\) This means that an interference with the essence of a fundamental right cannot be justified based on a necessity and proportionality assessment.\(^\text{999}\) Along similar lines, CJEU’s President Koen Lenaerts noted that where an ‘EU measure fails to take due account of the essence of a fundamental right, that measure is incompatible with the Charter and must be annulled or declared invalid.’\(^\text{1000}\) As the Advocate General Henrik Saugmandsgaard Øe argued in the Schrems II case,

\[
\text{when an interference compromises [the essence of] those rights and freedoms, no legitimate objective can justify it. The interference is then deemed to be contrary to the Charter without it being necessary to examine whether it is appropriate and necessary for the purpose of achieving the objective pursued.} \quad \text{1001}
\]

\(^{999}\) Ibid., p. 883.
\(^{1000}\) Lenaerts (2019), pp. 779, 782.
\(^{1001}\) Opinion AG in Schrems II, para. 272. See also EDPS, Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data, 19 December 2019, p. 8.
In other words, a measure interfering with the essence of a fundamental right is ‘automatically disproportionate’,\(^{1002}\) which makes, in Lenaerts’ view, the ‘essence test’ and the ‘proportionality test’ (including where there is a particularly serious interference with a fundamental right at stake) two separate lines of inquiry under Article 52(1) of the EU Charter.\(^{1003}\) Building on the CJEU’s judgement in Schrems I, Lenaerts further explains that the ‘essence’ of a fundamental right refers to its ‘hard nucleus’, which is *absolute* and ‘must always remain free from interference’.\(^{1004}\) This concept thus suggests that the EU legislator may only ‘determine non-essential elements’ of those rights, and that secondary law may not affect the absolute ‘nucleus’ of those rights under the Charter.\(^{1005}\) More generally and relatedly, the EU legislator’s discretion in using secondary law to operationalise fundamental rights is proportionate to the level of interference with fundamental rights that the legislation in question entails.\(^{1006}\) Applying this line of reasoning to the GDPR, one can conclude that the GDPR, which operationalises the fundamental rights to privacy and data protection by setting the limits within which these fundamental rights can be interfered with,\(^{1007}\) may only permit derogation from these fundamental rights to the extent it does not interfere with their nucleus. Put differently, any GDPR rule must respect the ‘essence’ of the fundamental rights affected by data processing, and primarily the rights to privacy (Article 7 of EU Charter), the protection of personal data (Article 8 of EU Charter) and judicial remedy (Article 47 of EU Charter), which most often feature in the CJEU case law touching upon the ‘essence’ of fundamental rights in the context of personal data processing.

To sum up, unlike the shades of grey in balancing in the assessment of necessity and proportionality under Article 52(1) of the EU Charter, the assessment of whether the ‘essence’ of fundamental rights was respected is black and white: either the interference with the fundamental right respects the essence of that right, or it does not.

5.2.4 The ‘essence’ of the fundamental rights to privacy, protection of personal data and judicial remedy

In order to operationalise the concept of the ‘essence’ of fundamental rights in the context of this thesis, it is important to understand what – if anything – constitutes the essence of the fundamental rights to privacy and the protection of personal data, as well as

---


\(^{1007}\) As noted above, in the view of the CJEU and the EU Data protection Authorities, any processing of personal data constitutes a derogation from the fundamental right to privacy and the protection of personal data. CJEU, *Digital Rights Ireland*, paras. 34 – 36; CJEU, *Volker und Markus Schecke*, para. 58. See also EDPS, *Assessing the Necessity of Measures That Limit the Fundamental Right to the Protection of Personal Data: A Toolkit*, 11 April 2017, p. 7.
the right to effective remedy in the context of interferences with the first two fundamental rights, as applied in a line of CJEU jurisprudence. Unfortunately, both the role of the ‘essence’ and the definition of the ‘essence’ in relation to the above-mentioned fundamental rights is not yet fully developed in the CJEU jurisprudence and academic literature.1008

Although the Court’s approach to the conceptualisation of essence and its conclusions could be criticised as ‘contentious’1009 and lacking ‘coherence’ and ‘conceptual clarity’,1010 it is beyond the scope of this thesis to engage more fully with such critique. Using available CJEU jurisprudence on the topic and its interpretation in literature, this thesis addresses only three issues that are germane to it. First, it considers the aspects that constitute the essence of the fundamental rights protection of privacy, personal data and the right to effective remedy in the context of the first two rights based on existing CJEU case law. Second, it analyses whether restrictions on transfers of personal data outside the EEA, and the concept of ‘essential equivalence’, constitute a part of the essence of the right to the protection of personal data. Third, it examines whether there is a ‘rule of thumb’ on how to identify the essence of the relevant fundamental rights in situations not yet addressed by the CJEU, in particular, in relation to transfers of personal data outside the EEA.

The CJEU has interpreted the notion of the ‘essence’ of the fundamental rights to privacy, the protection of personal data and judicial remedy (in the context of the other two rights) in five judgements thus far: Digital Rights Ireland, Tele2 Sverige, Schrems I and II, and Opinion on EU-Canada PNR Agreement. In Schrems I, the CJEU held that ‘legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter.’1011 In contrast, legislation, which ‘authorises, on a generalised basis, storage of all the personal data of all the persons whose data has been transferred … without any differentiation, limitation or exception being made’ does not interfere with the ‘essence’ of the right to privacy, but rather violates the principle of ‘strict necessity’ under the second sentence of Article 52(1) of the Charter.1012 The Court reached the same conclusion in

1011 CJEU, Schrems I, para. 94 (emphasis added). Brkan extensively criticises this distinction between the data that constitutes the content of electronic communications and the metadata, as large volumes of metadata can reveal almost as much personal data about the individuals as, or even more than, the content of communications. Brkan (2019), pp. 872-873, 879.
1012 CJEU, Schrems I, para. 93.
In his Opinion in Schrems II, the Advocate General continued the CJEU’s approach in prior cases that, as long as there is no ‘generalised access by the public authorities to the content of the electronic communications’, there is no ‘breach of the very essence’ of the right to privacy. In its Schrems II judgement, the CJEU, however, followed neither its own line of reasoning in Schrems I nor that of the Advocate General; it remained silent on whether the EU-US Privacy Shield interfered with the essence of the right to privacy or the right to protection of personal data. Instead, it held that EU-US Privacy Shield did not ensure ‘essential equivalent’ protection because ‘limitations on the protection of personal data arising from the domestic law of the United States … are not circumscribed in a way that satisfies requirements that are essentially equivalent to those required, under EU law, by the second sentence of Article 52(1) of the Charter.’ The CJEU also did not mention the issue of generalised access by public authorities to the content of electronic communications. In the Opinion on EU-Canada PNR Agreement, where access to content or other electronic communications data was not the issue, the CJEU concluded that the EU-Canada PNR Agreement did not interfere with the right to privacy because although ‘PNR data may, in some circumstances, reveal very specific information concerning the private life of a person, the nature of that information is limited to certain aspects of that private life, in particular, relating to air travel between Canada and the European Union.’

In relation to the right to effective remedy under Article 47 of the Charter, in the context of the rights to privacy and the protection of personal data, the CJEU found that the essence of this right was not respected in two cases. In Schrems I and Schrems II the CJEU held that ‘legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter.’

Unlike the fundamental right to privacy, the CJEU has not yet found a violation of essence of the fundamental right to the protection of personal data. In Digital Rights Ireland, the Court concluded that there was no such interference because the contested Data Retention Directive required respect of ‘certain principles of data protection and data

1013 CJEU, Digital Rights Ireland, paras. 37, 39, 69, 73.
1014 CJEU, Tele2 Sverige, para. 101.
1015 Opinion AG in Schrems II, para 278.
1016 CJEU, Schrems II, para. 185. This deviation from Schrems I could be attributed to the critique of the CJEU’s Schrems I approach to finding the interference with essence of the fundamental right. See e.g. Brkan (2019), pp. 877-878.
1017 Ibid.
1018 Ibid.
1019 CJEU, Opinion on EU-Canada PNR Agreement, para 150.
1019 CJEU, Schrems I, para. 95; CJEU, Schrems II, para. 187 (emphasis added).
security’ in order to ‘ensure that appropriate technical and organisational measures are adopted against accidental or unlawful destruction, accidental loss or alteration of the data.’ In Tele2 Sverige, where the CJEU discussed the right to privacy and to the protection of personal data jointly, the CJEU held that as long as the contested legislation ‘does not permit retention of the content of a communication’, it does not affect adversely the essence of the right to the protection of personal data. In the Opinion on EU-Canada PNR Agreement, the CJEU found that the EU-Canada PNR Agreement did not interfere with the essence of the fundamental right to data protection for two reasons: first, because it limited ‘the purposes for which PNR data may be processed’, and second, because it contained the rules to ensure ‘the security, confidentiality and integrity of that data, and to protect it against unlawful access and processing’. The Advocate General in his Opinion in Schrems II followed the CJEU’s line of reasoning in Opinion on EU-Canada PNR Agreement, namely that the essence of the right to protection of personal data, guaranteed in Article 8 of the Charter, is preserved when the purposes of the processing are limited and the processing is accompanied by rules designed to ensure, inter alia, the security, confidentiality and integrity of the data, and also to protect them against unlawful access and processing.

The Advocate General further noted that, although there was a doubt whether the US surveillance programmes, allowed under the EU-US Privacy Shield, defined the purposes of processing of personal data ‘with sufficient clarity and precision to ensure a level of protection essentially equivalent to that prevailing in the legal order of the Union’, ‘those possible weaknesses would not suffice … to substantiate a finding that such programmes would … violate the essence of the right to protection of personal data’. In its Schrems II judgement, the CJEU did not separate the issue of interference with the essence of the fundamental right to protection of personal data from the interference with the fundamental right to privacy.

Brkan criticises the CJEU’s approach to the essence of fundamental rights, noting that in relation to privacy it is quantitative instead of qualitative, and in relation to the protection of personal data – ‘extremely restrictive and technical’. In the latter case, she

---

1020 CJEU, Digital Rights Ireland, para. 40.
1021 CJEU, Tele2 Sverige, para. 101. The Court discusses the right to privacy and the right to the protection of personal data at the same time by referring to ‘these rights’.
1022 CJEU, Opinion on EU-Canada PNR Agreement, para 150.
1023 Opinion AG in Schrems II, para 279.
1024 Ibid., para 280.
1025 See, e.g., CJEU, Schrems II, paras. 169-172, 178, 199.
1027 Ibid., pp. 878-879.
argues, the Court reduced the essence of the right to certain aspects of it, turning the core of the right to a minimum rather than a maximum standard.\textsuperscript{1028} In contrast, Lenaerts argues that the essence of the fundamental rights to privacy and the right to effective judicial remedy is only compromised when ‘the limitation in question empties those rights of their content or calls their very existence into question’.\textsuperscript{1029} The same logic arguably applies to the protection of personal data. From his perspective, the ‘essence’ should be interpreted restrictively so that it can only be compromised in ‘extreme cases’, because a broad understanding of this concept would make fundamental rights absolute, which is undesirable in a democratic society.\textsuperscript{1030}

This overview of the CJEU case law shows that the nucleus of the fundamental right to privacy and, even more so, the fundamental right to the protection of personal data is rather small. To sum up, the CJEU case law suggests that secondary EU law must:

- Not permit generalised access to the content of electronic communications \textit{in order to respect the essence of the fundamental right to privacy}.
- (a) Limit the purposes of processing (i.e. respect the purpose limitation principle); (b) require that the processing of personal data is accompanied by rules designed to ensure, inter alia, the security, confidentiality and integrity of the data, and also to protect them against unlawful access and processing, and (c) not permit retention of the content of communications \textit{in order to respect the essence of the fundamental right to the protection of personal data}; and
- Provide scope for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, in order to respect the \textit{essence of the fundamental right to judicial remedy in the context of privacy and data protection}.

From this summary it is clear that, rather than defining the ‘essence’ of the fundamental rights to privacy, protection of personal data and effective remedy, the CJEU has chosen to distil, on a case-by-case basis, a number of requirements that EU secondary law should meet in order for the essence of the respective rights to be respected.

The next question is whether restrictions on transfers of personal data and in particular the standard of ‘essential equivalence’ constitute the essence of the fundamental rights to privacy and the protection of personal data. At the outset, it should be mentioned that restrictions on transfers of personal data are not mentioned among the elements of this

\textsuperscript{1028} Brkan (2019), pp. 878-879.
\textsuperscript{1029} Lenaerts (2019), p. 784.
\textsuperscript{1030} Ibid., p. 793.
fundamental right codified in Article 8(2) of the EU Charter. This, however, is not a decisive factor, because, as Brkan convincingly argues, although these elements are ‘constitutive of this fundamental right’ they do not automatically constitute its essence.\footnote{Brkan (2019), p. 881-882. See also Dalla Corte (2020), p. 46 (expressing the same point of view.) But see Kuner (2015b), pp. 243-244 (suggesting as a preliminary thought that rights listed in Article 8 of the EU Charter could be viewed as the ‘essence’ of the fundamental right to the protection of personal data.)} Conversely, the fact that a certain element of the right is not mentioned in this provision does not mean that it does not constitute the essence of the right.

Based on the fact that both in Schrems I and II as well as in Opinion on EU-Canada PNR Agreement the CJEU assessed whether EU law instruments ensured an ‘essentially equivalent’ level of protection by conducting a balancing exercise on the basis of the second sentence of Article 52(1) of the EU Charter, one can conclude that the ‘essential equivalence’ requirement does not constitute the essence of any of the fundamental rights discussed in this Section.\footnote{Brkan’s analysis of whether essentially equivalent level of protection and the concept of essence of fundamental rights should be equated supports this conclusion. Brkan (2019), p. 865.} The assessment of whether the standard of ‘essential equivalence’ is met is the second step in the assessment under Article 52(1) of the EU Charter. This conclusion confirms the finding above that ‘essential equivalence’ is the instantiation of the ‘strict necessity’ requirement of Article 52(1) of the EU Charter in application to transfers of personal data outside the EEA.

Until now, the CJEU dealt with the question of the essence of the fundamental rights to privacy, the protection of personal data, and to judicial remedy (in the context of the first two rights) on a case-by-case basis. One could ask whether there is, or could be, a rule of thumb which would allow a line to be drawn between the absence of respect of the essence of a fundamental right and a particularly serious interference with the right, which should be balanced with an overriding public interest on the basis of principles of necessity and proportionality.

Although the requirements listed above apply to all secondary data protection rules, including those governing transfers of personal data outside the EEA, the CJEU case law does not offer a rule of thumb to determine, more generally, what constitutes the essence of the fundamental rights to privacy, data protection and judicial remedy (in the context of the first two rights), and whether a specific design of rules on transfers of personal data outside the EEA is necessary in order to respect this essence. While some scholars argue that there is no ‘fixed or universally valid essence of rights that can be conceptually deduced’ and that the “‘European essence” of fundamental rights’ can only be determined ‘inductively by analysing the jurisprudence of the courts with regard to certain infringements upon certain rights that cannot be justified’\footnote{Von Bogdandy, Kottmann, Antpöhler, Dickschen, Hentrei, Smrkolj (2012), p. 511.}, others offer ways of thinking
about the essence of the fundamental rights, which could be useful in answering the question posed above.

Generalising the Court’s approach, Lenaerts concludes that the limitation of a fundamental right respects its essence if it ‘does not call [it] into question as such’.1034 Therefore, if a limitation concerns only ‘certain aspects of a fundamental right, leaving others untouched, or that only applies in a specific set of circumstances regarding the individual conduct of the person concerned’, the essence of the fundamental right is respected.1035 The key factors the Court uses in this assessment are the intensity and the extent of the limitation of the fundamental right at issue.1036 The next Section discusses how this analysis can apply to rules on transfers of personal data outside the EEA.

5.2.5 The ‘essence’ and restrictions on transfers of personal data outside the EEA

Although transfers of personal data outside the EEA affect not only the fundamental right to the protection of personal data but also the right to privacy, this Section focuses on the essence of the fundamental right to the protection of personal data. The reason for this is that the ‘home’ of the EU secondary law framework on transfers of personal data outside the EEA is in the GDPR, which, in the first place, effectuates the fundamental right to the protection of personal data. This right is thus most relevant for the purposes of this Section, which considers approaches to the essence of fundamental rights proposed in the context of the governance of data processing in the GDPR.

For the purposes of this Section, the most useful ways of thinking about the essence of the fundamental right to the protection of personal data are those proposed by Clifford and Ausloos and by Dalla Corte.1037 Clifford and Ausloos claim that ‘control constitutes the essence of the right to data protection. “Control” here - they argue - should be interpreted broadly and not simply as an individual’s “control” over their personal data but

---

1034 Lenaerts (2019), pp. 785, 792. Brkan proposes a second prong to this test, namely that to establish whether there is an interference with the essence of a fundamental right it is also necessary to evaluate whether there is an overriding public interest that can justify such interference. As long as there exists such an interest, the CJEU should engage in proportionality assessment and rule out the breach of essence of the fundamental right at issue. Brkan (2019), p. 869.

1035 Lenaerts (2019), pp. 785, 792.

1036 Ibid. See also Brkan (2019), pp. 877-878 (arguing that in EU-Canada PNR Opinion the CJEU ‘adopts a position that the interference with the essence of the right to privacy is a question of a degree of interference with the fundamental right, given that it takes as a benchmark the limited nature of the acquired and processed data.’)

1037 Porcedda also extensively discusses the essence of the fundamental right to data protection in her work. See, e.g., Porcedda (2018). Her proposal to defining the essence of the fundamental right to the protection of personal data by using the concept of ‘attributes’ of the right is less helpful for the purposes of analysis in this Section as she does not touch upon the rules on transfers of personal data outside the EEA.
as a robust architecture of control that actively pursues individual autonomy.\textsuperscript{1038} In arriving at such a conclusion, they emphasise the flexibility of the notion of ‘respect’ in Article 52(1) of the EU Charter in the protection of the essence of a right.\textsuperscript{1039} In other words, it seems that, in these authors’ view, the requirement of ‘respect’ allows a filtering out of the most appalling interferences with the right. Once the threshold of ‘respect’ is passed, interferences with the ‘essence’ of the rights are subject to a balancing test under the second sentence of Article 52(1) of the EU Charter. The checks and balances effectuating control as the essence of all fundamental rights and freedoms under the EU Charter (and not only the right to the protection of personal data), they argue, play a role at the level of the secondary framework, such as the GDPR.\textsuperscript{1040}

Dalla Corte contends that the value of the fundamental right to data protection (as opposed to the right to privacy and other rights implicated by data processing), is ‘in the very existence of a system of rules and norms applying to the processing of personal data, regardless of its connection with concepts like privacy, or the secrecy and confidentiality of the information processed.’\textsuperscript{1041} In other words, from his perspective, the fundamental right to the protection of personal data is ‘our fundamental “right to a rule” regulating personal data processing’.\textsuperscript{1042} Thus, ‘[a] violation of the essence of the right to data protection would … exist in cases where the interference with the right challenges, explicitly or implicitly, the very societal choice of having an omnibus regime regulating the processing of personal data.’\textsuperscript{1043} It ‘endangers … the very functioning and legitimacy of the collective posture towards personal data processing in its entirety, and hence ultimately its deepest roots: the rule of law and the democratic legitimacy of EU regulation.’\textsuperscript{1044} In this context, it is also worth recalling that, in a line of cases, the CJEU established that the objective pursued by the EU secondary data protection law (and, in particular, the Data Protection Directive) is to ensure ‘effective and complete’ protection of individuals.\textsuperscript{1045}

Applying the – in a way similar – approaches to the essence of the right to the protection of personal data proposed by these authors, one could conclude that in relation to the governance of transfers of personal data outside the EEA, the very presence of the

\textsuperscript{1038} Clifford, Ausloos (2018), pp. 144-145 (emphasis added). These authors also argue – as opposed to what has been discussed above - that the essence of the right to data protection can be limited, provided that ‘effective balancing mechanisms are in place as specified in Articles 8(2) and 8(3) of the Charter’.

\textsuperscript{1039} Ibid., p. 145.

\textsuperscript{1040} Ibid., p. 152.


\textsuperscript{1042} Ibid., p. 53.

\textsuperscript{1043} Ibid., p. 51-52.

\textsuperscript{1044} Ibid., p. 53.

\textsuperscript{1045} CJEU, Google Spain, para 34; CJEU, Wirtschaftsakademie, para 28; CJEU, Jehovan todistajat, para. 66; CJEU, Fashion ID, paras. 66, 70.
restrictions (in general) on transfers of personal data outside the EEA constitutes a part of the essence of the right to the protection of personal data, as their complete absence would strip this fundamental right, and the system of checks and balances instantiating it in secondary law, of their meaning and content. This is because, in the absence of any restrictions on transfers of personal data, the entire EU legal framework governing the processing of personal data could be easily circumvented. It is the prevention of this circumvention, as has been shown above, that constitutes the very constitutional function of such restrictions. In a similar vein, restrictions on onward transfers of personal data from the first country of destination outside the EEA to other countries outside the EEA are equally essential in performing this function and, therefore, should also be considered a part of the essence of the fundamental right to protection of personal data. At the same time, the particular design of restrictions on transfers and onward transfers of personal data, apart from the rules identified in Section 5.2.5 above, is a matter of strict necessity and proportionality balancing.

To sum up, this Section has argued that there is a dynamic relationship between EU primary and secondary data protection law. ‘Essential equivalence’ is the constitutional benchmark for strict necessity and proportionality balancing in the design and application of rules on cross-border transfers. The essence of the fundamental rights to privacy, protection of personal data and judicial remedy will be respected – based on state of the art of CJEU case law and academic literature – when secondary data protection law meets all of the following conditions:

- provides for some limitations on transfers of personal data outside the EEA and on onward transfers,
- contains safeguards preventing generalised access of foreign authorities to the content of electronic communications,
- ensures that purposes for processing personal data are limited,
- requires that the processing of personal data is accompanied by rules designed to ensure, inter alia, the security, confidentiality and integrity of the data, and also to protect them against unlawful access and processing,
- does not permit retention of the content of communications, and
- provides for some possibility for an individual to pursue legal remedies in order to have access to personal data relating to him or her, or to obtain the rectification or erasure of such data.

5.3 Weaknesses of the EU’s framework for transfers of personal data from the EU Charter perspective

The previous Section has argued that the EU secondary law framework for transfers of personal data outside the EEA under Chapter V of the GDPR can and should be
evaluated for compliance with the EU primary law envisaged in the EU Charter. This Section conducts such an evaluation in the light of the constitutional function of this framework to prevent circumvention of the EU data protection framework and, ultimately, to ensure that the aim of the EU secondary data protection legislation – ‘effective and complete’ protection of fundamental rights in the course of processing personal data – is not undermined. This evaluation is conducted against the backdrop of ever-changing political, geopolitical and economic circumstances, which contrasts with the comparatively static nature of the EU secondary law framework for transfers of personal data outside the EEA. The discussion in this Section presumes, and does not question, the fact that the current GDPR rules respect the essence of the fundamental rights to privacy, the protection of personal data and judicial remedy and meets the strict necessity and proportionality tests under Article 52(1) of the EU Charter. The starting point for the analysis is that the rules on transfers of personal data in Chapter V of the GDPR may not be the most fit for the constitutional purpose of the framework.

As already explained in this thesis, the EU framework for transfers of personal data outside the EEA was designed in early 1990s and first introduced by the 1995 Data Protection Directive. The GDPR changed the particularities of the framework by adding some flexibilities, but it did not alter its core structure. For the reader’s convenience, this Section briefly reiterates the structure of the EU’s framework for transfers of personal data outside the EEA. As discussed in Section 2.2.1.3, just like the Data Protection Directive, the GDPR, as interpreted by the EDPB, adopts a layered approach to transfers of personal data, where each of the subsequent layers is subsidiary to the one above it. The first layer is an adequacy decision by the European Commission establishing that a third country’s legal framework – both in general and in relation to the protection of personal data – is ‘essentially equivalent’ to that of the EU. Personal data can flow freely to a third country that has been afforded an adequacy decision, as if it is being processed within the EEA. The second layer of mechanisms for transfers of personal data, which apply in the absence of an adequacy decision, is the ‘appropriate safeguards’ put in place by the data controller or possessor (such as standard contractual clauses (SCCs), binding corporate rules (BCRs), certification, or codes of conduct). Data exporters and data importers must include the model SCCs, approved by the European Commission, verbatim into their agreements involving transfers of personal data. BCRs are codes of conduct regulating the processing of personal data by a group of undertakings or group of

1046 Kuner questions, however, whether this is still the case following the CJEU Schrems II judgement. Kuner (2020b).
1047 Art. 45 GDPR; CJEU, Schrems I, para. 73.
1048 Arts. 46-47 GDPR.
1049 Recital 81, Art. 46(2)(c) GDPR.
enterprises engaged in a joint economic activity. As clarified by the CJEU in *Schrems II*, when using appropriate safeguards for transfers of personal data to third countries that have not been afforded an adequacy decision, data exporters and importers must conduct a comprehensive case-by-case assessment of whether the use of such safeguards will ensure *in practice* a level of personal data protection ‘essentially equivalent’ to that in the EU. In exceptional circumstances, exporters of personal data may resort to the third layer of data transfer mechanisms – limited derogations under Article 49 GDPR (such as unambiguous consent of the data subject or the performance or conclusion of a contract with or in the interest of the data subject). The derogations may only be used for non-repetitive and occasional transfers, however. The layered approach requires that before using any of the derogations data exporters should first ‘endeavour possibilities to frame the transfer’ with one of the appropriate safeguards.

Between 1995, when the Data Protection Directive was adopted, and 2016, the year of adoption of the GDPR, at least three changes occurred, and they are crucial for the discussion in this Section. First, as mentioned in Chapter 2, the rights to the protection of privacy and personal data became binding fundamental rights in the EU. Second, following the Edward Snowden revelations, access to personal data transferred outside the EEA in a commercial context by the public authorities of a third country, and the availability of judicial redress against such authorities, became the most contentious issue in assessing the essential equivalence of third countries’ legal systems. Not only for the purposes of affording adequacy decisions under the GDPR but, in general, for the EU framework for transfers of personal data outside the EEA. Recall, that in the aftermath of those revelations, in its 2015 *Schrems I* judgement, the CJEU invalidated the EU-US Safe Harbor framework for transfers of personal data from the EU to the US. *Schrems I* marked a watershed in the history of transfers of personal data. Five years later, in its *Schrems II* judgement the CJEU invalidated the Safe Harbor’s successor – the EU-US Privacy Shield – on similar grounds. Furthermore, as explained above, the court expanded the application of the ‘essential equivalence’ standard to all mechanisms for

---

1050 Art. 47 GDPR.
1051 For a discussion, see Section 5.3.1.
1052 Art. 49 GDPR.
1054 Ibid., at 4.
1055 See Section 2.2.1.1.
1057 Article 29 Working Party, Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees), WP 237, 13 April 2016, pp. 1, 6.
1058 CJEU, *Schrems I*.
systematic personal data transfers under the GDPR. The third and final change is that the last 25 years have seen an exponential growth of cross-border commerce powered by personal and other data. The importance of data flows for pan-European and global trade form an integral part of the EU’s economic digital trade discourse advanced in parallel and, at times, contrary to the fundamental rights discourse. The ubiquitous character of data flows in digital commerce and online activities has further intensified global economic interdependence. It puts insurmountable pressure on the legal framework setting boundaries for the flows of personal data.

The changes introduced into the EU’s framework for transfers of personal data in the GDPR, as compared to the Data Protection Directive, addressed some of the political, legal and economic changes identified above. Indeed, several recitals of the GDPR acknowledge the challenges for the data protection regime brought by technological developments and globalisation. In its 2017 Communication ‘Exchanging and Protecting Personal Data in a Globalised World’, the European Commission praised the GDPR for providing ‘a diverse set of mechanisms that are flexible enough to adapt to a variety of different transfer situations’, citing notably the SCCs, the codes of conduct and certification mechanisms. Indeed, as compared to the Data Protection Directive, the GDPR’s transfer mechanisms are somewhat more flexible. For example, the GDPR allows for the adoption of an adequacy decision not only to a third country overall, but also to an international organisation, a territory or one or more specified sectors within that third country. In addition, the GDPR has explicitly codified the BCRs – which were applied in practice, but were merely implied in the text of the Directive – as one of the appropriate safeguards for transfers of personal data. The GDPR also added two new appropriate safeguards, namely certification and codes of conduct, which, at the time of writing, have not yet been operationalised. Finally, the specific derogations allowed under Article 49 of the GDPR were complemented by an open-ended, but extremely hard to comply with, safeguard allowing the transfer of personal data for the purposes of compelling legitimate interests of the data controller.

---

1060 For a discussion, see Section 5.2.2.
1061 See Introduction to this thesis.
1062 See Section 3.3.2.
1063 Recitals 5-7 GDPR.
1065 Compare Art. 25(1) Data Protection Directive and Art. 45(1) GDPR. Note, however, that two adequacy decisions under the Directive (namely, Adequacy decision for Canada, EU-U.S. Safe Harbor), despite absence of a direct mentioning of the possibility to adopt and adequacy decision for a specific sector the text of the Data Protection Directive, were adopted solely for commercial sector transfers.
1066 Article 46(2)(e) and (f) GDPR.
On a more critical note, more than four years after the adoption of the GDPR, few of these flexibilities have ever been used or operationalised. To wit: no adequacy decisions have been adopted for international organisations, territories or sectors of economy; only one adequacy decision for a third country (Japan) has been adopted under the GDPR; certification mechanisms and codes of conducts are not yet used as mechanisms for data transfers; and the SCCs for controller to controller and controller to processor transfers, adopted by the European Commission in 2004 and 2010 respectively, have not been updated to meet the GDPR standard and the demands of business. In practice, most of the systematic transfers of personal data outside the EEA still rely on the SCCs. This raises the question of whether the above-mentioned flexibilities are merely paying lip service to the EU’s economic discourse on digital trade, as discussed in Chapter 3 of this thesis, rather than a genuine effort to reform the framework for transfers of personal data.

This Section argues that, although the framework did – on paper - become more flexible, these changes did not rectify the key structural issues inherent within it. Against the backdrop of the three developments mentioned at the beginning of this Section, the discussion below is centred around the three principal deficiencies of the EU’s framework under Chapter V of the GDPR. First, although the CJEU’s Schrems II judgement contributed to bridging the qualitative gap between adequacy decisions and private law mechanisms for systematic transfers of personal data, it did not eliminate the problem completely. Although it is too early to judge, this Section contemplates that Schrems II may instead lead to other problems, such as the fragmentation of standards for transfers of personal data across the EU due to: (a) the deficiencies of coordination between European DPAs; (b) limitations of enforcement resources of European DPAs and a resulting shift towards private enforcement; which will, in turn result in (c) a fragmentation of case law across the EU member states in the short and medium terms. It also argues that, overall, in the future the secondary EU framework for transfers of personal data may not be the right tool to address the surveillance issue in transfers of personal data outside the EEA. Second, in practice, the adequacy decisions themselves, including the most recent one for Japan adopted on the basis of the GDPR, suffer from a number of weaknesses which impair their

---

1067 See Kuner (2020c).
1069 IAPP-EY (2019), p. 110 (showing that in 2019 (i.e. prior to the CJEU Schrems II judgement) 88% of personal data transfers from the EU to the US are based on the SCCs.)
ability to ensure, in practice, continuity of personal data protection as required by their constitutional function. Third, there is a mismatch between the transformation of the role of personal data in cross-border commerce since 1995, when the core of the EU framework for transfers of personal data was designed, on the one hand, and the rigidity of this framework in the sense that it does not take into account the different degree of risks to fundamental rights inherent in transfers of personal data in different circumstances, on the other hand. The Section therefore contends that the rules of Chapter V of the GDPR lack scalability and are thus not fully adequate for the digital age. The discussion below elaborates on each of these arguments.

5.3.1 The foreign surveillance issue after Schrems II

The interpretation of ‘adequacy’ of personal data protection as ‘essential equivalence’ by the CJEU in Schrems I created a qualitative gap between the level of protection that, in theory, is given to personal data transferred on the basis of adequacy decisions, on the one hand, and the level of protection afforded to personal data transferred on the basis of so-called ‘appropriate safeguards’, on the other hand. The CJEU’s conclusions and the ensuing guidance by the European DPAs, as well as the above-mentioned qualitative gap – were later codified in the GDPR. As compared to Article 25(2) of the Data Protection Directive, the list of factors set forth in Article 45(2) of the GDPR (that the European Commission must consider when assessing the adequacy of the level of protection of personal data in a third country) has been sufficiently expanded. In particular, it requires the Commission to evaluate the access of public authorities to personal data, as well as the implementation of the foreign legislation to see whether it contains effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred. By strengthening the adequacy assessment, however, the GDPR inadvertently created a situation where the level of personal data protection achieved by all other mechanisms for data transfers (most importantly, appropriate safeguards under Article 46 GDPR, which on a par with adequacy, can underlie systematic transfers of personal data) became lower than that afforded (in theory) by an adequacy decision.

Adequacy decisions are adopted by implementing acts of the Commission after a thorough assessment of the third country’s legal system and data protection framework. The adequacy decision for Japan, which is the most recent – and so far, the only adequacy decision adopted under the GDPR, – contains commitments by Japan in relation to personal

1070 Article 29 Working Party, Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees), WP 237, 13 April 2016.
1071 Art. 45(2)(a) GDPR.
data transferred from the EEA. These commitments are included in the ‘Supplementary Rules under the Act on the Protection of Personal Information for the Handling of Personal Data Transferred from the EU based on an Adequacy Decision’, hereinafter referred to as the ‘Supplementary Rules’, which are legally binding for Japanese businesses. In contrast, the appropriate safeguards and specific derogations are merely private law mechanisms. An adequacy decision certifies (in theory) that a particular third country ensures a level of personal data protection ‘essentially equivalent’ to that in the EU. The ‘level of personal data protection’ means here not only the quality of the data protection rules, but multiple other factors, including the respect for the rule of law and human rights, access of public authorities to personal data, existence and effective functioning of independent supervisory authorities, existence of effective judicial review designed to ensure compliance with provisions of EU law. None of the other mechanisms for data transfers required – until the Schrems II judgement – such a thorough assessment. Most specifically, these mechanisms as described in the GDPR, did not seem to provide individuals with any safeguards against the access to their data by third country’s public authorities. After the CJEU’s invalidation of the Safe Harbor framework in Schrems I in 2015, Kuner rightly noted that:

> [t]he conclusions of the CJEU in Schrems have thus undermined the logical consistency of using adequate safeguards to transfer personal data. The European Commission and the DPAs have allowed standard contractual clauses and BCRs to be used for years although it has been clear that they cannot provide effective protection against intelligence surveillance, suggesting that until now they have implicitly factored the possibility of such surveillance into the definition of “adequate safeguards.” The strict standard for data protection rights applied by the CJEU in Schrems judgments raises the question of whether this is compatible with EU fundamental rights law.

It is precisely this deficiency of private law mechanisms for transfers of personal data that led to a challenge of the validity of the European Commission’s Decision approving the SCCs, along with the EU-US Privacy Shield, in the light of the EU Charter, which resulted in the CJEU’s 2020 Schrems II judgement. In particular, in the judgement of

---

1072 Annex 1 to Adequacy decision for Japan.
1073 CJEU, Schrems I, para. 73.
1074 Art. 45 GDPR; CJEU, Schrems I, paras. 91-96; Article 29 Working Party, Working document on Adequacy Referential, WP 254rev.01, 6 February 2018, Chapter 4.
1076 CJEU, Schrems II, referred to the CJEU by Irish High Court (Commercial), The Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems 2016 No. 4809 P., 3 October 2017.
the Irish High Court referring the case to the CJEU, Justice Costello argued that neither the ‘Privacy Shield’ nor the SCCs are sufficient to protect the fundamental rights that apply to personal data in the EU Charter. In particular, they limit the right to an effective remedy before an independent tribunal guaranteed by Article 47 of the EU Charter beyond the limits set by Article 52(1) of the EU Charter. Justice Costello also noted that ‘[i]f there are inadequacies in the laws [of the foreign country] within the meaning of Union law, the SCCs cannot and do not remedy or compensate for these inadequacies’.

As has already been mentioned above, in Schrems II, the CJEU reinstated the logical consistency of the EU framework for data transfers. Despite running the risk of being repetitive, for the purposes of discussion below it is important to summarise all the CJEU’s conclusions in relation to the validity of the SCCs and, indirectly, all other appropriate safeguards under Article 46 of the GDPR:

1. The requirement of ‘essential equivalence’ equally applies to all mechanisms for systematic transfers of personal data under the GDPR, including appropriate safeguards under Article 46 GDPR, also in the context of access to personal data by foreign authorities in a national surveillance context;

2. ‘Essential equivalence’ of the level of protection in third countries that have been afforded an adequacy decision is presumed;

3. The SCCs ‘are solely intended to provide contractual guarantees … independently of the level of protection guaranteed in each third country’, and are valid;

4. Prior to using the SCCs and other appropriate safeguards for third countries that have not been granted an adequacy decision, the data exporter must conduct a comprehensive assessment, in particular, on the basis of factors ‘set out, in a non-

---

1077 Irish High Court (Commercial), The Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems 2016 No. 4809 P., 3 October 2017, para. 334, stating that the limitations on the exercise of the right to an effective remedy before an independent tribunal, as required by Article 47 [of the EU Charter], for EU citizens whose data privacy rights are infringed by the intelligence agencies are not proportionate or necessary or needed to protect the rights and freedoms of others. Neither the introduction of the Privacy Shield Ombudsperson mechanism nor the provisions of Article 4 of the SCC decisions eliminate the well-founded concerns raised by the [Irish Data Protection Commissioner] in relation to the adequacy of the protection afforded to EU data subjects whose personal data is wrongfully interfered with by the intelligence services of the United States once their personal data has been transferred for processing to the United States.

1078 CJEU, Schrems II, para. 154.

1079 Kuner (2020d).

1080 CJEU, Schrems II, para 96, 105; see also Opinion AG in Schrems II, para. 117. See also EDPB, Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 - Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems, 23 July 2020, questions 6 and 7.

1081 CJEU, Schrems II, para. 118.

1082 Ibid., para. 133.

1083 Ibid., paras. 136, 147. See also Opinion AG in Schrems II, para.126.
exhaustive manner, in Article 45(2) [GDPR]’ of whether those safeguards can, in practice, ensure essentially equivalent protection of personal data (so-called ‘mini-adequacy’ assessments);\(^\text{1085}\)

5. If, based on the assessment above, the data exporter concludes that an ‘essentially equivalent’ level of data protection cannot be ensured by appropriate safeguards, the data exporter must implement what the CJEU calls ‘additional safeguards’ or ‘supplementary measures’, which should be determined on a case-by-case basis;\(^\text{1086}\)

6. If the data exporter established in the EU is not able to take ‘additional measures’ to guarantee ‘essentially equivalent’ protection of personal data, the data exporter must suspend or end the transfer; this is, in particular, the case where the law of the third country imposes obligations on the recipient of personal data, which are contrary to the SCCs;\(^\text{1087}\)

7. The DPAs must proactively monitor transfers of personal data under appropriate safeguards and suspend or prohibit data transfers that do not meet the requirement of ‘essential equivalence’;\(^\text{1088}\) and

8. To prevent the fragmentation of rules, which could result from different EU member states’ DPAs arriving at different conclusions regarding lawfulness of transfers, the DPAs must work together through coordination mechanisms under the GDPR.\(^\text{1089}\)

On the face of it, the CJEU closed the qualitative gap between adequacy decisions and appropriate safeguards under Article 46 GDPR, while preserving the lawfulness of the most commonly used mechanism for data transfers in the absence of an adequacy decision.\(^\text{1090}\) The way the CJEU answered the questions referred to it in Schrems II is, indeed, perhaps, the only logical way the Court could restore the consistency of the EU secondary law framework for transfers of personal data and assert the importance of fundamental rights vis-à-vis the economic interests embedded in data transfers, on the one hand, and without upsetting the delicate institutional balance in the EU, on the other hand. If the CJEU invalidated the SCCs as a mechanism for transfers of personal data, this would undermine the validity of all other private law mechanisms in the GDPR. Not only the BCRs but also the certification mechanisms and codes of conduct added into the GDPR,

---

\(^{1084}\) Ibid., para. 105.

\(^{1085}\) Ibid (2020d).

\(^{1086}\) CJEU, Schrems II, paras. 131-134, 137, 142.

\(^{1087}\) Ibid., para. 135.

\(^{1088}\) Ibid., paras. 108, 121.

\(^{1089}\) Ibid., para. 147.

\(^{1090}\) IAPP-EY (2019), p. 110 (showing that in 2019 (i.e. prior to the CJEU Schrems II judgement) 88% of personal data transfers from the EU to the US are based on the SCCs.)

\(^{1091}\) See Kuner (2020d); Christakis (2020).
which the European Commission frequently emphasises as bringing extra flexibility to the modernised ‘toolbox’ for data transfers.\textsuperscript{1092} Such a state of affairs would also undermine the system of cross-border transfers in the GDPR as a whole.\textsuperscript{1093} Thus, this approach would create – \textit{de jure} – data localisation in respect of all countries, short of 12 afforded adequacy decisions, which would be contrary to the EU’s external digital trade policy and digital trade discourse (discussed in Chapters 3 and 4 above). Specific derogations under Article 49 GDPR, which were not considered in Schrems II, can only be used for occasional and non-repetitive transfers.\textsuperscript{1094} Neither could the CJEU invalidate the model SCCs approved by the European Commission: as the CJEU demonstrated itself, they do provide the safeguards required under Article 45(2) of the GDPR, provided that a third country’s legal framework does not interfere with their application.\textsuperscript{1095}

The CJEU also did not use the window of opportunity – opened by the Advocate General’s opinion – to modify its position in Schrems I and apply a lower threshold for situations where foreign authorities’ access transferred personal data for national security purposes, thus amplifying the tension between the CJEU’s approach to national security measures interfering with fundamental rights abroad and in the EU member states.\textsuperscript{1096} In particular, the Advocate General had noted that:

‘essential equivalence’ test should therefore … be applied in such a way as to preserve a certain flexibility in order to take the various legal and cultural traditions into account. That test implies, however, if it is not to be deprived of its substance, that certain minimum safeguards and general requirements for the protection of fundamental rights that follow from the Charter and the ECHR have an equivalent in the legal order of the third country of destination.\textsuperscript{1097}

Thus, the Advocate General had argued that both the standards of the Charter and the ECHR are the relevant comparators for the assessment of the foreign legal framework. He had also observed that ‘the standards resulting from Articles 7, 8 and 47 of the Charter, as interpreted by [the CJEU], are in certain respects stricter than those arising under Article 8 of the ECHR according to the interpretation of those provisions by the European Court of


\textsuperscript{1093} For a discussion of this scenario, see Swire (2016), pp. 1-33 – 1-36.


\textsuperscript{1095} CJEU, \textit{Schrems II}, paras. 126-148.

\textsuperscript{1096} See Section 2.2.2.

\textsuperscript{1097} Opinion AG in \textit{Schrems II}, para. 249.
Human Rights (“the ECtHR”). The ECtHR may, however, reconsider its approach in several pending cases.

In practice, the CJEU pushed the foreign surveillance problem in the context of personal data transfers further down the line. As argued in Chapter 2, the Schrems II has restricted the possibility of using the SCCs in practice, especially in the light of some of the DPAs recommending European companies to localise data where possible. Furthermore, and most importantly, it is questionable whether the Schrems II approach will allow a bridge to be built between the qualitative gap between the adequacy assessments and appropriate safeguards under Article 46 for several reasons. It is unclear whether companies are in the right position to conduct assessments of the third country’s legal regime similar to adequacy assessments, which the European Commission typically conducts for several years and which, even then, do not always result in bullet-proof adequacy decisions as this Section illuminates below. Many companies, especially small and medium enterprises, will have neither the resources nor the expertise to conduct comprehensive research into third countries’ legal frameworks. Companies that could have both the resources and expertise to do so, do not seem to have complied with the Schrems II requirements in a timely manner. Even more importantly, the CJEU’s approach gives companies – the very actors which ‘encroach upon the private sphere’ – a crucial role in setting the boundaries for data transfers and resulting interference with fundamental rights.

While companies are driven by their bottom-lines, it is the role of governments and European institutions to ensure that fundamental rights are protected. It is also questionable whether the lack of ‘essential equivalence’ can be remedied by additional guarantees that companies must implement in order to continue data transfers. Thus, on the one hand, it is clear, that many countries in the world do not meet the ‘essential equivalence’ standard as formulated by the CJEU. On the other hand, it is similarly clear that additional private law guarantees cannot remedy those deficiencies. In the present-day interconnected world, data flows will not simply stop and in practice (in the view of low risk of enforcement by DPAs), many companies are likely to continue with ‘business as usual’. As a result, the level of compliance and the quality of assessment are unlikely to be satisfactory.

---

1098 Ibid., para. 251.
1099 Ibid., para. 252.
1100 See Section 2.2.2.
1101 As of October 2020, big companies like Microsoft, have not adjusted their practices to comply with Schrems II. See, e.g., Unabhängiges Datenschutz Zentrum Saarland, Pressemitteilung: Microsoft Office 365: Bewertung der Datenschutz-Konferenz zu undifferenziert – Nachbesserungen gleichwohl geboten, 02 October 2020.
1102 For a discussion on why giving companies too much power in setting the boundaries for data processing could be a problem, see Quelle (2017a).
Furthermore, it is questionable whether the DPAs themselves are well situated to assess the adequacy of legal frameworks in third countries and monitor compliance with the new rules, given the pervasiveness of data flows and the lack of financial and human resources. The reluctance of the Irish DPA to take a firm action against Facebook’s transfers to the US back in 2013, which resulted in Schrems I and II in the first place, and its reluctance to actively enforce the Schrems II judgement, is telling. Thus, although in Schrems II the CJEU restored the coherence of the framework for transfers of personal data, it did not close the gap between the ‘reality and illusion’ of personal data protection in the context of data transfers.

While it has put the DPAs at centre stage for ensuring the lawfulness of transfers, the CJEU has explicitly dismissed the risk of divergent decisions by the EU DPAs to suspend or prohibit transfers by referring to coordination mechanisms within the EDPB under the GDPR. This coordination mechanism, however, has not been effective until now, in part due to differences in administrative procedures in EU member states. While DPAs and the EDPB are crafting guidelines on additional safeguards that companies can implement to ensure the SCCs guarantee ‘essentially equivalent’ protection in practice, private lawsuits, including mass claims, may well take over as the primary mode of enforcement. The relatively new possibilities for mass damages claims under Articles 80 and 82 of the GDPR and EU member states' laws are becoming increasingly attractive for NGOs and professional litigation funders. The GDPR provisions allow a not-for-profit body, organisation or association that has been mandated by an individual – in some EU member states, this mandate is not needed – and meets certain requirements, to exercise individual rights to judicial remedy, including an ability to claim compensation.

In response to the inaction of Irish and other DPAs following the Schrems II judgement, noyb, the NGO run by Max Schrems, has recently filed 101 complaints to various European

---

1103 According to the EDPB’s survey, as of 2019, more than 50% of EU member states DPAs have less than 60 FTE and budget below EUR 4.5 million. EDPB, Contribution of the EDPB to the evaluation of the GDPR under Article 97, Adopted on 18 February 2020, pp. 26-30. See also BEUC (2020).
1104 Noyb (2020b).
1105 Kuner (2017), discussing the ‘reality and illusion’ in EU personal data transfer regulation post Schrems I.
1106 CJEU, Schrems II, para. 147.
1107 See EDPB, Contribution of the EDPB to the evaluation of the GDPR under Article 97, Adopted on 18 February 2020, p. 3; Communication from the Commission, Data Protection Rules as a Pillar of Citizens Empowerment and EU’s Approach to Digital Transition - Two Years of Application of the General Data Protection Regulation, COM(2020) 264 final, 24 June 2020, p. 5 (noting that ‘developing a truly common European data protection culture between data protection authorities is still an on-going process. Data protection authorities have not yet made full use of the tools the GDPR provides, such as joint operations that could lead to joint investigations.’)
1108 See, e.g., Manancourt (2020). See also The Privacy Collective (2020), para. 4.6.5 (in Dutch).
1109 For an overview of collective damage compensation systems for data protection violations in different EU member states, see Pato (2019a); Pato (2019b), p. 98ff.
Noyb also stated that it ‘is planning to gradually increase the pressure on EU and US companies to review their data transfer arrangements and adapt to the clear ruling by the [CJEU]’, hinting at the imminence of private enforcement. Sooner or later, domestic courts will need to evaluate whether transfers to certain jurisdictions meet the Schrems II requirements and which additional measures are appropriate in specific circumstances. This may, as alluded to above, result in a fragmentation of the case law throughout the EU in the short and medium term, and in more references to the CJEU in the long term.

Despite this critique, it is undeniable that the Schrems II judgement marks an important milestone in asserting the fundamental rights to privacy and the protection of personal data in the context of digital trade. The fact that the CJEU put the burden on private companies and the DPAs, should be taken as an intermediary solution: the lesser of two evils, the other being the prohibition of systematic data transfers on the basis of appropriate safeguards. It is a wake-up call to the EU and its trading partners to start a dialogue on the interplay between digital trade, fundamental rights and national security. The core issue raised in Schrems I and II cannot be fully addressed by businesses, DPAs or even the EU secondary rules, such as the GDPR or the adequacy decisions. As rightly noted by several commentators in relation to the invalidation of the EU-US Privacy Shield and the standards the EU Charter requires from foreign legal frameworks, ‘any hope of a stable and viable accommodation for data transfers between the EU and the US can only be based on changes to US law’. This is also true for other third countries: as discussed in the following Section, few of the existing adequacy decisions can meet the high threshold of essential equivalence set by the CJEU in Schrems I and confirmed in Schrems II judgements.

In a global – or, at a minimum, multilateral setting – reconciling the policy objectives of digital trade, national security and fundamental rights is an intricate political challenge. As Farrell and Newman demonstrate, global economic interdependence and seamless data flows have been ‘weaponised’ by surveillance authorities that leveraged global networks for surveillance purposes (authors call this phenomenon ‘weaponized interdependence’). Schrems II, they argue, is an opportunity to address this changed relationship between national security and civil liberties by democratic states, and primarily by the US and the EU. Arguably, putting the burden on companies to assess
essential equivalence of third countries’ legal frameworks and hoping for companies operating in legal regimes with insufficient privacy protection to push their governments to change this regime – a bottom-up change – has not worked in the past and, if the past is prologue, will not work in the future. Addressing the issue at the international level is much more in line with the EU’s ambition to ‘promote convergence of data protection standards at international level, as a way to facilitate data flows and thus trade’.  

What the optimal forum for addressing this issue should be is a broader question, one which is outside the scope of this thesis. At this stage, one could, however, argue that this dialogue should not be part of international trade negotiations. As noted several times throughout this thesis, privacy and data protection as well as national security interests are built into the international trading system as exceptions. The economic ethos of the international trading system, as argued in Chapter 3, could lead to a lower level of fundamental rights protection. Furthermore, this would be against the current EU approach to digital trade negotiations discussed in Chapter 4.

5.3.2 Inadequacies of adequacy decisions

This Section argues that, although – based on the criteria for assessment in Article 45(2) of the GDPR – adequacy decisions, in theory, must ensure an essentially equivalent level of protection, in practice this mechanism for data transfers not only suffers from political pressures, which result in assessment less rigorous than required by Article 52(1) of the EU Charter, but also from the problems inherent in any domestic legal instrument with extraterritorial reach, namely, the ‘snapshot’, the ‘heavy burden’ and the ‘onward transfer’ problems. As a result, as Kuner argues, ‘while adequacy purports to provide a strong level of protection for personal data, such protection is actually difficult to enforce outside the borders of the EU.’

The flaws of adequacy decisions discussed in this Section suggest that the adequacy framework does not fully prevent, in practice, the circumvention of the EU data protection framework when personal data leaves the EEA borders and does not fulfil the function of securing ‘effective and complete’ protection of the fundamental rights to the protection of privacy and personal data in the EU.

5.3.2.1 Adequacy decisions: between protection of fundamental rights and trade politics

Despite being the primary mechanism for transfers of personal data outside the EEA in the layered structure of the EU legal framework, the adequacy assessments mechanism

1117 Cf Irion (2020a), But see Reidenberg (2001), pp. 739, 748 proposing to negotiate a ‘General Agreement on Information Privacy’ at the WTO. 
1118 Kuner (2009), pp. 8-9.
lacks a clear procedure and is extremely slow. From 1995 when the adequacy mechanism was first introduced, the EU has granted adequacy only 14 times. EU Commission’s adequacy decisions were challenged twice at the CJEU, both times for the US, and both challenges resulted in the invalidation of the decisions.\textsuperscript{1119} It takes on average several years to obtain adequacy.\textsuperscript{1120}

The adequacy mechanism is a powerful negotiation tool between the EU and its trading partners.\textsuperscript{1121} For example, in its 2017 Communication, the European Commission stated that it will ‘actively engage with key trading partners in East and South-East Asia’, starting with Japan and Korea in 2017 and, depending on progress towards the modernisation of its data protection laws, with India, but also with countries in Latin America (in particular Mercosur members), and countries in the ‘the European neighbourhood’ that have expressed an interest in obtaining an ‘adequacy finding’.\textsuperscript{1122} Several leading scholars have argued that adequacy decisions are not strict legal assessments.\textsuperscript{1123} For example, Schwartz contends that in evaluating adequacy ‘the EU has demonstrated a wide range of flexible approaches with regard to this standard.’\textsuperscript{1124} Although under the GDPR, adequacy is a unilateral assessment, the EU negotiators have not ‘exercised unilateral power’, but rather ‘flexibly assessed the adequacy of different legal systems as it suits the EU’s goals at the time’.\textsuperscript{1125} Similarly, Kuner argues that ‘adequacy decisions are far from always being objective and logical, and do not provide a watertight standard of data protection’,\textsuperscript{1126} and that ‘[i]n practice, it can be difficult for a State or regional organization to pass judgment on a foreign regulatory system without political considerations playing some role’.\textsuperscript{1127} He illustrates his point by referring to the adequacy decision for Argentina, where serious human rights abuses were flagged by Amnesty International right after that decision was granted.\textsuperscript{1128} The assessment of Argentina’s adequacy by Article 29 Working Party was conducted ‘on the basis of … assumptions and explanations and in the absence of any substantial experience with the practical application of the legislation, both at federal or provincial level.’\textsuperscript{1129} In a similar

\begin{thebibliography}{99}
\bibitem{1119} CJEU, \textit{Schrems I} invalidated the EU-US Safe Harbor and CJEU, \textit{Schrems II} invalidated the EU-US Privacy Shield.
\bibitem{1120} Most recent example is Adequacy Decision for Japan.
\bibitem{1123} For a discussion, see Yakovleva, Irion (2016), p. 205.
\bibitem{1124} Schwartz (2019), p. 806.
\bibitem{1125} \textit{Ibid.}, p. 806-807.
\bibitem{1126} Kuner (2009), p. 8-9.
\bibitem{1127} Kuner (2013), p. 66.
\end{thebibliography}
vein, one of the factors that played a role in the assessment and finding of adequacy of New Zealand was the volume of EU’s trade with this country.\textsuperscript{1130} Concerns regarding the absence of onward transfer restrictions in New Zealand law was addressed by simply pointing out the remote geographical location of the country and low likelihood of such transfers.\textsuperscript{1131} The adequacy decision for Israel, despite Israeli intelligence agency practices, is yet another example of a political compromise in the assessment of adequacy.\textsuperscript{1132}

The recently invalidated EU-US Privacy Shield (which superseded the EU-US Safe Harbor, invalidated by the CJEU in 2015), was hastily negotiated and concluded in record time: 8 months as opposed to the ‘lengthy and troubled negotiations of the Safe Harbor’\textsuperscript{1133} and other adequacy decisions.\textsuperscript{1134} Political pressure from the US government and powerful transatlantic business stakeholders not only explains the faster pace of the negotiations, but also the fact that this adequacy decision for the US was adopted despite reservations from the Article 29 Working Party (the EDPB’s predecessor), the European Parliament and the EDPS.\textsuperscript{1135} It therefore comes as no great surprise that just like its predecessor, the Privacy Shield did not survive CJEU scrutiny.\textsuperscript{1136}

The adequacy decision for Japan is the most recent example of the same phenomenon. As mentioned in Chapter 4, trade negotiations with Japan played a significant role in granting Japan an adequacy decision, which indeed coincided with the conclusion of the bilateral trade agreement. Japan’s adequacy decision contains (besides the Commission’s assessment of Japan’s regulatory framework) additional rules that Japan agreed to implement specifically in relation to personal data transferred from the EEA, thus creating a double standard for personal data protection within the country.\textsuperscript{1137} As rightly mentioned by France in its submission for the 2020 review of the GDPR, the purpose of the adequacy decision is the assessment of an existing framework, not the creation of an

\textsuperscript{1131} Roth (2017), pp. 60-61.
\textsuperscript{1132} Kuner (2013), p. 66.
\textsuperscript{1133} House Hearing. (2001), p. 72.
\textsuperscript{1134} The EU-US Safe Harbor was invalidated in October 2015, the EU-US Privacy Shield was adopted on 12 July 2016.
\textsuperscript{1135} European Parliament Resolution of 26 May 2016 on transatlantic data flows (2016/2727(RSP)); EDPS, Opinion 4/2016 on the EU-U.S. Privacy Shield draft adequacy decision, 30 May 2016; Article 29 Working Party, Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision, WP 238, 13 April 2016.
\textsuperscript{1136} Farrell, Newman (2020a) (arguing that ‘no one—including the European Union officials who negotiated it—ever thought that the Privacy Shield agreement that succeeded Safe Harbor had much chance of surviving CJEU scrutiny.’) See also Christakis (2020); Kuner (2020d).
\textsuperscript{1137} Annex 1 to Adequacy decision for Japan. In its comments to the EU Council on the evaluation of the GDPR France calls this approach an ‘ingenious solution,’ which, nonetheless, ‘should not be considered as a precedent for future adequacy decisions’. Preparation of the Council position on the evaluation and review of the General Data Protection Regulation (GDPR): Comments from Member States, 12756/1/19 REV 1, submission of France, p. 24.
additional layer of rules specifically for the EEA data to rectify gaps in a foreign country’s legal system.\textsuperscript{1138} Thus, by adding Supplementary Rules to the adequacy decision, the European Commission has, in effect, re-designed the adequacy framework under the GDPR. Furthermore, the adequacy decision for Japan was adopted despite the concerns of the EDPB and the European Parliament regarding, in particular, the compliance of the surveillance measures employed by the Japanese government with the adequacy standard established by the CJEU in \textit{Schrems I}, and relatively mild enforcement mechanisms (compared to those under GDPR) under Japanese law.\textsuperscript{1139} Although the 2020 reform of Japan’s Act on the Protection of Personal Information brought it closer to the GDPR, it did not alter the provisions on administrative fines.\textsuperscript{1140} Not surprisingly, Greenleaf criticised the adequacy decision for Japan, which, in his words, ‘discounts’ the EU law’s adequacy standard on several grounds, most importantly in that (a) the Japanese enforcement regime is not ‘essentially equivalent’ to that of the EU; (b) consent cannot be a sufficient ground for onward transfers (this issue is further discussed in Section 5.3.2.2 below); and (c) there was a lack of expert involvement in the assessment of the Japanese legal system.\textsuperscript{1141}

The adequacy decision mechanism has been, and continues to be, a powerful tool for the EU to export its data protection standards and seek further convergence of other countries’ data protection rules on the basis of the EU standards (the above-mentioned ‘Brussels Effect’\textsuperscript{1142}). The political component, however, has an impact on the robustness of the adequacy decisions to safeguard an ‘essentially equivalent’ level of protection of personal data transferred outside the EEA. Although none of the adequacy decisions (except those for the US) have yet been challenged at the CJEU, it is questionable whether most of them – given that 10 out of 11 adequacy decisions in force were granted before the 2015 \textit{Schrems I} judgement – would stand the ‘essential equivalence’ test articulated by the CJEU in \textit{Schrems I} and recently confirmed in \textit{Schrems II} in respect to the access of foreign surveillance authorities to transferred data, and right to effective judicial remedy.\textsuperscript{1143} This problem of staticity of adequacy assessments and other limitations of the adequacy framework are discussed below.

\textsuperscript{1138} Preparation of the Council position on the evaluation and review of the General Data Protection Regulation (GDPR): Comments from Member States, 12756/1/19 REV 1, submission of France, p. 24.
\textsuperscript{1140} For an overview of amendments, see One Trust Data Guidance (2020b).
\textsuperscript{1141} Greenleaf (2018b); see also Greenleaf (2018c), pp. 4-8; Greenleaf (2017b).
\textsuperscript{1142} Bradford (2012).
\textsuperscript{1143} See Christakis (2020).
5.3.2.2 Limitations of adequacy decisions inherent in legal instruments with extraterritorial application

This Section argues that, as domestic legal instruments with extraterritorial reach, adequacy decisions suffer from at least three weaknesses. First, they embody an assessment of a third country’s legal framework at a particular point in time and do not provide effective dynamic mechanisms for ensuring that the third country will maintain the same level of personal data protection throughout the life of the adequacy decision (the ‘snapshot’ problem). Second, if a foreign data controller or processor violates the third country’s data protection rules when processing a European’s personal data, enforcement of such rights abroad is burdensome (the ‘heavy burden’ problem). Third, adequacy decisions, at best, guarantee that personal data transferred from the EEA are equally protected in the first country of destination — the one granted an adequacy decision — but often fail to provide the same level of protection in relation to onward transfers of such data to other countries (the ‘onward transfer’ problem).

On the first point (the ‘snapshot’ problem), as mentioned above an adequacy decision for a third country (international organisation, territory or sector of industry) is the result of an assessment of that country’s system based on a snapshot of rules at a particular point in time. The GDPR requires that the adequacy decision should provide for a periodic review, at least every four years. In a fast-paced globalised present-day environment, review of the legal framework once in four years is simply not frequent enough. In addition, the GDPR requires the Commission to monitor developments in third countries and international organisations that could affect the functioning of the adequacy decisions and may, to the extent necessary, repeal, amend or suspend such adequacy decisions. Although the Data Protection Directive did not contain specific rules on the monitoring and review of adequacy decisions, similar requirements were initially included in the text of adequacy decisions themselves. These requirements were later expanded to include the monitoring of the developments on foreign authorities’ access to personal data in the aftermath of the CJEU Schrems I judgement. There is, however, no information on whether and how, if at all, the Commission actually conducts the monitoring of legal regimes in third countries that have been afforded adequacy. Furthermore, none of the adequacy decisions – except for the invalidated EU-US Privacy Shield, which was the only

1144 Kuner (2015b), pp. 236, 239 (arguing that although the EU rules for transfers of personal data is not ‘extraterritorial in scope within a literal meaning of the term, they do have extraterritorial effect’.)
1145 For simplicity, this section refers to country only, but implies organisation, territory, and sector of industry.
1146 Art. 45(3) GDPR.
1147 Art. 45(4) and (5) GDPR.
1148 See, e.g., Art. 4 of Adequacy decision for Canada; Art. 4 Adequacy decision for Uruguay.
1149 European Commission, Implementing Decisions amending Adequacy Decisions after Schrems I.
adequacy mechanism reviewed on an annual basis—have ever been reviewed. Of the 11 adequacy decisions adopted prior to the GDPR, which are currently in force, some have been in force for nearly 20 years (for example, adequacy for Switzerland adopted in 2000, for Canada, in 2001). Neither the 2013 Snowden revelations, followed by European Parliament reports and calls on the Commission to review adequacy decisions for New Zealand and Canada because of these countries participation in the ‘Five Eyes’ programme, nor the 2015 Schrems I judgement, triggered a review of such adequacy decisions by the Commission. Similarly, the Commission did not take action to remedy the deficiencies of the Safe-Harbor, despite having identified its weaknesses in its 2013 Communications, preceding the Safe Harbor’s invalidation by the CJEU in Schrems I. What is more, already back in 2001, just one year after the Safe Harbor framework came into being, a leading US academic proclaimed Safe Harbor ‘only a weak, seriously flawed solution for e-commerce’.

The European Commission announced the first review of all adequacy decisions in 2017. This review is still ongoing at the time of writing. The publication of the report on the review of adequacy decisions was postponed until after Schrems II. The Commission has, however, already indicated that it is discussing ‘additional safeguards’ with some of the countries and territories ‘to address relevant differences in protection’. It remains to be seen whether this review will result in qualitative improvements of the adequacy decisions.

1151 See Committee on Civil Liberties, Justice and Home Affairs, Report on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs. No 2013/2188(INI), 21 February 2014; European Parliament Resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs (2013/2188(INI)). For a discussion see Roth (2017), p. 64. In the aftermath of Schrems I the European Commission amended adequacy decisions in force at that time to include provisions regarding the monitoring of developments in third countries regarding government agencies' access to personal data, the communication between the European Commission and EU member states, and between the European Commission and third countries on the issue. European Commission, Implementing Decisions amending Adequacy Decisions after Schrems I.
1154 International Association of Privacy Professionals. (2017). See also EDPB, Agenda of the 40th EDPB meeting, 20 October 2020, suggesting that the Adequacy decision for Japan is also being reviewed.
One way or the other, at this juncture it seems clear that adequacy decisions do not fully factor in developments in the third countries’ legal systems, and practice of application after adequacy has been granted. Besides, the EU has little or no control over the way personal data transferred from the EEA is processed abroad. One of the reasons why the review of adequacy decisions has not been an effective mechanism, is that, as discussed above, granting and maintaining an adequacy decision is not purely a legal matter, but largely a political act, especially when the EU’s trade interests are at stake. Another reason is the design of the adequacy decision as a unilateral assessment by the EU. To constantly monitor developments in all countries that have been granted adequacy, especially in relation to the practice of application of the legal framework governing the processing of personal data, would require a substantial investment and granular expertise from the European Commission. In turn, third countries do not have any notification obligations regarding the changes of rules or practices related to personal data protection and national security programs, which makes the discovery of such changes burdensome for the EU. Even at the stage of negotiations, as the practice of negotiating the adequacy decision with Japan has shown, the Commission may not commission independent expert opinions on the third country’s legal system and instead relies solely on the statements of the foreign government.\footnote{Greenleaf (2018b), p. 9.}

On the second point (the ‘heavy burden’ problem), seeking judicial or administrative redress abroad under the rules of a foreign legal system may incur prohibitive costs for individuals.\footnote{Kuner (2009), pp. 8-9.} This is even assuming that the level of personal data protection guaranteed in a third country, including the level of administrative fines, does comply with the standard of ‘essential equivalence’. In the case of Japan, which as discussed above, has created a higher level of protection of personal data from the EEA as compared to Japanese citizens’ data, enforcement of those higher protections may also be more difficult as there will be scarce domestic practice on which Supplementary rules (applicable only to personal data transferred from the EEA) can be grounded. Similarly, even when the GDPR applies to the processing of personal data abroad (e.g. under Article 3(2) GDPR)\footnote{As discussed in Section 2.2.1.2, the question on the relationship between Chapter V GDPR rules on transfers of personal data and extraterritorial application of the GDPR under Art. 3(2) GDPR remains an open question.} and grants EU member state courts jurisdiction over the issue – for example, in relation to damage compensation under article 79(2) GDPR – the costs of enforcing such a decision against a foreign controller in a third country are likely to be much higher than the amount of damages the individual may obtain. In addition, the harm caused to individuals as a result of violation of their fundamental rights cannot be fully undone. Lack of enforceability

\footnotesize
\textsuperscript{1156} Greenleaf (2018b), p. 9.
\textsuperscript{1157} Kuner (2009), pp. 8-9.
\textsuperscript{1158} As discussed in Section 2.2.1.2, the question on the relationship between Chapter V GDPR rules on transfers of personal data and extraterritorial application of the GDPR under Art. 3(2) GDPR remains an open question.
however, significantly reduces the effectiveness of data protection rules, as Section 5.3.3 below discusses in more detail.

On the third point (the ‘onward transfer’ problem), assessment of the rules for onward transfers of personal data from country A (which is undergoing the adequacy assessment) to country B (which does not have adequacy) is one of the factors in the adequacy assessment under Article 45(2)(a) of the GDPR. This means that, in order to preserve continuity of personal data protection and prevent circumvention of the EU data protection framework, the mechanism for transfers of personal data under country A’s legal framework should be ‘essentially equivalent’ to that of the EU. Although most countries’ legislation provides for some form of restrictions on international transfers of personal data, those restrictions are typically milder than those under the GDPR.\textsuperscript{1159} Onward transfer mechanisms in existing adequacy decisions adopted by the Commission, which aim to compensate for the absence of restrictions on transfers of personal data from countries granted adequacy, provide for a lower level of protection to personal data transferred from country A (that has been granted adequacy) to countries B, C, and D (that have not been granted adequacy) than the level of protection that would have been granted to this data if it was transferred to countries B, C, and D directly from the EEA. In other words, onward transfer mechanisms under the adequacy decision could allow circumvention of the EU’s high level of personal data protection and restrictions on transfers of personal data to third countries that have not been granted adequacy. Another challenge in this context is that the rules for onward transfers of personal data included in the adequacy decisions only apply to data obtained from the EEA and not to any other data processed in country A. Different legal regimes applicable to different data sets within the same country make monitoring of compliance difficult and therefore diminish the effectiveness of restrictions on onward transfers. This makes rules on onward transfers under adequacy decisions the Achilles’ heel of the adequacy mechanism. Furthermore, and relatedly, just as there is no effective mechanism to monitor the rules in countries afforded adequacy, the EU framework does not have any monitoring mechanisms for the onward transfer rules.\textsuperscript{1160}

To illustrate the point, the discussion below looks at specific provisions on onward transfer mechanisms under the adequacy decisions for Canada and Japan. There are two

\textsuperscript{1159} Greenleaf (2017a). For an overview of restrictions see Ferracane (2017), pp. 10-27.
\textsuperscript{1160} The same argument was made by France in its submission to the Council of the European Union. Preparation of the Council position on the evaluation and review of the General Data Protection Regulation (GDPR): Comments from Member States, 12756/1/19 REV 1, submission of France, p. 24 (‘the existence of a precise and effective mechanism for monitoring these rules, in particular in regard to subsequent transfers of the European data transmitted, must be a sine qua non for the adoption of an adequacy decision, and must be regularly assessed by the European authorities.’) The importance of such monitoring is also highlighted by the EDPB. EDPB, Contribution of the EDPB to the evaluation of the GDPR under Article 97, Adopted on 18 February 2020, p. 6.
reasons for selecting these specific adequacy decisions. First, these countries are important trading partners of the EU, with which the EU has recently concluded a trade agreement.\textsuperscript{1161} Second, Japan’s decision is the most recent adequacy decision adopted by the EU and the only one so far adopted under the GDPR. In other words, it is the most up-to-date adequacy decision. In contrast, the adequacy decision for Canada is one of the oldest, adopted in 2001. Bringing both of them into analysis demonstrates the evolution in adequacy decisions over the last 20 years.

Onward transfers of personal data from Japan to third countries are regulated in the ‘Supplementary Rules’ included in Annex 1 of the adequacy decision for Japan. These rules oblige Japanese businesses ‘to ensure (e.g. by technical (“tagging”) or organisational means (storing in a dedicated database)) that they can identify personal data transferred from the EEA throughout their “life cycle.”'\textsuperscript{1162} Recital 75 of the adequacy decision requires that further recipients of EEA data outside Japan are subject to rules ensuring a ‘similar’ level of protection to that of the Japanese legal order. The ‘similar’ as opposed to ‘essentially equivalent’ standard suggests that the adequacy decision sets a lower threshold for the legal framework in a country of onward transfer to meet, than that threshold applicable to countries of destination where personal data is transferred directly from the EEA.

The adequacy decision for Japan, including the Supplementary Rules, provides for three principal options for onward transfers of EEA data from Japan. The first option allows onward transfers based on an individual’s consent.\textsuperscript{1163} Supplementary Rule 4 specifies that ‘consent’ means that the individual has been ‘provided information on the circumstances surrounding the transfer necessary for the principal\textsuperscript{1164} to make a decision on his/her consent’. According to Recital 76 of the adequacy decision, this provision ensures that ‘such consent will be particularly well informed’ and will allow [individuals] to assess the risk for the privacy involved in the transfer.’ Greenleaf, however, rightly argues that Japanese consent requirements are lower than those under the GDPR.\textsuperscript{1165} The second and third options allow an onward transfer of personal data from Japan without such consent if (a) the country of destination of the onward transfer has been recognised by the Japanese data protection authority as providing a level of protection of personal data ‘equivalent’ to that of Japan; or (b) if the data exporter from Japan and importer in a third country have together implemented binding arrangements that guarantee an equivalent

\textsuperscript{1161} CETA with Canada and JEFTA with Japan.
\textsuperscript{1162} Recital 15 Adequacy Decision for Japan.
\textsuperscript{1163} Recital 76 Adequacy Decision for Japan, Supplementary rule 4.
\textsuperscript{1164} In terms of the GDPR, ‘principal’ means ‘data subject’.
level of data protection to that in Japan by means of a contract, other forms of binding agreements or binding arrangements within a corporate group.\textsuperscript{1166}

The adequacy decision for Canada simply does not address at all the issue of onward transfers of personal data.\textsuperscript{1167} Under Canadian federal law (the Personal Information Protection and Electronic Documents Act (PIPEDA)), transfers of personal data outside Canada are regulated by the principle of accountability. The 2009 Guidance by the Office of the Privacy Commissioner (OPC) of Canada explains that a transfer of personal data to a third party for the purposes of processing (including when such party is outside Canada) does not constitute disclosure of such personal data; therefore additional consent is not required for such a transfer.\textsuperscript{1168} It stipulates that such transfers are subject to the accountability of the Canadian organisation transferring personal data outside Canada, which means that such an organisation remains responsible for protecting personal data under its control. The primary means of compliance with this principle is through contractual arrangements to ensure that the third party will provide a comparable (not ‘essentially equivalent’ as required by the GDPR) level of personal data protection.\textsuperscript{1169} The Canadian OPC also requires organisations to assess the risks and benefits of transferring personal data outside Canada, and recommends applying higher standards of protection to sensitive data, such as financial data, and to refrain from such transfers when the risks are too high (e.g. due to the ‘uncertain nature of the foreign regime’).\textsuperscript{1170} In its opinion on the adequacy of PIPEDA, the Article 29 Working Party noted that such contractual or other binding provisions are able to provide a comparable level of data protection.\textsuperscript{1171} After a public consultation concluded in September 2019, the OPC decided that the 2009 Guidelines should remain ‘unchanged under the current law’.\textsuperscript{1172}

\begin{itemize}
\item \textsuperscript{1166}The adequacy decision explicitly states that APEC Cross-Border Privacy Rules cannot be used as a mechanism for onward transfers of EEA personal data from Japan. Recital 79.
\item \textsuperscript{1167} Kuner (2009), p. 5 (‘It is also striking that in its own adequacy decisions, the European Commission does not always require that third countries found adequate themselves prohibit the transfer of personal data to non-adequate countries. For example, the Canadian Personal Information Protection and Electronic Documents Act (PIPED Act (PIPEDA)) has been found adequate, even though the Act itself contains no such prohibition.’)
\item \textsuperscript{1168} Office of the Privacy Commissioner of Canada, Guidelines for Processing Personal Data Across Borders, January 2009.
\item \textsuperscript{1169} Principle 1 of the CSA Model Code for the Protection of Personal Information, Schedule 1 of PIPEDA, states: An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.
\item \textsuperscript{1170} Office of the Privacy Commissioner of Canada, Guidelines for Processing Personal Data Across Borders, January 2009.
\item \textsuperscript{1171} Opinion 2/2001 on the adequacy of the Canadian Personal Information and Electronic Documents Act, WP 39, 26 January 2001, p. 6.
\item \textsuperscript{1172} Office of the Privacy Commissioner of Canada, Commissioner concludes consultation on transfers for processing, 23 September 2019.
\end{itemize}
time, the Privacy Commissioner acknowledged that the ‘PIPEDA’s accountability principle is not always effective in protecting Canadians in the context of international transfers’ and requires reform.\textsuperscript{1173} Similar to the situation with Japan’s adequacy decision, this shows that the standard required for onward transfers is lower than that required by the GDPR for transfers of personal data outside the EEA.

To sum up, the most recent adequacy decision for Japan devotes significantly more attention to the question of onward transfers of personal data than the earlier adequacy decision for Canada. Analysis of the onward transfer mechanisms in the adequacy decision for Japan shows, however, that the range of onward transfer mechanisms is narrower than the range of mechanisms for transfers of personal data available under Chapter V of the GDPR and is limited solely to contractual arrangements or binding arrangements within a group and individual consent. Despite the fact that the choice of onward transfer mechanisms is restricted, in substance their application is unlikely to meet the standard of ‘essential equivalence’ to the EU framework, and, therefore, the strict necessity and proportionality tests for derogation from these fundamental rights under Article 52(1) of the Charter.

In relation to consent, for example, Greenleaf convincingly argues that it cannot serve as a sufficient basis for onward transfers of personal data for at least three reasons.\textsuperscript{1174} First, the Supplementary Rules annexed to the adequacy decision for Japan do not require, when obtaining consent, individuals to be informed that their data will be subject to an onward transfer to a country with a lower level of data protection.\textsuperscript{1175} Second, as already mentioned above, the standard for actually obtaining consent under Japanese law is lower than that under the GDPR.\textsuperscript{1176} The third, and more systemic, issue is that, under the GDPR, consent is a specific derogation that is inappropriate for systematic transfers of personal data. The fact that it can be used as a legal ground for systematic onward transfers of personal data from Japan is inconsistent with the logic of the GDPR, where under Article 49 GDPR, as interpreted by the EDPB, consent can be used only for non-repetitive and occasional transfers.\textsuperscript{1177} This thesis contends that it is precisely because of the fact that specific derogations, such as consent, are not intended for systematic transfers, that the

\textsuperscript{1173} 2018-2019 Annual Report to Parliament on the Privacy Act and the Personal Information Protection and Electronic Documents Act. Data protection law reforms have been announced in December 2019 by Canada’s Prime Minister Trudeau. See Hunt (2019).
\textsuperscript{1174} Greenleaf (2018b), p. 8.
\textsuperscript{1175} Ibid. (‘Supplementary Rule (4) requires that the individuals concerned shall be “provided information on the circumstances surrounding the transfer necessary for the principal to make a decision on his/her consent”. However, there is no obligation to tell the person that their data will be transferred to a country with very weak privacy laws such as the US’. Internal footnotes omitted).
\textsuperscript{1176} Ibid.
CJEU in *Schrems II* did not impose the ‘essential equivalence’ standard on transfers using such derogations. As the Article 29 Working Party noted in the 2014 Opinion on data protection in Québec, ‘consent should not be promoted as the general legal basis for onward transfers as the recipient then does not commit to take any action to ensure an adequate level of protection; this situation should thus remain an exception.’\(^{1178}\) In essence, by allowing regular transfers on the basis of consent, the adequacy decision for Japan allows the circumvention of the GDPR rules restricting transfers of personal data on the basis of consent. This places Japanese companies in a more favourable position than those from third countries that have not been afforded adequacy, as unlike Japanese companies, those companies cannot rely on consent for systematic transfers of personal data from the EEA.

In respect of using contractual arrangements and binding agreements within the group as mechanisms for onward transfers, there are at least two potential problems. The first is that, unlike the SCCs and the BCRs in the GDPR framework, there are no specific requirements that such contractual and intra-group arrangements must incorporate. Recall that the model SCCs in the EU are approved by the Commission and must be incorporated verbatim in the contract. As confirmed by the CJEU in *Schrems II*, these provide for ‘effective mechanisms’ for protection of personal data, but only to the extent that transfers are suspended or prohibited when the recipient of data is unable to comply with those clauses.\(^{1179}\) In addition, the GDPR provides for extensive requirements as to the content of the BCRs, further elaborated in the EDPB guidance.\(^{1180}\) Furthermore, the compliance of BCRs with the GDPR is ultimately certified by the EDPB, which approves BCRs before they take effect.\(^{1181}\) The absence of similar requirements in relation to contractual and intra-group arrangements used for onward transfers of personal data from Japan and Canada is likely to lead to a lower level of data protection as compared to that under the SCCs and the BCRs. The second problem, as discussed in Section 5.3.1 above, is that appropriate safeguards like the SCCs and the BCRs can be used as mechanisms for systematic transfers of personal data to third countries that have not been afforded adequacy only subject to prior comprehensive case-by-case assessment by data exporters of such third country’s legal framework. Relying on the logic of the EU framework for transfers of personal data as interpreted by the CJEU in *Schrems II*, and in light of the aims pursued by the EU

---


\(^{1179}\) CJEU, *Schrems II*, para. 148.

\(^{1180}\) Art. 47(2) GDPR; Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, WP 256 rev.01, 6 February 2018; Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules, WP 257 rev.01, 6 February 2018.

\(^{1181}\) Art. 47(1) GDPR.
framework for transfers of personal data, the same assessment must be conducted whenever contractual or intragroup arrangements are used for onward transfers of personal data. This requirement could indeed be one of the outcomes of the above-mentioned ongoing review of adequacy decisions by the European Commission. The adequacy decision for Japan, however, is not covered by such review. Until this deficiency is rectified through amendment by the Commission, or interpretation in the light of *Schrems II* by the EDPB or domestic courts, this adequacy decision is unlikely to yield an essentially equivalent protection of personal data in the context of onward transfers.

A further complicating factor is, as already mentioned, that since 2018 both Japan and Canada have been subject to an obligation to ensure free cross-border data flows between the parties to the CPTPP, most of which do not have an adequacy decision from the EU.\footnote{Art. 14.11(2) CPTPP.} The USMCA contains a similar provision.\footnote{Art. 19.11 USMCA.} Unlike Canada, the US and Mexico do not have an adequacy decision from the EU. These international trade obligations put additional pressure on the mechanisms of onward transfers under the adequacy decisions. Given that the EU is refraining from including such obligations in its own trade agreements, countries, such as Japan and Canada, to which EU personal data can be transferred without restrictions, can become – in a multinational company’s setting - a transit point for data transfers to other countries not afforded adequacy, thus circumventing the EU framework for cross-border transfers of personal data.

5.3.3 Limited scalability of EU framework for transfers of personal data

Against the backdrop of the broad understanding of the notion of ‘personal data’ in the EU, this Section argues that the EU regime for transfers of personal data outside the EEA in Chapter V GDPR lacks granularity in the sense that the same rules apply irrespective of the context, volume and type of data transferred and other parameters of data transfers. In a world where massive volumes of personal data are transferred every second, it is unrealistic to expect that the stringent EU framework under Chapter V of the GDPR will be observed in all those transfers. Even more unrealistic is it to believe that the EU DPAs endowed with the powers to enforce this compliance can have the capacity to monitor such compliance and enforce against non-compliance in order to produce an effective level of deterrence to violate such rules. As a result, there is a mismatch between the *legal framework* and the *reality* of data transfers in the digitalised world.
EU law maintains a distinction between personal data and non-personal data, which are governed by two different legal frameworks. In the digital environment, where almost any data can be linked to an identifier, the distinction between what constitutes personal data and what remains non-personal data – and therefore not subject to the scrutiny of stringent data protection rules – is often difficult to make. While cross-border transfers of personal data are subject to a ‘border control’ regime as discussed above, transfers of non-personal data outside the EEA are not subject to restrictions on transfers under the GDPR. As a result, there is misalignment between reality, where it is hard to draw a distinction between personal and non-personal data, and the legal framework, which qualifies data as either personal and non-personal.

Schwartz and Solove succinctly summarise four main problems with this distinction. First, almost any data online can be qualified as personal data. The ‘built-in identifiability’ in cyberspace makes anonymity online a ‘myth’, as all online data can be linked to some identifier. Second, non-personal information can be transformed into personal data over time. Third, the distinction between personal and non-personal data has a dynamic nature, as the line between the two depends on technological developments. Fourth and finally, the borderline between personal and non-personal data is not firm, but rather contextual, as many kinds of data are not non-identifiable or identifiable in the abstract.

1184 Koops (2014), p. 257 (‘EU data protection law applies an all-or-nothing approach: data is either personal data (triggering the whole regime), or it is not (triggering nothing), but it cannot be something in between or something else’. While processing of personal data is regulated by the GDPR, non-personal data is governed by Regulation on Non-Personal Data.
1185 Recital 9 Regulation on Non-Personal Data. For a discussion, see Tene, Polonetsky (2013); Kondor, Hashemian, De Montjoye, Ratti (2018); Schwartz, Solove (2011); Purtova (2018), p. 78; Ohm (2010), p. 1706 (warning about the problems of re-identification of personal data and stressing that even truly anonymised personal data at some point in time may be re-identified.)
1187 Regulation on Non-Personal Data does not provide for any restrictions on cross-border transfers of non-personal data outside the EEA. See also Art. 11(1) the Proposal for a Directive of The European Parliament And Of The Council on the re-use of public sector information (recast). COM/2018/234 final - 2018/0111 (COD). (‘Any applicable conditions for the re-use of documents shall be non-discriminatory for comparable categories of re-use, including for cross-border re-use’.) See also Collington (2019); Irion, Williams (2019), p. 31.
1188 See also Ohm (2010), p. 1706 (warning about the problems of re-identification of personal data and stressing that even truly anonymised personal data at some point in time may be re-identified.)
1189 Schwartz, Solove (2011), pp. 1836 – 1848. Stating that '[f]irst, many people believe in an ‘anonymity myth,’ -that is, a belief that individuals remain anonymous if they have not formally used their name. This belief is especially prevalent for cyberspace activity. Yet, the growth of static IP addresses and other developments creates some built-in identifiability when one enters cyberspace. Second, information that is initially non- PII can be transformed into PII. Third, technology itself is constantly evolving, which means that the line between PII and non-PII is not fixed but rather depends upon changing technological developments. Fourth, the ability to distinguish PII from non-PII is frequently contextual. Many kinds of information are not inherently non- identifiable, or identifiable as an abstract matter.
The EU Regulation on Non-Personal Data illustrates a number of those points. It specifically mentions that examples of non-personal data include ‘aggregate and anonymised datasets used for big data analytics, data on precision farming that can help to monitor and optimise the use of pesticides and water, or data on maintenance needs for industrial machines’. The Regulation, however, also notes that ‘[i]f technological developments make it possible to turn anonymised data into personal data, such data are to be treated as personal data, and [the GDPR] is to apply accordingly’. Although the very existence of this Regulation is grounded on the possibility of separating the notions of personal and non-personal data, the Regulation itself suggests that such distinction is not clear-cut and requires constant re-assessment.

Maintaining this distinction between personal and non-personal data in a situation where almost any data element can be qualified as personal at a specific point in time can also be very costly. The transition of data from non-personal to personal leads to higher compliance costs and the risks of multimillion Euro fines. As a result, the problems of distinguishing personal and non-personal data exemplify a tendency of any data potentially becoming personal in the future and being treated as personal. The upshot of this is that the GDPR has become applicable to virtually any operations with data, which, in the words of Purtova, makes it ‘the law of everything’. Viewing this tendency critically, Koops argues that broadening the notion of personal data leads to an ‘artificial framing of data-processing problems in terms of personal data’. These authors predict that the

---

1190 Recital 9 Regulation on Non-Personal Data.
1191 Ibid.
1192 A 2019 OECD study shows that businesses across sectors overwhelmingly report that separating personal from non-personal data is likely to be costly or very costly. Casalini, López González (2019), p. 33 and figure 6 (‘The extent to which firms can identify and split personal from non-personal data was also identified as an issue for firms. Respondents to the business questionnaire overwhelmingly reported that separating data was likely to be costly or very costly, a response consistent across most sectors’)
1193 Art.83(4)-(5) GDPR.
1194 Ohm (2010), p. 1742. (‘No matter how effectively regulators follow the latest re-identification research, folding newly identified data fields into new laws and regulations, researchers will always find more data field types they have not yet covered. The list of potential PII categories will never stop growing until it includes everything’. Internal footnotes omitted); Purtova (2018), p. 41 arguing that ‘literally any data can be plausibly argued to be personal’.
1196 Koops (2014), p. 258 (arguing that in the EU all data processing ‘is seen through the lens of personal data, in the frame of data protection law’, which requires ‘stretching the concept of personal data (sometimes to the point of breaking, or perhaps rather of becoming void of meaning), or stretching the regulatory problem so that it becomes a problem of processing personal data’. He also argues that ‘the second problem of relying on law in the books is the expansion of data protection legislation to include almost all types of data processing, leading to an artificial framing of data-processing problems in terms of personal data’.) See also Granger, Irion (2018), p. 16 (highlighting ‘a recent tendency to overcharge EU data protection law with expectations that it would come to terms with the much more complex challenges of algorithmic decision-making and artificial intelligence.’) But see Dalla Corte (2019) (proposing a ‘nuanced epistemological approach’ to interpretation of the notion of ‘personal data’ in order to avoid overly extensive interpretation of this notion.)
application of the GDPR’s ‘highly intensive and non-scalable regime’ to virtually any data processing will devoid this data protection framework of any meaning,\textsuperscript{1197} by leading to paper compliance and selective enforcement.\textsuperscript{1198} In the same vein, Helen Dixon, the head of the Irish DPA – which is in charge of supervising the European data processing operations of a number of big tech companies – acknowledged in a media interview that ‘[o]ne of the problems with GDPR is that it has become the law of everything, and that it’s drawing data protection authorities, who are not elected officials, into making an awful lot of decisions that impact societies and individuals, which go well beyond data processing.’\textsuperscript{1199} As Bygrave noted in connection to this, the ‘general discourse on data protection has become extremely GDPR-centric’ in that ‘the [GDPR] has effectively created a vortex that sucks policy discussion into its fold’.\textsuperscript{1200}

The point about the broad definition of personal data is not made here with a view to criticise the breadth of this definition in the GDPR, as there are good normative reasons to support a broad definition of this notion.\textsuperscript{1201} Given that the rights to privacy and the protection of personal data are protected as fundamental rights, maintaining a broad concept of ‘personal data’ is essential to ensure a high level of protection of these fundamental rights.\textsuperscript{1202} Rather, this is meant here as a critique of the way in which EU institutions use the broad definition of personal data in their discourse to expand their competence through framing the issues beyond data protection as GDPR issues, as their competence to legislate on data protection is ‘clear-cut’.\textsuperscript{1203} Furthermore, to be clear, this thesis also does not propose to eliminate a legal distinction between personal and non-personal data and, as Purtova has suggested, to treat all data as personal,\textsuperscript{1204} as this would water down the legal data governance framework even further. The thesis does, however, call for a reform of data protection rules on transfers of personal data to make them more scalable and, therefore, more effective in practice.

\textsuperscript{1197} Purtova (2018), p. 75 (‘a highly intensive and non-scalable regime of rights and obligations created by the GDPR will not simply be difficult but impossible to maintain in a meaningful way’.)
\textsuperscript{1198} Ibid., pp. 77-78 (‘Facing the threat of effective and deterring sanctions, the controllers, instead of engaging in a meaningful assessment of fairness and necessity, will be pushed to create the formal appearance of compliance by using “compliance surrogates”, such as compliance roadmaps, “accountability tools,” trust marks and certification schemes’); Ibid., p. 78 (‘Alternatively, or in addition, enforcement of the data protection rights and obligations will likely become selective, determined by priority lists and short-cuts that the data protection authorities would develop to cope with the workload, including the “compliance surrogates”. Selective enforcement and the pretence of compliance will reinforce each other, ridiculing data protection law, and depriving its protection of meaning.’)
\textsuperscript{1199} Tene (2020a).
\textsuperscript{1200} Bygrave (2020).
\textsuperscript{1201} See, e.g., Demetzou (2020), p. 131.
\textsuperscript{1203} Tene (2020a).
\textsuperscript{1204} Purtova (2018), pp. 79-80.
To some extent, the GDPR has already made steps towards greater scalability by implementing a risk-based approach to data protection. In particular, the GDPR contains stricter rules for the processing of special categories of personal data, such as personal data relating to health, race or sexual orientation.\textsuperscript{1205} Data about criminal convictions, the content of electronic communications, and financial and location data have also been recognised as sensitive by the Article 29 Working Party and its successor, the EDPB, due to the higher risks of processing these types of data for individual rights. They are therefore, subject to a higher level of protection than personal data falling into what one might call the general category.\textsuperscript{1206} In addition, in several contexts (for example, in the balancing between the legitimate interest of the data controller as the legal ground for processing personal data with the risk to the fundamental rights of data subjects, data breach notification, accountability of data controller), the GDPR allows data controllers to calibrate their obligations in accordance with the risk that certain processing of personal data may pose to the fundamental rights of individuals.\textsuperscript{1207} Furthermore, the GDPR has codified a notion of \textit{pseudonymised data}.\textsuperscript{1208} Recital 28 of the preamble to the GDPR explicitly states that the ‘application of pseudonymisation to personal data can reduce the risks to the data subjects concerned’. As noted by various experts in the field and European Data Protection authorities, the GDPR already provides for more lenient rules for pseudonymised data when it comes to the rights of individuals, data breach notification requirement and the possibilities of using the data for purposes other than that for which it was originally collected.\textsuperscript{1209}

None of these flexibilities, however, are taken into account in the GDPR’s framework for transfers of personal data \textit{outside the EEA} in Chapter V. Therefore, the criticism of non-scalability, lack of nuance and a catch-all method fully applies to this set of rules. Moreover, as compared to the substantive data protection framework, which, to some extent has embraced a risk-based approach, the provisions on data transfers do not differentiate between different degrees of risks to fundamental rights that transfers of personal data may entail for individuals. Given the expansive scope of information that may constitute personal data, this ‘one-size-fits-all’ approach to cross-border transfers is

\textsuperscript{1205} Art. 9 GDPR.
\textsuperscript{1206} Article 29 Working Party, Guidelines on Data Protection Impact Assessment (DPIA), WP 248rev.01, 4 October 2017.
\textsuperscript{1207} Article 29 Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP 217, 9 April 2014. At the time of writing, the EDPB is working on the new guidelines on the topic.
\textsuperscript{1208} Art. 4(5) GDPR.
not sustainable in the long run as it applies to growing datasets including ‘Big Data’ corpora systematically crossing EEA borders. Under these circumstances, it is hardly realistic to expect that the same level of ‘effective and complete’ protection of all personal data transferred internationally can be achieved in practice. Requiring the same level of compliance with a strict regime for transfers of personal data for such a broad scope of data is simply inoperable. Kuner thus seems to be correct when he argues that ‘[t]he definition of transborder data flows is so broad that it can cover most acts of data processing on the Internet, and no national regulation could ever be consistently enforced with regard to such a vast amount of data processing on a global scale,’\textsuperscript{1210} It is therefore entirely unsurprising that enforcement of the rules on cross-border data flows has so far been ineffective.\textsuperscript{1211} Throughout the lifetime of the EU data protection framework, the only significant enforcement actions came from the CJEU, which, as discussed above, invalidated adequacy decisions issued by the European Commission for the US.\textsuperscript{1212} Just as there was ‘very little enforcement related to the Schrems I judgement’,\textsuperscript{1213} Schrems II is unlikely to lead to a surge of enforcement actions in the context of data transfers.\textsuperscript{1214} Apart from a few enforcement actions triggered by the CJEU, there have not been, until recently, any known enforcement cases for violations of rules on transfers of personal data. It was only in June 2020 that the EDPB initiated the first major enforcement action to date by establishing a taskforce to coordinate potential enforcement actions across Europe against TikTok, which covers, in particular, the company’s practices of transferring personal data to third countries.\textsuperscript{1215}

The risk of enforcement is one of the major drivers behind companies’ compliance with data protection rules. Thus, a lack of enforcement reduces the risks of non-compliance with the cross-border transfer rules, making them even less effective in performing their

\textsuperscript{1210} Kuner (2013), pp. 154-155. See also Koops (2014), p. 259: The regulatory disconnection of data protection law, with risks being enlarged rather than diminished through stretching the scope of data protection law to embrace new regulatory issues, together with a narrow focus on command-and-control law, demonstrate a fallacy of regulators to believe that every problem related to Internet data flows can be regulated by data protection law in the books. It does not work, as any realist looking at 21st century data processing practices will acknowledge.

\textsuperscript{1211} Kuner (2013), p. 144. (‘The levels of compliance and enforcement of transborder data flow regulation are important indicators of its effectiveness. A lack of enforcement, or inconsistent enforcement, may reduce respect for a particular rule, and for a regulatory system in general.’)

\textsuperscript{1212} CJEU, Schrems I and Schrems II.

\textsuperscript{1213} Kuner (2017), p. 885.

\textsuperscript{1214} Referring to the inaction on the part of the DPAs, Max Schrems, the activist behind the legal action that led to the CJEU Schrems II judgement has already filed 101 complaints with DPAs across Europe to pressurise the authorities to take action. Noyb (2020a). Some authorities, however (e.g. the Finnish DPA) have initiated several inquiries following the request. See Clark (2020).

\textsuperscript{1215} EDPB, Press Release, Thirty-first Plenary session: Establishment of a taskforce on TikTok, Response to MEPs on use of Clearview AI by law enforcement authorities, Response to ENISA Advisory Group, Response to Open Letter NYOB, 10 June 2020.
function of preventing the circumvention of the EU’s high level of personal data and privacy protection.

5.4 Directions of thought on how to improve the EU framework for transfers of personal data outside the EEA

A reform of the GDPR’s framework for transfers of personal data outside the EEA is necessary to address its weaknesses, as identified in the previous Section. This Section suggests and elaborates upon three possible lines of thought on how to improve the framework. It should be acknowledged that a fully-fledged reform proposal cannot be developed within the boundaries of this work for a few reasons, among them the fact that the aim of this thesis is to situate the need for reform in the context of international trade law and the EU’s approach to existing and future trade commitments. A comprehensive reform of the GDPR would require an interdisciplinary effort based on a host of both domestic and international factors, an endeavour which goes well beyond the scope of this thesis. Hence, this Section’s objective is to inform and suggest reform paths, but not to offer an exhaustive overview of opportunities for reform of the GDPR’s Chapter V.

The three proposed paths or lines of thought that this Section considers are as follows. The first, and the most moderate, is to improve specific elements of the mechanisms for transfers of personal data already present in Chapter V of the GDPR but without changing the design and composition of the framework. The second, intermediate, path incorporates the first but goes a step further by suggesting adding several new elements to the extant framework based on key recent developments in EU data protection law and technology. The third, and the most radical, path is a complete redesign of GDPR Chapter V’s framework, for example by re-anchoring it on a risk-based approach, with elements proposed as a part of the second line of thought. The three paths roughly correspond to short, medium, and long term strategies for the reform of Chapter V of the GDPR.

Before moving on to the discussion of each path, two remarks are in order. First, recall, that while some form of restrictions on transfers of personal data form part of the essence of the fundamental rights to privacy and the protection of personal data, their specific design – with some specific exceptions – is subject to balancing with the aim

---

1216 Based on the current CJEU case law, the elements of the design of the framework for transfers of personal data, which constitute a part of the essence of the fundamental rights to privacy and the protection of personal data, include: a) restrictions on generalised access to the content of electronic communications; b) compliance with the purpose limitation principle, the rules designed to ensure, inter alia, the security, confidentiality and integrity of the data, and to protect them against unlawful access and processing; c) limitations on the retention of the content of communications; d) rules that provide for some possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data. For a discussion see Section 5.2.3.2.
of ensuring ‘essentially equivalent’ protection of personal data. This balancing must be conducted on the basis of the principles of strict necessity and proportionality (Article 52(1) of the Charter), which, as Section 5.2.2 above explained, underlie the ‘essential equivalence’ standard. Second, the concept of ‘essential equivalence’ itself does not constitute the essence of the fundamental rights to privacy and the protection of personal data under the Charter. It does, however, constitute a part of the constitutional meaning of the above-mentioned fundamental rights and is not merely an interpretation of the secondary EU data protection law concept of ‘adequacy’.

5.4.1 Improving the operation of the current framework

This line of thought considers a number of improvements to existing mechanisms for transfers of personal data, in particular adequacy and the SCCs. It also recommends the operationalisation of the codes of conduct and certification mechanisms, which are envisaged as data transfer mechanisms in the GDPR but have not yet been implemented in practice. Although this line of thought does not resolve some of the conceptual drawbacks of the framework of Chapter V, its modesty makes it easier to implement, at least in the short term. Furthermore, it could yield an incremental improvement through fairly minor changes to the GDPR and CJEU jurisprudence without having to redesign the framework for transfers of personal data at its core, which seems a much longer-term exercise.

To address the proneness of adequacy decisions to political influence, the EU could adopt a transparent procedure governing such assessments. According to Kuner, the European Commission already has internal guidelines for evaluating adequacy, though they have never been published. A renewed procedure could, in particular, regulate the process of the selection of countries (or application by countries themselves) in relation to which the adequacy assessment is to be conducted and the detailed procedure for an adequacy assessment, including the due involvement of all stakeholders (such as the EDPB and European Parliament), the time frame for the whole process as well as for each step of the assessment. All this would ensure, among other things, that stakeholders have sufficient time and opportunity to review the assessment. The Commission could be required to respond and substantiate its deviation from the recommendations or opinion of stakeholders, and to involve experts in the assessment, so as to exclude situations where the review of the foreign legal system is conducted by the European Commission’s employees on the basis essentially consisting of submissions by the foreign government.

\[\text{Kuner (2017), p. 901.}\]

\[\text{EDPB, Contribution of the EDPB to the evaluation of the GDPR under Article 97, Adopted on 18 February 2020, pp. 4-6 (noting that the EDPB should have sufficient time to review adequacy decisions.)}\]
Such a procedure could be adopted by a Commission’s Implementing Regulation, which, however, would require including a relevant enabling provision in the GDPR.

To enhance ongoing monitoring of the foreign legal framework, and in order to mitigate the fact that an adequacy assessment (and its review once in four years) constitutes a snapshot of the foreign legal framework at a particular point in time, adequacy decisions could transition from a unilateral instrument to a reciprocal agreement, under which the foreign country would undertake certain obligations. For example, such an agreement could include a mechanism of notifications by the foreign government of any changes to legislation taken into account during the adequacy assessment, and provide for negative consequences for non-notification, if discovered during the periodic review. This change would not require any amendments to the GDPR.\(^\text{1219}\)

The onward transfer mechanisms should, as much as possible, mirror the appropriate safeguards provided for in the GDPR and as interpreted by the CJEU in Schrems II. This is necessary in order to avoid discrimination between transfers of personal data on the basis of appropriate safeguards to countries not afforded adequacy from the EEA (under Article 46 GDPR) and onward transfers of personal data from a country that has been afforded adequacy, to another country that has not been afforded adequacy. In particular, consent should not be generally allowed as a legal ground for systematic onward transfers (as discussed above, consent serves as one of the grounds for onward transfers in the EU adequacy decision for Japan). In addition, contractual mechanisms used for onward transfers should incorporate the SCCs approved by the European Commission; their wording should not be left to the discretion of the parties.

In relation to the SCCs, as Kuner argued, controller-to-controller SCCs could be improved by putting a greater emphasis on the practically enforceable redress mechanisms and dropping the obligations that are difficult to enforce in practice.\(^\text{1220}\) In particular, Kuner has proposed to reform the 2004 SCCs by eliminating or shifting some of the data importer’s obligations to the data exporter because they are difficult to enforce outside the EU.\(^\text{1221}\) To enhance the effectiveness of the SCCs, the European DPAs should also enhance their enforcement efforts on this issue, for example, through conducting industry scans and

\(^{1219}\) The most recent (and thus far the only) adequacy decision under the GDPR – Adequacy decision for Japan – contains Supplementary Rules, which Japan undertook in order to compensate for the deficiency of its legal framework for protection of personal data as compared to that of the EU. Similarly, the two adequacy decisions for the US – the invalidated EU-US Safe Harbor and the EU-US Privacy Shield – contain representations by the US Government in relation to the protection of personal data.


\(^{1221}\) Kuner (2009), pp. 8-9.
requests for information, while prioritising the transfers that that carry the greatest risks for individuals.\footnote{See Kuner (2011), p. 27.}

The issue of foreign governments’ access to personal data transferred from the EEA is a highly politically contentious one. It also cuts across an intricate relationship between the EU legislature and the CJEU, as it was the CJEU that introduced this issue to the EU framework for transfers of personal data in the first place. Although in the long term, as this thesis argues in Section 5.3.1 of this Chapter, this topic should be addressed by the EU at the international level, in the short term, the DPAs should issue comprehensive guidance on the assessment of the ‘essential equivalence’ of foreign legal frameworks for the purposes of relying on Article 46 for personal data transfers and formulate additional safeguards that companies could use to mitigate the lack of ‘essential equivalence’. This is essential in order to avoid a surge of private enforcement in this area, which would lead to the fragmentation of approaches across the EU, at least, in the short and medium term. The EDPB could also spearhead a platform with reliable resources necessary to assess the ‘essential equivalence’ of third countries’ frameworks, prioritising those where personal data is transferred most from the EEA.\footnote{A private crowd-sourced initiative has been recently launched by Christopher Schmidt. Although this resource provides useful insights, it does not guarantee accuracy of the information and that the EDPB will take this information into account in conducting their assessment during a possible enforcement action. EUROPEAN ESSENTIAL GUARANTEES GUIDE, https://www.essentialguarantees.com/}

\subsection*{5.4.2 Greater scalability}

A second, intermediate line of thought suggests adjustments to the GDPR’s framework for transfers of personal data \textit{complementing} those encompassed by the first line of thought discussed in the previous Section. It would require a more substantial revision of the GDPR and, therefore, could realistically be addressed only in the medium term. For example, it could be introduced as a result of the next review of the GDPR’s Chapter V under Article 97 of the GDPR, which is scheduled for 2024.

The two principle adjustments that could be introduced into Chapter V of the GDPR are (a) the introduction of the more lenient rules for transfers of pseudonymised data as long as such data does not include sensitive data;\footnote{Just like pseudonymised personal data remains personal, pseudonymised sensitive data remains sensitive data. This means that processing pseudonymised sensitive data still involves a higher risk than processing pseudonymised ‘ordinary’ personal data.} and (b) a codification of the legal significance of technological means for protection of personal data, including as a means of ensuring that pseudonymised data will not be re-identified after the transfer. In his 2014 article, Koops suggested that pseudonymised data could become a ‘useful in-between
category’ between personal and non-personal data.\textsuperscript{1225} He proposed, accordingly, the creation of a special legal regime for pseudonymised data that would be ‘milder’ than the regime for personal data but stricter than for non-personal data.\textsuperscript{1226} Kuner proposed relaxing restrictions on cross-border transfers of pseudonymised and encrypted data under appropriate circumstances,\textsuperscript{1227} and data in transit.\textsuperscript{1228} Similarly, but in more general form, Schwartz and Solove have suggested calibrating the intensity of the data protection regime depending on the risk of identification of individuals, based on three categories of personal information (or data): (a) identified, (b) identifiable, or (c) non-identifiable.\textsuperscript{1229} As one of the advantages of their proposed approach, Schwartz and Solove name the incentives to companies to invest resources in maintaining data in the less identifiable form. In contrast, in the current EU regime that treats identifiable and identified data as equal, such incentive is absent.\textsuperscript{1230} Most recently, some data protection authorities and scholars proposed to use encryption, pseudonymisation and other privacy enhancing technologies as one of the additional safeguards that data exporters can implement while transferring personal data to countries that do not ensure an adequate level of data protection based on the SCCs.\textsuperscript{1231}

Since the adoption of the GDPR, pseudonymised data, defined in article 4(5) GDPR, gained more prominence in the EU data protection framework. Recital 28 of the preamble to the GDPR explicitly states that the ‘application of pseudonymisation to personal data can reduce the risks to the data subjects concerned’. As noted by various experts in the field and European DPAs, the GDPR already provides for more lenient rules for pseudonymised data, when it comes to the rights of individuals, data breach notification requirements, and the possibilities of using the data for purposes other than that for which it was originally stored.

---

\textsuperscript{1225} Koops (2014), p. 257, fn. 40. At the same time, Koops criticises the definition of ‘pseudonymised data’ in the (then draft) GDPR. That wording, however, has not changed in the final version of the GDPR.

\textsuperscript{1226} Ibid., p. 257 (‘… not all identifiers function in the same way, and it makes sense to differentiate in the legal regimes for different types of identifiers’.)

\textsuperscript{1227} Kuner (2013), pp. 97, 99.

Pseudonymization is used on a wide scale in some important areas (eg, in clinical trials of pharmaceutical products), and can be regarded as a form of encryption, since it allows identification of an individual only under limited conditions and by certain parties; it should be encouraged by relaxing restrictions on transborder data flows under appropriate circumstances. … [G]reater use should be made of technology in the context of transborder data flow regulation, such as by the creation of ‘safe harbours’ to ease regulatory approval of transborder flows of encrypted data.

See also Hon, Millard (2012), p. 27.

\textsuperscript{1228} Kuner (2013), p. 175.


\textsuperscript{1231} See e.g. One Trust Data Guidance (2020a); Christakis (2020).
Relaxation of these data protection principles, two of which are explicitly mentioned in Article 8 of the EU Charter, in relation to pseudonymised data, suggests that a lighter touch regulatory approach to transfers of such data outside the EEA could be compliant with the EU Charter and the GDPR. In particular circumstances, such as scientific or academic research, where societal benefits of data processing are high and risks of interference with fundamental rights could be minimised through various technological means, such as differential privacy and ethical safeguards of the profession, the transfer of pseudonymised data could be allowed without restrictions. Such a possibility would be welcome, for example, in global health crises such as the one triggered by the COVID-19 pandemic in 2020. It should, however, also be acknowledged that pseudonymisation is effectively a security measure which reduces the risks associated with personal data processing. The way in which this measure should be taken into account in designing more flexible rules for transfers of personal data outside the EEA requires further research.

In relation to the role of technology in governing information flows, Reidenberg in his seminal 1998 article ‘Lex Informatica’, showed that ‘for network environments and the Information Society … law and government regulation are not the only source of rule-making. … The creation and implementation of information policy are embedded in network designs and standards as well as in system configurations.’ He argued that Lex Informatica – ‘the set of rules for information flows imposed by technology and communication networks’ – had an equally important role to play, along with the law, in governing information flows online. Similarly, Kuner argued more recently that ‘technology could play a greater role in transborder data flow regulation’; in particular, through the principle of ‘privacy by design’ (which is now codified in the GDPR), it could explicitly include a possibility to regulate cross-border data flows in part by technological solutions. He also noted that companies already routinely configure their international IT systems to regulate cross-border flows of data and access rights in their IT networks.


For a discussion, see Kuner (2020a). Although Kuner does conclude that the current framework is flexible enough for the times of pandemic, he also emphasises its limitations.


Kuner (2013), p. 96. (‘But technology could play a greater role in transborder data flow regulation than is now the case. … Data controllers routinely configure information technology systems so as to regulate the transborder flow of data, and it is not uncommon for an international company to structure its IT system so that certain types of data may not be accessed by its employees outside a specific country or region’.)

Ibid.
Gürses and van Hoboken suggest that the question of information flows should be tackled at the level of the design and production of functionality, where some of the individual harms due to reidentification of data can be mitigated though privacy technologies, such as differential or pan-privacy. In addition, those authors note that certain privacy intrusive practices adopted by service providers can be leveraged by ‘automated privacy support that allows users to evaluate which information flows they want to engage in and how they can control these when they use services.’

It should, of course, be acknowledged that technology is not a panacea to correct inefficiencies of the legal framework in governing transfers of personal data, but it could provide an effective complementary regime to mitigate those inefficiencies. In his 2009 OECD study, Schwartz demonstrated based on several case studies that cross-border transfers of data are ‘not a finite event’ and ‘occur in a multi-directional fashion throughout the globe, and involve more companies and entities in the processing activities’. In other words, they ‘occur as part of a networked series of processes made to deliver a business result.’ The implication of this transformation is that regulating cross-border transfers of personal data based on the outdated views of information flows as point-to-point transfers is increasingly challenging, and is perhaps missing the forest for the trees. Technological tools in combination with data privacy industry standards could be more effective in tracing cross-border data flows and ensure that the legal regime for protection of personal data is not circumvented. The EU has already to some extent resorted to technological means in governing cross-border data flows in its adequacy decision for Japan. Because the adequacy decision creates – through Supplementary Rules – a higher level of data protection for data from the EEA in contrast to Japanese data, the Supplementary Rules require that Japanese business operators must ‘ensure (e.g. by

\[1238\] Gürses, van Hoboken (2018), p. 597:

If every form of digital functionality has the potential to be transformed into a data intensive machine learning product, the application of principles such as data minimization, purpose specification and policies that enforce some sort of control over data on the side of end-users is going to be challenging. At the same time, much of service capture creates prime opportunities to apply privacy technologies such as differential or pan privacy. The application of these techniques could protect users from individual harms due to reidentification of data.


\[1240\] Kuner (2013), p. 99 (‘The use of technology to regulate transborder data flows is not a panacea. Technological or ‘code-based’ solutions to regulatory problems can raise questions about democratic legitimacy and discrimination; for example, States can adopt national technical standards to disadvantage foreign providers, or mandate the use of domestic products. Procedures would thus have to be developed to ensure accountability and transparency in the implementation of technological solutions’.) See also Lessig (1999), at 138.

\[1241\] Schwartz (2009), pp. 12, 36.

technical ("tagging") or organisational means (storing in a dedicated database)) that they can identify such personal data throughout its “life cycle”.

Implementing these ideas in Chapter V of the GDPR would add more scalability to the regime for transfers of personal data, facilitate and enhance enforcement of compliance with the framework.

5.4.3 Redesign

In the longer term, addressing all the weaknesses of the GDPR’s Chapter V framework for transfers of personal data outside the EEA identified in Section 5.3 may require a much more thorough redesign. This redesign could grow organically out of improvements to the GDPR proposed as a part of the second line of thought. One way of doing so would be to replace the current one-size-fits-all approach, in which different mechanisms for transfers of personal data do not take into account the context and the parameters of the transfer, with rules designed on a risk-based approach. Ironically perhaps, such an approach to rules on transfers of personal data outside the EEA would fit much better into the logic of the GDPR, part of which already reflects a risk-based approach. In particular, this is the case in relation to some data protection elements explicitly or implicitly envisaged in Article 8 of the Charter, such as the legitimate interest that can be used as a legal ground for processing of personal data, the stricter rules for processing special categories of personal data, the principle of accountability, the provisions on records of processing activities, the data breach notification requirement, provisions on security of processing, the obligation of prior consultation with a data protection authority, and finally in the data protection impact assessment...

---

1243 Para. 15 Adequacy Decision for Japan.
1244 For a discussion on the role of the concept of risk in the GDPR, see, e.g., Demetzou (2020).
1245 It is, however, worth keeping in mind that the implementation of the risk-based approach in the GDPR is incomplete and is, arguably, in tension with the rights of the data subject envisaged in Chapter III GDPR. See, e.g., Quelle (2017b), pp. 20-21.
1247 Recital 51, Art. 9 GDPR.
1248 Recitals 74-77, Arts. 24 GDPR.
1249 Recital 82, Art. 30(5) GDPR.
1250 Recitals 85 – 88, Arts 33-34 GDPR.
1251 Recital 83, Art. 32 GDPR.
1252 Recitals 94-96, Art. 36 GDPR.
This strongly suggests that a risk-based approach to data transfers would also be feasible, and indeed arguably preferable.\textsuperscript{1254}

In light of the \textit{function} of the framework for restrictions on transfers of personal data based on the EU Charter, as discussed in the previous Sections of this Chapter, the main risk that the redesigned framework should address is the circumvention of the EU data protection regime when personal data are transferred abroad.\textsuperscript{1255} In fundamental rights terms, this can be reformulated as the risk that transfers of personal data outside the EEA can interfere with the fundamental rights to privacy and the protection of personal data more than is strictly necessary and proportionate to pursue a legitimate public policy objective.

In an effort to improve Chapter V, safeguards required for transfers of personal data could be differentiated in the GDPR depending on the remoteness of link between personal data and individuals to which it relates or, in other words, the risk of reidentification (which can serve as a proxy for the risk to a particular individual from a data transfer, including where data is accessed by foreign surveillance authorities) and threat of harm.\textsuperscript{1256} One could, for instance, use Ohm’s non-exhaustive list of five factors for assessing the risk of privacy harms in general, and apply it to harms associated with transfers of personal data:\textsuperscript{1257}

(1) data-handling techniques (risk of re-identification can be labelled as high, medium or low based on a rough relative ordering of different techniques that could potentially be developed by computer scientists\textsuperscript{1258});

(2) private versus public release (the level of protection of publicly released data should be higher than that of data shared between trusted parties due to higher privacy risks inherent in public release of data for privacy\textsuperscript{1259});

(3) quantity (larger volumes of data sets are more susceptible to reidentification through matching different data sets\textsuperscript{1260});

\textsuperscript{1253} Recitals 84, 89, 90-93, 95, Art. 35 GDPR.
\textsuperscript{1254} There is, however, some critique of this approach. See, in particular Quelle (2018); Quelle (2015); Quelle (2017b).
\textsuperscript{1256} For a discussion on this approach to regulating privacy in general, see Ohm (2010), pp. 1761, 1764. Schwartz and Solove are critical of this approach as it requires ex ante cost-benefit assessment of information flows, which, in their view, is not only speculative in nature but may also amount to rejecting potentially beneficial collections and use of large data sets. Schwartz, Solove (2011) pp. 1868-1869.
\textsuperscript{1257} Ohm (2010), pp. 1765-1768.
\textsuperscript{1258} \textit{Ibid.}, p. 1765.
\textsuperscript{1259} \textit{Ibid.}, p. 1766.
\textsuperscript{1260} \textit{Ibid.}, pp. 1766-1767.
(4) motive (the legal constraints on sharing data, the motives of owners of data sets to share them as well as the economic incentives for reidentification also have an impact on the risk of reidentification.\textsuperscript{1261}); and

(5) trust (society’s trust in people and institutions in privacy regulatory framework\textsuperscript{1262}).

In line with the first of those five factors, and incorporating the proposals made as a part of the second line of thought above, more lenient transfer rules could be designed for data that only has a remote link with individuals, such as pseudonymised data, when such data are transferred without additional information necessary to link the data to particular individuals. By definition, pseudonymised data cannot be attributed to a specific individual without the use of additional information, \textit{provided} such information is kept separately and adequately protected.\textsuperscript{1263} Beyond this, differentiation between the intensity of restrictions on transfers should not be solely or mostly based on the distinctions between different categories of data (such as sensitive data), because such distinctions are often highly contextual,\textsuperscript{1264} which makes differentiation between such categories difficult in practice.\textsuperscript{1265}

Several authors have emphasized that the data protection framework in general, and the framework for transfers of personal data in particular, should be focused on \textit{harm} or effects on individuals of data processing (or data transfers).\textsuperscript{1266} The risk of harm can also be captured by a risk-based approach. Kuner suggests, in relation to regulation of cross-border data flows, that focusing on the situations where cross-border data flows cause harm to individuals could be one way to improve the level of data protection compliance and enforcement.\textsuperscript{1267} He also notes, however, that under EU law and the European Convention on Human Rights it is unclear how to define ‘harm’ in the context of cross-border data flows.\textsuperscript{1268} Purtova argues that focusing on harm is generally in line with the case law of the CJEU.\textsuperscript{1269}

Another factor that could be useful in designing an improved framework for cross border transfers of personal data based on risk-based approach is the \textit{sector} in which the transfer of personal data occurs. For example, as one of the measures to increase availability of data for businesses, the European Commission has recently proposed to

\begin{itemize}
\item \textsuperscript{1261} Ibid., p. 1767.
\item \textsuperscript{1262} Ibid., p. 1767.
\item \textsuperscript{1263} Art. 4(5) GDPR.
\item \textsuperscript{1264} Koops (2014), p. 260; Moerel (2020).
\item \textsuperscript{1265} Purtova (2018), pp. 79, 80.
\item \textsuperscript{1267} Kuner (2013), pp. 147-148.
\item \textsuperscript{1268} Ibid.
\item \textsuperscript{1269} Purtova (2018), p. 62.
\end{itemize}
develop sectoral data spaces within the EU in strategic areas, such as manufacturing, agriculture, health and mobility.\textsuperscript{1270} This approach could also be usefully explored for transfers of personal data outside the EEA.

5.5 Conclusion

This Chapter has demonstrated that the framework for transfers of personal data outside the EEA in Chapter V of the GDPR represents only one possible design of such a framework in the light of the EU Charter requirements. Only the presence of some restrictions and a few aspects of such restrictions constitute the essence of the fundamental rights to privacy, the protection of personal data and the right to judicial remedy (in the context of the first two rights) and, therefore, cannot be altered by EU secondary law. Other elements of such a framework can be determined by the EU secondary legislator on the basis of strict necessity and proportionality assessment, with the aim of ensuring its constitutional function, which is to prevent circumvention of the high level of personal data protection in the EU. Section 5.3 of this Chapter has shed light on several weaknesses of the current framework’s elements and overall design, and argued that due to economic, political, geopolitical and legal changes, this framework is no longer actually fit for its constitutional purpose. To ameliorate these weaknesses within the boundaries set by the EU Charter, this Chapter has proposed three paths to how to improve this framework, corresponding to a short, medium,-and long term strategy for the EU.

\textsuperscript{1270} Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, A European Strategy for Data, COM(2020) 66 final, 19 February 2020, p.6.
6. Conclusions

This thesis has tackled the timely issue of reconciling the governance of cross-border data flows from the perspectives of EU data privacy protection and international trade law. It has demonstrated a real clash between international trade and European data privacy law when it comes to the governance of cross-border flows of personal data. This clash is the result of the coming together of a multitude of factors. Among them, the following three are of particular importance: (a) the pivotal importance of personal data in digital commerce; (b) the increased level of protection of the rights to privacy and the protection of personal data since 2009 as binding fundamental rights under the EU Charter; and (c) the recent trend of governing cross-border data flows by regional, plurilateral and multilateral trade agreements.

This thesis has provided the necessary background and analysis of EU rules governing cross-border transfers of personal data in the light of the EU Charter and the ways in which this issue is addressed in the current and proposed trade agreements led by the EU and the US. It also put the developments in both areas against the background of EU constitutionalisation and trade policy. In order to resolve the tensions caused by the above-mentioned clash, this thesis has analysed and proposed ways to ameliorate the situation from both ends (trade and personal data protection), specifically through reforms of both international trade rules in future trade agreements and GDPR rules. To explain how such reforms could be effectuated, the thesis has also aimed to fill in a significant lacuna in existing literature by looking at the role of discourse in the evolution of trade law, in particular in its relation to cross-border data flows. In doing so, the thesis considered the digital trade discourses currently advanced by the EU and the US in the course of negotiations of digital trade agreements, revolving around the issue of whether, and to what extent, restrictions on cross-border data flows amount to ‘digital protectionism’. The thesis has shown the importance of discourse in any attempt to reform trade rules.

This thesis answered the following research question:

how should commitments on cross-border data flows in future EU trade agreements be reconciled with the protection of the fundamental rights to privacy and personal data?

In answering this research question, this thesis has concluded that, in order to reconcile cross-border data flows with data protection and privacy without undermining fundamental rights, a reform of trade law rules in the EU’s future trade agreements and the GDPR rules on transfers of personal data outside the EEA is necessary. Tackling each of the research sub-questions specifically, the thesis has made the following propositions.
1. Simultaneous application of international trade and EU Charter rules to the restrictions on transfers of personal data outside the EEA may create a catch-22 compliance deadlock for the EU. On the one hand, there is a risk of inconsistency between the obligation on cross-border personal data flows, which can be deduced from the EU’s commitments under the GATS in the context of digitally provided services, and the restrictions on transfers of personal data under the GDPR. This inconsistency may not be justifiable under the general exception for privacy and data protection in trade agreements. On the other hand, from an EU Charter perspective, the level of liberalisation of cross-border data flows required by the GATS constitutes an interference with the fundamental rights to privacy and the protection of personal data under the EU Charter. This interference may not be justifiable under Article 52(1) of the Charter.

Although the GATS does not specifically regulate cross-border data flows, in Section 2.2 the thesis concludes that the different treatment of transfers of personal data outside the EEA to countries that have been an granted adequacy decision, and other countries, could be in violation of the MFN clause contained in the GATS. Similarly, the different treatment of personal data transfers to companies that have an establishment in the EEA compared to those who do not could result in a violation of the national treatment. The 2020 Schrems II judgement of the CJEU puts more pressure on the GDPR’s framework for transfers of personal data from an international trade perspective. In particular, the (soft) data localisation, that could follow in the aftermath of the judgement allows for the interpretation of this CJEU judgement as a violation of the EU’s market access commitments.

Next, Section 2.3 concludes that the scope of the general exception contained in GATS Article XIV(c)(ii) – perhaps the most important legal mechanism to accommodate the EU’s autonomy to adopt and maintain rules that would otherwise be inconsistent with its GATS commitments – may not be broad enough to justify the EU’s restrictions on transfers of personal data outside the EEA. The main reason for that insufficiency is that these restrictions are unlikely to pass the necessity test (referred to as the ‘trade necessity test’ in this thesis), which lies at the core of this exception. The trade necessity test requires, in particular, that a GATS-inconsistent trade-restrictive measure be the least trade restrictive of all reasonably available measures to achieve the level of protection of the public interest at stake. Relying on existing WTO case law, the thesis concludes that there are at least two reasons for the tension.

First, within the ‘range of degrees of necessity’ in WTO caselaw, the nexus between the existing EU framework for transfers of personal data – specifically the adequacy requirement – and the underlying purpose of ensuring a high level of protection of personal
data, is closer to ‘making a contribution’ rather than ‘indispensable’. The sizeable gap between what the EU framework for transfers of personal data outside the EEA should and can deliver makes it far from clear that it would pass the necessity test of the general exception in trade agreements.

Second, the EU’s restrictions on transfers of personal data are among the most restrictive in the world. Against the backdrop of the weaknesses that the EU framework for transfers of personal data contains (elaborated upon in greater detail in Section 5.3), one could argue that other approaches to personal data transfers could be ‘reasonably available’ to the EU to achieve the same level of protection. Such other approaches could, for example, include the OECD and the APEC frameworks or the framework codified in Convention 108+. This argument is, however, only valid if the same level of protection is viewed as that actually achieved by the current framework as opposed to the desired level of protection in the light of the EU Charter.

The thesis then flips the analysis by looking at it from the perspective of the EU Charter, which requires that rules, including international agreements and interfering with the fundamental rights to privacy and the protection of personal data, should be least restrictive of such rights. While international trade law starts from the premise that cross-border data flows should be allowed, the EU Charter instead posits that those data flows outside the EEA should be conditionally restricted. As a result, should a WTO adjudicating body find EU restrictions inconsistent with the GATS and unable to be justified under the general exception, compliance with such a decision could be inconsistent with the necessity test under Article 52(1) of the EU Charter. This provision sets constitutional limits on the extent to which the EU institutions can derogate from the fundamental rights, including the rights to privacy and the protection of personal data. Although the EU Charter does not establish any hierarchy between fundamental rights, in a line of cases (that includes most notably Volker und Markus Schecke, Digital Rights Ireland, Tele 2, Schrems I, Opinion on EU-Canada PNR Agreement and, most recently, Schrems II), the CJEU has elevated the EU Charter necessity test to the level of ‘strict necessity’ in relation to derogations from the fundamental rights to privacy and the protection of personal data. Relaxing restrictions on transfers of personal data to the extent consistent with the requirement of being the least trade restrictive is unlikely to pass the strict necessity test under the EU Charter. In other words, international trade obligations governing cross-border data flows may require the EU to derogate from these fundamental rights further than it is allowed within its own constitutional boundaries. Facing the choice of violating its trade obligations or the EU Charter, the EU may find itself in a catch-22 compliance deadlock.

Although in the hierarchy of EU law, the EU Charter, as primary EU law, is situated above international trade agreements, this does not make international trade law less binding on the EU. From an international law perspective, the EU must perform its
international trade obligations in good faith and may face liability and retaliation for failing to do so. This is why constitutional restrictions on compliance with trade obligations or decisions of trade adjudicating bodies could present a serious problem, especially in the context of international trade negotiations of future trade agreements, for at least two reasons. First, the TFEU requires that in the course of international trade negotiations the EU institutions must ensure compatibility of any trade agreements with the internal EU policies and rules. Failure to do so may result in a CJEU judgement under Article 218(11) TFEU, finding that a prospective trade agreement is inconsistent with the EU acquis and ultimately requiring EU institutions to renegotiate a (part) of the agreement. Second, the EU’s rhetoric in trade policy discourse, which is that personal data and privacy cannot be traded, is an important internal political message. An attempt to negotiate an exception for privacy and data protection that could potentially undermine the EU’s domestic framework safeguarding such protection is likely to be opposed by the European Parliament, both during the negotiations and the actual legislative process. Therefore, to alleviate the possible tension between the trade and EU Charter necessity tests, this thesis has concluded that, from a trade law perspective, the EU’s future trade agreements containing more elaborate provisions governing cross-border data flows should not replicate the general exception for privacy and data protection from GATS Article XIV.

2. It is not possible to strike the right balance between domestic data privacy protection and liberalisation of digital trade by just ruling out ‘protectionism’. Where the line should be drawn between legitimate protection and protectionism is strongly influenced by the discourse governing policy conversations on domestic privacy and the protection of personal data in the context of international trade. Therefore it is crucial for the EU to frame future digital trade negotiations in terms of pluralist – as opposed to purely economic – discourse. Under the narrow, effects-based definition of ‘protectionism’ generated by neoliberal discourse on international trade, EU restrictions on transfers of personal data outside the EEA can be viewed as protectionist. A broader, pluralist discourse is necessary to allow the EU to strike the right balance between globalisation, democratic politics, and the domestic autonomy to pursue domestic values such as the fundamental rights to privacy and data protection.

Before diving into the discussion of the ways in which to reform the exception for privacy and data protection in future trade agreements in Chapter 4, in Chapter 3 the thesis takes a step back and offers a bird’s eye perspective on the dynamics of international trade reforms through trade negotiations and the interpretation of trade rules by adjudicating bodies. Informed by established methods of discourse analysis, Section 3.2 demonstrates the role of discourse in the redefinition of ‘protectionism’ in trade negotiations and in the interpretation of trade rules throughout the history of the development of the international
trading system. It explicates that the term ‘protectionism’ is not endowed with a specific meaning, and shows that its definition is, to a large extent, a product of discourse. Against this backdrop, Section 3.3 juxtaposes the digital trade discourses of the EU and the US and shows how the meaning of what these trading partners label as ‘digital protectionism’ differs depending on the values underlying each discourse. Using the economics-based ‘digital trade’ discourse advanced by the US, this section demonstrates how ‘digital protectionism’ and similar terms that are often used to label restrictive data protection regimes, trigger a fundamental redefinition of what constitutes a barrier to trade and, thus, pushes towards deeper trade liberalisation and favours the deregulation of personal data transfers. Furthermore, Section 3.4 of the thesis concludes that the value structures attending the discourse ultimately predetermine where the line will be drawn between legitimate privacy and personal data protection, and illegitimate protectionism – both in the relevant provisions of international trade agreements and in the interpretation of such provisions by trade adjudicating bodies. Exposing the limitations of the dominant economic discourse when it comes to protection of privacy and personal data as fundamental rights, the thesis highlights the importance for the EU of maintaining a pluralist discourse.

Ultimately, the definitional distinction between privacy and personal data protection and protectionism is in part a moral question, that is, it should not be viewed just as a question of economic efficiency. Therefore, when a policy conversation, such as the one on cross-border flows of personal data, involves non-economic spill-over effects to individual rights, such conversation should not be confined within the straightjacket of trade economics, but rather placed in a broader normative perspective.

From a global perspective, the thesis concludes that a consensus on discourse and its underlying values is likely to be essential for the success of ongoing multilateral trade negotiations. This discourse should be defined on the basis of the goals of international trade for the twenty-first century and how far domestic regimes are willing to let trade rules interfere in their autonomy to protect their societal, cultural and political values. What actually constitutes ‘protectionism’ should be defined based on the outcome of this discussion.

3. The trade law model clauses on cross-border data flows and the protection of personal data and privacy proposed by the EU do not allow the EU to strike the right balance between fundamental rights protection and the EU digital trade policy objectives. These clauses, however, do allow the EU to fully safeguard its autonomy to protect privacy and personal data as fundamental rights. They also send a clear message to the public about the EU’s commitment to do so. Nevertheless, these clauses are unlikely to fulfil the EU’s ambition to liberalise the flows of data into the EU and
maintain a multilateral rules-based trading system. One of important ways to improve the clauses is to replace the threshold ‘it deems appropriate’, contained in the proposed exception for privacy and data protection, with a standard of non-circumvention, non-avoidance or reasonableness. When implemented in trade agreements, these standards should be complemented by restrictive mechanisms imposing checks and balances on trade adjudicators’ powers of interpretation.

As this thesis concludes in Chapter 2, the exception for privacy and data protection in the EU’s future trade agreements requires a lower threshold than the necessity test in the GATS general exception. In an attempt to design such a new exception, in 2018 the EU proposed model clauses for its prospective digital trade agreements, which included a provision on cross-border data flows and an exception for the protection of privacy and personal data (the ‘digital trade exception’). These clauses are a part of the current EU’s digital trade policy aiming, in particular, at removing ‘protectionist’ restrictions on cross-border data flows from other countries into the EU. As a part of its general trade policy, the EU promotes multilateralism and a rules-based global trading system.

The provision on cross-border data flows prohibits an enumerated list of restrictions on such flows. None of these prohibitions is likely to affect the EU’s own restrictions on transfers of personal data outside the EEA under the GDPR. The digital trade exception includes a subjective ‘it deems appropriate’ test – modelled after the ‘it considers necessary’ test of the national security exceptions in the WTO Agreements (for example, Article XXI GATT and Article XIVbis GATS). That is the broadest of all current exceptions in international trade law. If one were to put the trade necessity test and the ‘it deems appropriate’ test on a continuum, from most restrictive to least restrictive thresholds for domestic autonomy in international trade, they would be at the opposite ends of such a continuum.

Chapter 4 of this thesis concludes that the proposed model clauses suffer from at least three weaknesses and should be improved. As a result, they do not allow the EU to reconcile fundamental rights protection with its digital trade policy, while promoting a rules-based trading system. First, the material scope of the proposed digital trade exception is uncertain due to unclear relationship between this exception and the general exception for privacy and data protection, which is simultaneously included in the EU proposals for trade agreements. The best way to address this concern would be to replace the two separate exceptions with a consolidated one that would apply throughout the trade agreement. However, this may be hard to achieve in practice due to the high costs of renegotiating the general exception, and its ‘legacy clout’. Therefore, as a minimum, the relationship between the two exceptions should be clarified.
Second, modelling the threshold for the proposed digital trade exception on the national security exception is undesirable. Because the prohibitions on cross-border data flows are targeted at the EU’s trading partners, it is these partners – and not the EU itself – who are most likely to invoke the digital trade exception. The breadth of the ‘it deems appropriate’ threshold, on which this exception is based, can justify almost any derogation from a prohibition of restrictions on data flows. As a result, it may undermine the EU’s trade policy objective of removing restrictions on cross-border data flows abroad. In addition, including such a low threshold (until now reserved only for national security interests that are vital for any state) in an exception for privacy and data protection, on the one hand, puts the latter policy objectives on par with national security and above other policy objectives that still fall under the general exception (for example, public health). This creates an incentive to frame a broader set of policy objectives as privacy and data protection to escape international trade law disciplines. On the other hand, this also opens the door for using the same low threshold in other exceptions in the future. Ultimately, including such a low threshold in the digital trade exception may contribute to further undermining of the international rules-based trading system. Therefore, the proposed digital trade exception should be based on a different threshold – somewhere in between an overly broad ‘it deems appropriate’ test, and an overly restrictive ‘necessity’ test.

Based on an in-depth analysis of academic literature and the WTO case law concerning other thresholds used in WTO agreements to balance trade liberalisation against other public policy objectives, Chapter 4 of this thesis concludes that a ‘non-circumvention’, ‘non-avoidance’, or ‘reasonableness’ threshold would be a better option than the ‘it deems appropriate’ threshold proposed in the digital trade exception. All of these thresholds are interpreted by recourse to the principle of good faith and the prohibition of abuse of right, which preserves the flexibility of the ‘it deems appropriate’ test but acts as a counterweight to the almost unrestricted nature of the latter. To control for the drawbacks that come with the flexibility of those principles, the use of any of these thresholds should be complemented by restrictive mechanisms, such as institutional controls already implemented in the Understanding on the interpretation of the prudential carve-out in CETA. In particular, this mechanism requires involving competent domestic authorities in the adjudicating process and deferring to their opinion on the interpretation of relevant concepts.

Third, and finally, the proposed digital trade exception requires the EU’s trading partners to recognise the protection of privacy and personal data as fundamental rights. Given that not all EU trading partners assign the same importance to these policy objectives, this provision is EU-centric. This thesis has proposed to rephrase this provision in a way that would allow the EU to maintain its high level of privacy and personal data
protection as fundamental rights while allowing other parties to adopt a lower level of protection if they so choose.

4. Some form of restrictions on transfers of personal data outside the EEA constitutes a part of the essence of the fundamental rights to privacy and the protection of personal data under the EU Charter. However, the actual design of the framework for such transfers is not a part of such essence. Although Article 52(1) of the EU Charter places some constraints on the EU legislator, the latter has sufficient flexibility to reform the GDPR rules governing transfers of personal data outside the EEA. This is necessary in order to make those rules more scalable and apt for performing their constitutional function of preventing the circumvention of ‘effective and complete’ protection of the fundamental rights to privacy and the protection of personal data in the EU. The thesis proposes three lines of thought for accomplishing this reform corresponding to a short, medium, and long term strategy.

Section 5.2 concludes that the EU Charter, as EU primary law, and the GDPR, as EU secondary law, are in a dynamic relationship with each other. While the GDPR has been adopted to effectuate the fundamental right to the protection of personal data (and other rights enabled by it), interpretation of its rules and the rules of the 1995 Data Protection Directive has informed the constitutional content of that fundamental right. To illustrate the point, from a mere constitutional interpretation of the secondary law concept of ‘adequacy’, the standard of ‘essential equivalence’ has become the constitutional benchmark and an instantiation of the strict necessity and proportionality requirements under Article 52(1) of the EU Charter in respect of the whole secondary law framework on transfers of personal data outside the EEA.

Next, Section 5.2 concludes that restrictions on transfers of personal data per se constitute a part of the essence of the fundamental rights to privacy and the protection of personal data, as their complete absence allows these rights to be easily circumvented and deprives them of their content. However, the particular design of those restrictions, as well as the standard of ‘essential equivalence’ setting constitutional boundaries on such a design, do not constitute a part of the essence of the above-mentioned fundamental rights. Based on the current CJEU case law, Section 5.2 argues that in order to respect the essence of the fundamental rights to privacy and the protection of personal data, the EU secondary law framework for transfers of personal data outside the EEA must incorporate the following elements:

• provide for some limitations on transfers of personal data outside the EEA and on onward transfers,

• contain safeguards preventing generalised access of foreign authorities to the content of electronic communications,
• ensure that purposes for processing personal data are limited,
• require that the processing of personal data is accompanied by rules designed to ensure, inter alia, the security, confidentiality and integrity of the data, and also to protect them against unlawful access and processing,
• not permit retention of the content of communications, and
• provide for some possibility for an individual to pursue legal remedies in order to have access to personal data relating to him or her, or to obtain the rectification or erasure of such data.

Using the constitutional function of the EU rules for transfers of personal data to prevent the circumvention of the ‘effective and complete’ protection of privacy and personal data in the EU, Section 5.3 identifies several weaknesses of those rules. These weaknesses are put in the context of broader political, societal and technological changes between 1995 (when those rules were first adopted) and 2020. First, this thesis argues that the CJEU Schrems II judgement has reinstated – on the books – the logical consistency of the tools for systematic transfers of personal data: the adequacy mechanisms, and appropriate safeguards under Article 46 of the GDPR, such as the SCCs and the BCRs. However, in practice, this judgement would either lead to the increased localisation of personal data in the EEA or to a fairly low level of compliance - on the ground. The problem is that, as a matter of fact, data will continue flowing across borders. At the same time, (most) companies have insufficient expertise and resources to ensure that all personal data transferred on the basis of appropriate safeguards is safeguarded the level of protection abroad that is essentially equivalent to the protection in the EU. Furthermore, the DPAs have neither the financial nor the human resources to monitor such compliance. If individuals resort to private enforcement, including mass claims, to compensate for lack of public enforcement – which is increasingly the case – interpretation of the ‘essential equivalence’ standard in relation to transfers of personal data to various third countries by different EU member states courts is likely to lead to a fragmentation of the EU regime for transfers of personal data. Section 5.3, therefore, argues that the problem of foreign surveillance, which lies at the core of this issue, should rather be addressed by the EU and its trading partners in an international forum, which should not coincide with international trade negotiations.

Second, the thesis argues that the adequacy framework itself suffers from political pressures as well as from what the thesis has called the ‘snapshot’, the ‘heavy burden’, and the ‘onward transfer’ problems. Third, and more generally, the thesis contends that the EU framework for transfers of personal data outside the EEA lacks granularity in the sense that the same rules apply irrespective of the context, volume and type of data transferred, and other parameters of data transfers. In a world where massive volumes of various kinds of
personal data are transferred every second, it is unrealistic to expect that the stringent EU framework under Chapter V of the GDPR will be fully observed, and most importantly, monitored and enforced by authorities in all those transfers.

Section 5.4 suggests and elaborates upon three possible lines of thought on how to improve the current GDPR framework for transfers of personal data outside the EEA. The first, and the most moderate, line of thought proposes to improve *specific* elements of mechanisms for transfers of personal data, without changing the design and composition of the framework. In particular, it proposes:

1. to adopt a transparent procedure governing adequacy assessment to address proneness of adequacy mechanism to political influence;
2. to transition adequacy assessments from a unilateral instrument to a reciprocal agreement, under which the foreign country would undertake certain obligations, such as to notify about any changes in legislation considered during the adequacy assessments, and to accept negative consequences of the failure to notify;
3. to ensure that onward transfer mechanisms in adequacy decisions, as much as possible, mirror the appropriate safeguards provided for in the GDPR and as interpreted by the CJEU in *Schrems II*. Consent should not be allowed as a legal ground for systematic onward transfers;
4. to reform the SCCs to meet the GDPR standards and to issue practical guidance on additional measures that could be taken to compensate for absence of ‘essentially equivalent’ protection of personal data in third countries that have not been afforded an adequacy decision.

The second, intermediate, line of thought proposes to add greater scalability to the framework while improving its particularities. It requires a more substantial revision of the GDPR and, therefore, could realistically be addressed only in the medium term – for example, in the next review of the GDPR’s Chapter V under Article 97 GDPR in 2024. In addition to the reform proposals outlined in the first line of thought, the second line of thought proposes two principle adjustments to Chapter V of the GDPR:

1. introducing more lenient rules for transfers of personal data in relation to pseudonymised data, with the exception of pseudonymised sensitive data, and data in transit; and
2. giving legal significance in Chapter V of the GDPR to technological means for protection of personal data, including as a means of ensuring that pseudonymised data will not be re-identified after the transfer.

The third, long term, line of thought proposes a more fundamental redesign of the EU framework for transfers of personal data. One way of doing so would be to replace the
current one-size-fits-all approach, in which different mechanisms for transfers of personal data do not take into account the context and the parameters of the transfer, with rules designed on a risk-based approach, which is already implemented in some GDPR provisions. In the light of the constitutional function of the EU framework for transfers of personal data, as mentioned above, the main risk that the redesigned framework should address is the circumvention of the ‘effective and complete’ protection of privacy and personal data protection that the EU affords, when personal data is transferred abroad. Reformulating this in fundamental rights term, it is a risk that transfers of personal data outside the EEA can interfere with the fundamental rights to privacy and the protection of personal data more than is strictly necessary and proportionate to pursue a legitimate public policy objective. Safeguards required for transfers of personal data could be differentiated depending on the remoteness of link between personal data and the individuals to which it relates or, in other words, on the risk of the reidentification of individuals and threat of harm to their fundamental rights.

**Avenues for further research**

This thesis has aimed to demonstrate the need to reform the EU framework for transfers of personal data outside the EEA in Chapter V of the GDPR, and situated it within the context of international trade law and the reform of trade law, including the EU’s proposed model clauses for future trade agreements. In the case of the GDPR, an effort based on a host of both domestic and international factors that goes well beyond this work, is needed to design a fully-fledged reform proposal.

Beyond strictly legal questions, cross-border transfers of personal and other data also raise questions of social justice, especially in the context of using personal data to develop, fine-tune, and regulate the use of AI systems. So far, privacy and data protection are the only policy objectives that are juxtaposed with those of digital trade liberalisation in EU digital trade discourse. However, in designing exceptions from data flow provisions, questions of who benefits and who loses from data flows should also be considered, especially in a multilateral setting. Put simply, research is necessary to explore how distributional issues should be incorporated in the design of digital trade provisions.

Finally, national security interests are increasingly taking centerstage in governments’ policy on data flows and trade policy. This topic has four dimensions. First, national security concerns lead some governments, like the United States, to restrict transfers of personal data to non-democratic countries like China, viewing such transfers as a national security threat. Second, the United States’ national security programmes, which allow the US authorities to access Europeans’ data for national security purposes, recently led the CJEU to invalidate the most commonly-used mechanism for transfers of personal data to the United States – the EU – US Privacy Shield (*Schrems II* judgment).
Similarly (albeit for different reasons), as mentioned in Section 5.4, DPAs across Europe are investigating TikTok’s data processing practices in Europe, and specifically transfers of personal data to China. Third, as recently confirmed by the CJEU in the *Schrems II* and *Privacy International* cases, the EU Charter guarantees under Articles 7 and 8 apply to rules governing surveillance authorities’ access to personal data for national security purposes, when such data is obtained by authorities from private parties (such as telecommunication services providers or platforms), both under EU member states law and the law of foreign states receiving personal data from the EEA. Fourth, the national security exception plays a special role in international trade agreements due to its breadth, and it has been invoked recently by countries trying to derogate from their trade commitments for reasons only marginally related to national security. Furthermore, as discussed in Chapter 4, the US has broadened the national security exception in its digital trade agreements by removing the factual circumstances in which it can be invoked, present in the WTO exception, thus removing an important objective constraint on the invocation of the exception. At the same time, cross-border data flows are increasingly regulated by international trade agreements, which means that, in a trade setting, countries could potentially invoke a national security exception to restrict data flows as well. As a result, there is a tension between the tendency, on the one hand, to keep the national security exception as broad as possible due to the quintessential importance of national security for the very existence of the states and, on the other hand, to use the national security exception as a means to derogate from the increasingly broader scope of trade commitments on the grounds unrelated to traditional security interests. This tension will either lead to the narrowing of the regulatory autonomy of states to invoke national security, or erode the foundations of the rule-based multilateral trading system. Using the issue of cross-border data flows as a case study to demonstrate how national security concerns can drive countries towards imposing data localisation, further research is needed to consider whether a reform of the national security exception in trade agreements is necessary. This research could also include finding an international law solution to the problem of foreign surveillance authorities’ access to personal data from companies that received such data in the course of conducting business.
References

Secondary sources


Beattie, A. (2017). EU Trade Data Flows Are Becoming the New GMOs, *Financial Times*, retrieved from https://www.ft.com/content/9da22968-d8ee-11e7-a039-c64b1c09b482


Tene, O. (2020a). GDPR’s Second Anniversary: A Cause for Celebration — and Concern. *International Association of Privacy Professionals*. Retrieved from https://iapp.org/news/a/gdprs-second-anniversary-a-cause-for-celebration-and-concern/?mktt_tok=eyJpIjoiTmJmQXNzV2QzNjVtZ2FoYzAzMmJiZmY4MjE2NzYxN2EiLCJpbGciOiJjb2RlZ3JvdXJkYXRlIiwiczI6IjY1NzUxMDI0MiIsIml2IjoiMTg1MjQ5Mzc2NjI0NTk1ODc1LTAxMDcyMDk2MDE0OTY5LTA1MzQ5OTE5NjUifQ==


Primary Sources

Legal Texts

International Treaties and Conventions


Dominican Republic-Central America-US FTA: Dominican Republic-Central America-United States Free Trade Agreement, 28 May 2004, 43 I.L.M. 514


EU Schedule of Specific Commitments: European Communities and Their Member States, Schedule of Specific Commitments, Supplement 4, Revision, 18 November 1999, GATS/SC/31/Suppl.4/Rev.1.

EU-Central America Association Agreement: Agreement Establishing an Association between Central America, on the one hand, and the European Union and its Member States, on the other, 29 June 2012 [2012] OJ L 346/3


GATS Annex on Financial Services


KORUS: United States-Korea Free Trade Agreement, 1 April 2007, 46 I.L.M. 642


US – Panama TPA: United States-Panama Trade Promotion Agreement, 31 October 2012


US-Chile FTA: United States-Chile Free Trade Agreement, U.S.-Chile, 6 June 2003, KAV 6375


US-Japan Digital Trade Agreement: Agreement between the United States of America and Japan Concerning Digital Trade, 7 October 2019,


Proposed International Agreements


Modernised EU-Chile Association Agreement: EU proposal for a Digital trade title in the Trade Part of a possible modernised EU-Chile Association Agreement, 5


Council of Europe


European Union: Treaties and Charter


European Union: Regulations and Directives


European Union: Proposed Legislation


Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), /*
COM/2012/011 final - 2012/0011 (COD)

European Commission Implementing Decisions: Adequacy Decisions


European Parliament

Committee on Civil Liberties, Justice and Home Affairs, Report on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs. No 2013/2188(INI), 21 February 2014.

European Parliament Resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs 2013/2188(INI)).

European Parliament resolution of 8 July 2015 containing the European Parliament’s recommendations to the European Commission on the negotiations for the Transatlantic Trade and Investment Partnership (TTIP) (2014/2228(INI)).

European Parliament resolution of 3 February 2016 containing the European Parliament’s recommendations to the Commission on the negotiations for the Trade in Services Agreement (TiSA) (2015/2233(INI)).

European Parliament Resolution of 26 May 2016 on transatlantic data flows (2016/2727(RSP)).

European Parliament resolution of 13 December 2018 on the adequacy of the protection of personal data afforded by Japan (2018/2979(RSP)).
EU Council Decisions

EU Member States National Legislation
The Netherlands: Parliamentary Documents
Initiatiefnota van het lid Verhoeven over mededinging in de digitale economie; Motie van het lid Buitenweg c.s. over vormgeving van data trusts in Nederland, 16 december 2019, KST351347, 35134, nr. 7.

Foreign legislation
Russia
Федеральный закон ‘О персональных данных’ от 27.07.2006 N 152-ФЗ (Federal Law on Personal Data of 27 July 2006 No. 152-FZ)

China

Canada
PIPEDA: Personal Information Protection and Electronic Documents Act of 13 April 2000 (S.C. 2000, c. 5)

Official Documents
United Nations
Guidelines for the Regulation of Computerized Personal Data Files, adopted by General Assembly resolution 45/95 of 14 December 1990.
Personal Data Protection and Privacy Principles, Adopted by the UN High-Level Committee on Management (HLCM) at its 36th Meeting on 11 October 2018.

Organisation for Economic Co-operation and Development (OECD)
Asia-Pacific Economic Cooperation (APEC)


World Trade Organization (WTO)

Background Note by the Secretariat, Financial Services, S/C/W/312, S/FIN/W/73, 3 February 2010.

Dispute Settlement Body, Minutes of Meeting, WT/DSB/M/24, 16 October 1996.


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.


Note by Secretariat, ‘Necessity tests’ in the WTO, S/WPDR/W/27, 2 December 2003


Request for the Establishment of a Panel by the European Communities, United States – The Cuban Liberty And Democratic Solidarity Act. WT/DS38/2, 8 October 1996.


General Agreement on Tariffs and Trade (GATT)


European Union

European Commission


Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, A New Industrial Strategy for Europe, COM/2020/102 final, 10 March 2020.

Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, Strengthening the Rule of Law Within the Union. A Blueprint for Action, COM/2019/343 final, 17 July 2019.


Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, A European Strategy for Data, COM(2020) 66 final, 19 February 2020.

Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of
the Regions, Trade for All Towards a More Responsible Trade and Investment Policy, COM/2015/0497 final, 14 October 2015.


Standard contractual clauses (Set I) for controller to controller transfers: Commission Decision 2001/497/EC of 15 June 2001 on Standard Contractual

Standard contractual clauses (Set II) for controller to controller transfers:


Council of the European Union
Concept paper on data flows in trade agreements, 28 January 2017 (on file with author).

Council of Europe


Article 29 Working Party
Guidelines on Personal data breach notification under Regulation 2016/679, WP250rev.01, 6 February 2018.
Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision, WP 238, 13 April 2016.
Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes, WP 215, 10 April 2014.
Opinion 11/2011 on the level of protection of personal data in New Zealand, WP 182, 4 April 2011.


Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees), WP 237, 13 April 2016.

Working document on Adequacy Referential, WP 254rev.01, 6 February 2018.


Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, WP 256 rev.01, 6 February 2018.

Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules, WP 257 rev.01, 6 February 2018.

European Data Protection Board (EDPB)

Agenda of the 40th EDPB meeting, 20 October 2020.

Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 - Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems, 23 July 2020.


Press Release, Thirty-first Plenary session: Establishment of a taskforce on TikTok, Response to MEPs on use of Clearview AI by law enforcement authorities, Response to ENISA Advisory Group, Response to Open Letter NYOB, 10 June 2020.

Contribution of the EDPB to the evaluation of the GDPR under Article 97, Adopted on 18 February 2020.


Guidelines 1/2018 on certification and identifying certification criteria in accordance with arts 42 and 43 of the Regulation, including Annex 2, 4 June 2019.


Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), 16 November 2018, version 1.0, for publication consultation.

**European Data Protection Supervisor (EDPS)**


Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data, 19 December 2019.


Opinion 4/2016 on the EU-U.S. Privacy Shield draft adequacy decision, 30 May 2016.

Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content.

**National Data Protection Authorities**

**Netherlands**


**Germany**


**Foreign Data Protection Authorities**

**Canada**


United States Trade Representative

Case Law

Alphabetically ordered. When available, citations refer to the European Case Law Identifier (ECLI)

Court of Justice of the European Union (CJEU): Judgements


**Digital Rights Ireland:** Judgment of 8 April 2014, Digital Rights Ireland and Seitlinger and others (C-293/12 and C-594/12) ECLI:EU:C:2014:238.

**Google Spain:** Judgment of 13 May 2014, Google Spain and Google (C-131/12) ECLI:EU:C:2014:317.

**Schrems I:** Judgment of 6 October 2015, Schrems (C-362/14) ECLI:EU:C:2015:650

**Tele2 Sverige:** Judgment of 21 December 2016, Tele2 Sverige (C-203/15 and C-698/15) ECLI:EU:C:2016:970.

**Nowak:** Judgment of 20 December 2017, Nowak (C-434/16) ECLI:EU:C:2017:994


**Jehovan todistajat:** Judgment of 10 July 2018, Jehovan todistajat (C-25/17) ECLI:EU:C:2018:551.

**Fashion ID:** Judgment of 29 July 2019, Fashion ID (C-40/17) ECLI:EU:C:2019:629.


**Schrems II:** Judgment of 16 July 2020, Facebook Ireland and Schrems (C-311/18) ECLI:EU:C:2020:559.

**Opinion on EU-Canada PNR Agreement:** Opinion 1/15 (EU-Canada PNR Agreement), of 26 July 2017 (Digital Reports) ECLI:EU:C:2017:592.


**La Quadrature du Net and others:** Judgment of 6 October 2020, La Quadrature du Net and others (C-511/18, C-512/18 and C-520/18) ECLI:EU:C:2020:791.

**Court of Justice of the European Union (CJEU): Advocate General (AG) Opinions**

**Opinion AG in Schrems II:** Opinion of Advocate General Saugmandsgaard Øe delivered on 19 December 2019, Case C-311/18, Facebook Ireland and Schrems, ECLI:EU:C:2019:1145.


**European Court of Human Rights (ECtHR)**

**Big Brother Watch and others v. United Kingdom.** Applications nos. 58170/13, 62322/14 and 24960/15, Judgement of 13 September 2018 (under review of the Grand Chamber).

World Trade Organization (WTO)


Australia – Tobacco Plain Packaging (Honduras and Dominican Republic): Appellate Body Report, Australia – Certain Measures concerning Trademarks, Geographical Indications and other Plain Packaging Requirements applicable to Tobacco Products and Packaging, WT/DS435/AB/R, WT/DS441/AB/R and Add.1, adopted 29 June 2020


General Agreement on Tariffs and Trade (GATT)


International Centre for Settlement of Investment Disputes

National Cases

Germany


Ireland

Irish High Court (Commercial), The Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems 2016 No. 4809 P., 3 October 2017.

Electronic Sources


EUROPEAN ESSENTIAL GUARANTEES GUIDE, https://www.essentialguarantees.com/


OXFORD ENGLISH DICTIONARY ONLINE, *deem*,

OXFORD ENGLISH DICTIONARY ONLINE, *necessary*,

TRANSPARENCY REGISTER,

UNCTAD, *Data Protection and Privacy Legislation Worldwide*,

WORLD TRADE ORGANIZATION, *Financial Services*,

WORLD TRADE ORGANIZATION, *Regional Trade Agreements*,
Short Summary

GOVERNING CROSS-BORDER DATA FLOWS:
RECONCILING EU DATA PROTECTION AND INTERNATIONAL TRADE LAW

This thesis explores the difficulty of reconciling two important legal and policy objectives of the European Union. On the one hand, the EU Charter of Fundamental Rights (EU Charter) guarantees the protection of the rights to privacy and the protection of personal data as fundamental rights. On the other hand, in its external trade policy the EU seeks to liberalise cross-border data flows and to maintain and further develop a globally binding rules-based trading system that ensures appropriate access to foreign markets for EU businesses. Until recently in EU external policy, the two objectives had little in common and, therefore, did not come into conflict. In recent years, however, as cross-border flows of personal and other data have become ‘the lifeblood of international trade’, those conflicts have now emerged. Indeed, the area of digital commerce is taking up a growing share of world trade. Yet the collection and commercial use of personal data also implicates essential noneconomic values. Those values explain why personal data is protected by the EU Charter, and why it was instantiated with a high degree of specificity by the General Data Protection Regulation (GDPR). The thesis examines how these two objectives may be pursued simultaneously.

Although individuals can gain from the free flow and ubiquitous monetisation of their data by companies – for example, in the form of personalised services – they also have a lot to lose. From a global perspective, massive cross-border appropriation of personal data has been compared to resource extraction. Potential damage to individuals, and to society as a whole, far transcends the direct economic losses suffered from data breaches and identity threats.

Since 2009, the right to the protection of personal data has been a binding fundamental right in the EU, that is, separate from the (also fundamental) right to privacy. Just as personal data has both economic and societal value, the European data protection regime has a dual objective: protecting the fundamental rights and freedoms of individuals (in particular their right to the protection of personal data), and ensuring the free flow of personal data within the European Economic Area (EEA). However, the constitutionalisation of the EU has brought the non-economic goals of current European data protection law to the fore, placing them ahead of economic needs. Recently, robust protection of the fundamental rights to privacy and personal data has formed part of the EU response to growing concerns about technological or digital sovereignty with regard to the growing economic and social influence of non-EU (primarily American) technology companies.
There is a countervailing view that domestic restrictions on international data flows in general, and on personal data flows in particular, are a form of undesirable ‘protectionism’. That view is now front and centre in academic, public and policy conversations on the topic, as the focus of international trade negotiations shift to digital trade. The push for international trade law to liberalise international flows of personal and other data is seen as being at odds with legal regimes that restrict such flows on privacy and data protection grounds, especially that of the European Union. Unlike the internal trade liberalisation within the EU single market (which led to the emergence of the EU data protection framework in the past), the EU’s external trade liberalisation goal is in tension with the EU data privacy law, due to their opposite normative valences.

The World Trade Organization (WTO) is the main body administering international trade rules. Both the EU and its member states are WTO members. However, the WTO’s role has recently decreased due to political circumstances and the multiplication of regional and bilateral trade agreements. So-called ‘new generation’ free trade (such as the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), the United States–Mexico–Canada Agreement (USMCA) and the US-Japan Digital Trade Agreement), entered into by the EU’s most important trading partners, such as Canada, Japan and the US, include provisions obliging parties to allow free cross-border flows of information, including personal data. Cross-border data flows are also high on the agenda in the recently launched negotiations on e-commerce at the WTO.

The elimination of restrictions on data flows has been one of the most contentious issues in many recent trade negotiations in Asia, Europe, and North America. With the international trade regime increasingly moving towards ‘free’ digital trade, and the Court of Justice of the European Union (CJEU) asserting the protection of EU fundamental rights as a pre-requisite for such transfers, this thesis argues that the risk that the EU’s commitment to liberalising the cross-border movement of services under the General Agreement on Trade in Services (GATS), on the one hand, and to the protection of the fundamental right to the protection of personal data, on the other hand, will clash is very real. This clash is not in and of itself a reason to cry foul. Both the EU Charter and international trade law contain exceptions that allow each system to tolerate encroachments on their respective rules by the other, within certain limits. The majority of international trade agreements, including the GATS, provide for a so-called ‘general exception’. This exception preserves the regulatory autonomy of parties to an international trade agreement and enables them to adopt and maintain measures ‘necessary’ to protect the privacy of individuals in relation to the processing and dissemination of personal data, even if such measures run counter to the member’s international commitments (the trade necessity test). Article 52(2) of the EU Charter, in turn, allows the EU to limit fundamental rights if this is ‘necessary’ to meet objectives of general interest to the EU or to protect the rights and
freedoms of others (the EU Charter necessity test). However, as this thesis argues in Chapter 2, the trade necessity test, as interpreted by the WTO adjudicating bodies, could be insufficient to safeguard the EU’s autonomy to protect the fundamental right to data privacy under the EU Charter.

In 2018, in search of a better alternative, the EU developed horizontal provisions on cross-border data flows and the protection of privacy and personal data for its prospective digital trade agreements. The EU has tabled these model clauses in digital trade negotiations with its trading partners ever since (for example, with Australia, Indonesia, New Zealand, Tunisia and the UK), and included them in the EU proposal for the WTO rules on electronic commerce. The EU’s proposed model clauses contain a narrower prohibition on restrictions of cross-border data flows than the US approach (which has been implemented in the CCTPP, the USMCA, and the US-Japan Digital Trade Agreement), and an exception for domestic privacy and data protection rules which is significantly broader than the above-mentioned general exception (also replicated in the US model).

Against this backdrop, the primary research question answered in this thesis is:

*how should commitments on cross-border data flows in future EU trade agreements be reconciled with the protection of the fundamental rights to privacy and personal data?*

The thesis answers the question by addressing the four sets of sub-questions, answered sequentially in Chapters 2-5.

**Chapter 2** identifies and sets out the key issue underlying this thesis: namely that of the increasing tension between the governance of cross-border transfers of personal data by EU and international trade law. It develops the argument that EU restrictions on transfers of personal data could conflict with the EU’s commitments under the GATS and post-GATS trade agreements. It contends that such restrictions are unlikely to meet the trade necessity test even in its most lenient interpretation because they arguably go beyond the limits set by the GATS provisions and the general exception for privacy and data protection. At the same time, under the strict necessity test contained in the EU Charter (as interpreted by the CJEU), the regulatory autonomy under EU law to derogate from the protection of the fundamental rights to privacy and the protection of personal data may be insufficient to comply with the EU’s international trade obligations when it comes to cross-border flows of personal data. The sequential application of the two ‘necessity tests’ creates a risk that the two ‘necessities’ may clash, putting the EU in a catch-22 compliance deadlock between the violation of trade law or unjustifiable derogation from the fundamental right to the protection of personal data, as construed by the CJEU.
In the context of the ongoing digital trade negotiations that the EU is conducting with its trading partners on cross-border data flows, privacy and data protection, this state of affairs is not sustainable. Under EU primary law, EU institutions may not negotiate international trade rules inconsistent with the EU acquis. At the same time, despite international trade agreements ranking below EU primary law in the hierarchy of EU law, the EU cannot be relieved of its international trade obligations for the sole reason that they are inconsistent with EU primary law. Therefore, the EU should be able to comply with the Charter and its international trade obligations simultaneously. The path forward suggested in this thesis, and further elaborated on in Chapters 3 and 4, is guided by three principal considerations. First, from a practical perspective, it is risky to wait until EU restrictions are struck down by – or even challenged by – an international trade adjudicating body, which would force the EU’s hand and possibly impose an unrealistic reaction timeframe. A more proactive approach seems preferable. Second, and relatedly, ongoing uncertainty surrounding the lawfulness of transfers of personal data outside the EEA, on the one hand, and compliance with the restrictions on such transfers with the EU’s international trade commitments, on the other hand, may have a chilling effect on cross-border trade to the detriment of EU businesses. Third, although the approach to transfers of personal data outside the EEA that would make the most solid contribution to the ‘effective and complete’ protection of the fundamental rights to privacy and the protection of personal data is a total ban on such transfers, this rather extreme approach would undermine the very existence of digital cross-border trade with the EU and is thus unwarranted.

Chapter 3 takes a step back and investigates what the term ‘protectionism’ entails and whether EU restrictions on transfers of personal data outside the EEA are protectionist. Applying insights from the work of Michel Foucault on the relationship between discourse and power, this Chapter demonstrates that it is not possible to strike the right balance between digital trade liberalisation and the protection of data privacy by simply ruling out ‘protectionism’. Chapter 3 also argues that the distinction between protection and protectionism is not clear-cut: the placing of the line between protection and protectionism is ultimately a judgement call. On a spectrum between the two extremes, there is a grey area that includes domestic measures, with an element of uncertainty as to what type of regulatory goal is at stake: protectionism in disguise or genuine protection, which only incidentally benefits domestic industries. Whether measures in this grey area should fall under the label of ‘protection’ or ‘protectionism’ – in other words, whether trade adjudicating bodies should err on the side of protection or protectionism – essentially depends on the discourse. Within an economic discourse, where free trade alone is high on the value scale, such regulation would be excluded as protectionist. In contrast, in a pluralist discourse where equal value is assigned to free trade and protection of
fundamental rights, allowing some mildly protectionist measures to go unchallenged in order to safeguard states’ domestic autonomy to adopt socially beneficial regulation may be a preferred approach.

Therefore, the choice of the right discourse for policy conversations on domestic privacy and the protection of personal data, in the context of negotiating and interpreting international trade law, is crucial. The value structures attending it will ultimately strongly affect where the line will be drawn between legitimate privacy and personal data protection, and illegitimate protectionism, both in the relevant provisions of international trade agreements and in the interpretation of such provisions by trade adjudicating bodies. Against this backdrop, Chapter 3 asserts that countries should be conscious of the value frameworks that come with a certain discourse and should ensure that their mutual values determine such discourse, as opposed to the other way around. This Chapter contends that the distinction between privacy and personal data protection, and protectionism is in part a moral question, that is, not just a question of economic efficiency. Therefore, when a policy conversation, such as the one on cross-border flows of personal data, involves non-economic values such as individual rights, the conversation should not be confined within the narrow field of trade economics but rather placed in a broader normative perspective.

On the subject of restrictions on cross-border flows of personal data, Chapter 3 argues that such restrictions are, and will remain, necessary. Unless approaches to data protection and privacy are harmonised, countries need more regulatory space to determine the design of domestic data protection regimes. It is precisely because data protection standards in other countries are low (perhaps strategically low) that countries with higher standards need to impose restrictions on personal data transfers.

Chapter 4 turns to the specific international trade law aspects of the problem identified in Chapter 2. It is divided into three parts. In the first part, this Chapter questions whether the model clauses on cross-border data flows and the protection of privacy and personal data, proposed by the European Commission in 2018, would allow the EU to overcome the potential catch-22 compliance deadlock in future trade agreements, while at the same time pursuing the goals of facilitating cross-border data flows and promoting a rules-based multilateral trading system. It argues that, superficially, the 2018 clauses do seem to provide the EU with the broad autonomy to protect privacy and personal data as fundamental rights while outlawing a number of measures restricting cross-border data flows. Compared to the US model, the prohibition of restrictions on cross-border data flows in the EU proposed clauses is formulated more narrowly. Furthermore, the proposed clauses assert that the normative rationale for the protection of personal data and privacy is the protection of fundamental rights. In addition, the breadth of the proposed exception for privacy and data protection (referred to as the ‘digital trade exception’), modelled after
the national security exceptions in the WTO Agreements, secures the EU’s ability to maintain restrictions on transfers of personal data outside the EEA under the GDPR. The proposed digital trade exception explicitly recognises the rules for cross-border transfers of personal data as an example of the types of measures that would be allowed under the exception.

The first part of Chapter 4 contends, however, that the proposed model clauses suffer from at least three essential flaws that could make them unable to safeguard the fundamental rights to privacy and the protection of personal data, and that undermine the goals of the EU digital trade policy, as identified above. First, the imprecise nature of the relationship between the proposed digital trade exception for privacy and data protection (intended for the digital chapters of trade agreements) and the general exception (typically included in the exceptions chapter of the same proposed trade agreements), creates legal uncertainty as to the material scope of the proposed exception. Second, the breadth of the proposed digital trade exception for privacy and data protection may nullify the impact of the proposed provision on cross-border data flows in the same model clauses. More generally, Chapter 4 argues that using the extremely low threshold of national security exceptions as a model for a digital trade exception for privacy and data protection could further undermine the stability of the rules-based international trading order. Third, the proposed model clauses are overly EU-centric in the sense that they require a recognition of the protection of privacy and personal data as fundamental rights – a commitment that not all EU trading partners may be willing to accept or implement in practice.

In the second part, Chapter 4 suggests three ways to improve the proposed model clauses. First, future trade agreements should either include a provision clarifying the relationship between the general and the digital trade exceptions for privacy and data protection, or contain a single exception for privacy and data protection which would apply throughout the agreement (acknowledging that the latter could be problematic in practice). Second, in the course of negotiations, the EU should consider replacing the ‘it deems appropriate’ threshold of the digital trade exception for privacy and data protection with a threshold which is higher than the ‘it deems appropriate’ standard but lower than the necessity test standard of the general exception. Third, the provision requiring the parties to recognise that the protection of personal data and privacy is a fundamental right should be rephrased in a way which, on the one hand, safeguards the EU’s autonomy to maintain its fundamental rights protection of these rights but, on the other hand, allows other trading partners to adopt a lower level of protection (within international human rights law bounds) if they so choose.

In the third and final part, Chapter 4 considers thresholds other than the ‘it deems appropriate’ test, that the EU could fall back on without compromising on the fundamental
rights to privacy and data protection. It looks at other alternatives found in WTO agreements and bi-lateral and regional trade agreements, that are on the continuum between the ‘necessity’ in the general exception (the current test for privacy and data protection), and the ‘it deems appropriate’ test proposed for a digital trade exception for privacy and data protection by the EU. Chapter 4 argues that the standards of non-circumvention, non-avoidance and reasonableness could be viable alternatives to the ‘it deems appropriate’ standard, provided that they are accompanied by appropriate restrictive mechanisms constraining the discretion of trade adjudicators, and are applied in a nuanced manner.

Building on the conclusions of previous chapters, Chapter 5 addresses the problem of the ‘two necessities’ identified in Chapter 2 of the thesis, from both an EU Charter and EU data protection law perspectives. The analysis in this Chapter is structured along the following three broad issues: (1) the constitutional boundaries the EU Charter imposes on EU secondary data protection law and specifically the extent to which the EU framework for transfers of personal data outside the EEA in the GDPR can be changed within such boundaries; (2) the ability of this framework to perform its constitutional function to prevent circumvention of the high level of personal data protection in the EU and, ultimately, to ensure ‘effective and complete’ protection of fundamental rights; and (3) the reform proposal for such a framework in response to changed political, geopolitical and economic circumstances.

On the first issue, Chapter 5 argues that there is a dynamic relationship between the GDPR (as a secondary EU law instrument) and the EU Charter (as a primary law instrument). At the same time, this Chapter demonstrates that the framework for transfers of personal data outside the EEA in Chapter V of the GDPR represents only one possible design of such a framework in the light of the EU Charter requirements. Only the presence of some restrictions, and a few aspects of such restrictions, constitute the essence of the fundamental rights to privacy, the protection of personal data and the right to judicial remedy (in the context of the first two rights), and therefore cannot be altered by EU secondary law. Other elements of such a framework can be determined by the EU secondary legislator on the basis of strict necessity and proportionality assessment, with the aim of ensuring its constitutional function, which is to prevent circumvention of the high level of personal data protection in the EU. The concept of ‘essential equivalence’, which, following the CJEU’s Schrems II judgement, can be seen as the constitutional benchmark for the secondary law framework on transfers of personal data, does not constitute a part of the essence of the above-mentioned fundamental rights. Instead, it governs the balancing of the above-mentioned fundamental rights against competing policy objectives: primarily the economic benefits inherent in unrestricted cross-border flows of personal data, and the national security interests of foreign countries. Chapter 5, therefore, contends that the EU legislator has sufficient wiggle room to change the design
318 of the rules currently codified in Chapter V of the GDPR.

In the second part, Chapter 5 identifies four weaknesses in the EU framework for transfers of personal data outside the EEA. The first weakness is that, despite the recent Schrems II decision, there is a persistent qualitative gap between the adequacy decisions on the one hand, and the appropriate safeguards under Article 46 of the GDPR on the other (both of which serve as mechanisms for systematic transfers). The EU should address the foreign surveillance problem – which is the main reason why issues relating to transfers of personal data land at the CJEU – on the international level rather than through its own secondary law. The second weakness is that adequacy decisions are prone to political pressures in the context of EU trade policy. The third weakness is that adequacy decisions are unable to perform their constitutional function due to lack of regular reviews of the assessment on which the adequacy decisions are based (the ‘snapshot’ problem), the difficulties of enforcing individual rights in foreign jurisdictions (the ‘heavy burden’ problem), and the inadequacy of onward transfer mechanism embedded in the adequacy decisions (the ‘onward transfer’ problem). The fourth and last weakness is, on a more abstract level, the limited scalability of the current regime for personal data transfers in Chapter V of the GDPR in view of the technological developments that have occurred since the 1990s, when the core of the framework was first designed.

In its third and final part, Chapter 5 proposes three directions of thought on how to improve the framework of Chapter V of the GDPR within the boundaries set by the EU Charter, reflecting possible short, medium, and long term strategies for the EU in this area.

The first, and most moderate, line of thought proposes to improve specific elements of mechanisms for transfers of personal data without changing the design and composition of the framework. For example, it proposes the adoption of a transparent procedure governing adequacy assessment to address the proneness of the adequacy mechanism to political influence and to transition adequacy assessments from a unilateral instrument to a reciprocal agreement. The second, intermediate, line of thought proposes adding greater scalability to the framework while improving its particularities. It requires a more substantial revision of the GDPR and, therefore, could realistically be addressed only in the medium term – for example, in the next review of the GDPR’s Chapter V under Article 97 GDPR in 2024. In addition to the reform proposals outlined in the first line of thought, the second line of thought proposes two principle adjustments to Chapter V of the GDPR: more lenient rules for transfers of non-sensitive pseudonymised data and giving legal significance to technological means for protection of personal data. The third, long term, line of thought proposes a more fundamental redesign of the EU framework for transfers of personal data. One way of doing so would be to replace the current one-size-fits-all approach, in which different mechanisms for transfers of personal data do not take into
account the context and the parameters of the transfer, with rules designed on a risk-based approach, which is already implemented in some GDPR provisions.

**Chapter 6** offers conclusions structured as responses to the main research question and sub-questions. The thesis concludes that, in order to reconcile cross-border data flows with data protection and privacy without undermining fundamental rights, a reform of trade law rules in the EU’s future trade agreements and the GDPR rules on transfers of personal data outside the EEA is necessary. The thesis paves the way for further research necessary in order to design a fully-fledged reform proposal of the EU framework for transfer of personal data outside the EEA. Chapter 6 also suggests an examination of the issues of social justice in the context of commercial use of personal data and of the increasingly intertwined relationship between national security, state surveillance, data privacy and international trade.
Samenvatting

DE REGULERING VAN GRENSOVERSCHRIJDENDE GEGEVENSSTROMEN:
VERZOEENING VAN EU-GEGEVENSBesCHERMING EN HET INTERNATIONALE
HANDELSRECHT

In dit proefschrift wordt onderzocht hoe twee belangrijke beleidsdoelstellingen van de Europese Unie juridisch met elkaar kunnen worden verenigd. Enerzijds garandeert het EU-Handvest van de grondrechten (EU-Handvest) de bescherming van het recht op privacy en de bescherming van persoonsgegevens als grondrechten. Anderzijds streeft de EU er in haar externe handelsbeleid naar de grensoverschrijdende gegevensstromen te liberaliseren en een wereldwijd bindend, op regels gebaseerd handelssysteem in stand te houden en verder te ontwikkelen waarmee EU-bedrijven een passende toegang tot buitenlandse markten wordt gegarandeerd. Tot voor kort bestonden beide doelstellingen in het externe beleid van de EU naast elkaar zonder met elkaar in conflict te komen. Meer recent zijn de grensoverschrijdende gegevensstromen het ‘lifeblood’ van de internationale handel geworden waardoor conflicten wel ontstaan. De digitale handel neemt immers een steeds groter deel van de wereldhandel in beslag. Het verzamelen en commercieel gebruiken van persoonsgegevens heeft echter ook een essentiële niet-economische waarde. Deze waarde is de reden waarom persoonsgegevens door het EU-Handvest worden beschermd en waarom dit is bevestigd met de invoering van de Algemene verordening gegevensbescherming (AVG). In dit proefschrift wordt onderzocht hoe deze uiteenlopende doelstellingen met elkaar kunnen worden verzoend.

Hoewel individuen kunnen profiteren van de vrije stroom en de alomtegenwoordige monetisatie van hun gegevens door bedrijven - bijvoorbeeld in de vorm van gepersonaliseerde diensten - hebben zij ook veel te verliezen. Op mondiaal niveau is de massale grensoverschrijdende toe-eigening van persoonsgegevens ook wel vergeleken met de winning van natuurlijke hulpbronnen: de potentiële schade voor individuen en voor de samenleving als geheel is veel groter dan de directe economische verliezen die worden geleden door gegevensinbreuken en identiteitsdreigingen.

Sinds 2009 is het recht op bescherming van persoonsgegevens erkend als een zelfstandig grondrecht in de EU naast het (eveneens fundamentele) recht op privacy. Net zoals persoonsgegevens zowel een economische als een maatschappelijke waarde hebben, heeft de Europese gegevensbeschermingsregeling een tweeledig doel: enerzijds de bescherming van de fundamentele rechten en vrijheden van personen (met name hun recht op bescherming van persoonsgegevens), anderzijds het waarborgen van het vrije verkeer van persoonsgegevens binnen de Europese Economische Ruimte (EER). Echter, de constitutionalisering van de EU en de vaststelling van Europese wetgeving inzake gegevensbescherming, heeft deze niet-economische doelstelling op de voorgrond geplaatst.
en prevaleert deze boven de economische doelstelling. Sterker nog: vanwege de toenemende bezorgdheid over de eigen technologische of digitale 'soevereiniteit' ten opzichte van de groeiende economische en sociale invloed van technologiebedrijven van buiten de EU (voornamelijk Amerikaanse) ligt de laatste tijd meer nadruk op de bescherming van privacy en de bescherming van gegevens.

Er is echter ook kritiek: beperkingen van internationale gegevensstromen meer in het bijzonder van persoonlijke gegevensstromen zouden een vorm van ongewenst 'protectionisme' zijn. Nu het zwaartepunt van de internationale handelsbesprekingen verschuift naar de digitale handel, is dit een centraal punt in het academische, publieke en politieke debat. De trend in het internationale handelsrecht om internationale stromen van (persoons)gegevens te liberaliseren, kan worden gezien als strijdig met wettelijke regelingen, zoals die van de EU, die dergelijke stromen om privacy- en gegevensbeschermingsredenen aan banden willen leggen. Liberalisering van digitale handel binnen de EU is vanwege de harmonisatie van het EU-kader voor gegevensbescherming echter niet langer een probleem omdat de normatieve waarde van grondrechtenbescherming in evenwicht is gebracht met de economische waarde die aan de liberalisering van digitale handel ten grondslag ligt. Bij de externe digitale handel zijn beide waarden nog niet met elkaar in evenwicht; er is immers geen sprake van een geharmoniseerd kader voor gegevensbescherming, terwijl dit voor de EU een voorwaarde is voor liberalisering.

De Wereldhandelsorganisatie (WTO) is het belangrijkste orgaan dat de internationale handelsregels beheert. Zowel de EU als haar lidstaten zijn lid van de WTO. De rol van de WTO is de laatste tijd echter afgenomen als gevolg van politieke omstandigheden waardoor het aantal regionale en bilaterale handelsovereenkomsten is toegenomen. De zogenaamde 'nieuwe generatie' vrije handelsovereenkomsten (zoals de Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), de handelsovereenkomst tussen de Verenigde Staten en Mexico/Canada (USMCA) en de digitale handelsovereenkomst tussen de VS en Japan), die door de belangrijkste handelspartners van de EU, Canada, Japan en de VS, zijn gemaakt, bevatten bepalingen die partijen verplichten om vrije grensoverschrijdende informatiestromen, met inbegrip van persoonsgegevens, toe te staan. Het faciliteren van deze gegevensstromen is ook een belangrijk thema bij de onlangs gestarte onderhandelingen over e-handel in de WTO.

Het opheffen van de beperkingen op gegevensstromen was onlangs een van de meest omstreden onderwerpen in handelsbesprekingen in Azië, Europa en Noord-Amerika. Nu de internationale handelsregeling steeds meer tendeert naar vrije digitale handel en het Hof van Justitie van de Europese Unie (HvJEU) de effectieve bescherming van de grondrechten van de EU als voorwaarde voor dergelijke overdrachten stelt, is het een logisch gevolg dat
de ambitie van de EU voor de liberalisering van het grensoverschrijdende dienstenverkeer in het kader van de Algemene Overeenkomst betreffende de handel in diensten (GATS) enerzijds en het recht op de bescherming van persoonsgegevens anderzijds met elkaar in conflict komen. Dit is op zich geen reden tot bezorgdheid. Zowel het EU-Handvest als het internationale handelsrecht bevatten immers uitzonderingen die het mogelijk maken dat elk systeem binnen bepaalde grenzen inbreuken op de respectievelijke regels van de andere systemen tolereert. De meeste internationale handelsovereenkomsten, waaronder de GATS, voorzien in een zogenaamde 'algemene uitzondering'. Deze uitzondering garandeert dat partijen bij een internationale handelsovereenkomst maatregelen kunnen nemen en handhaven die ten behoeve van de verwerking en verspreiding van persoonsgegevens noodzakelijk zijn voor de bescherming van de persoonlijke levenssfeer van personen (de handelsnoodzakelijkheidstoets), zelfs als dergelijke maatregelen in strijd zijn met de internationale verbintenissen van de deelnemers. Op grond van artikel 52, lid 2, van het EU-Handvest kan ook de EU grondrechten beperken indien dit noodzakelijk is om doelstellingen van algemeen belang te verwezenlijken of om de rechten en vrijheden van anderen te beschermen (de noodzakelijkheidstoets van het EU-Handvest). In hoofdstuk 2 wordt echter geconcludeerd dat de handelsnoodzakelijkheidstoets, zoals door de WTO-onderzoeksinstanties geïnterpreteerd, onvoldoende is om de EU het grondrecht op privacy en gegevensbescherming afdoende te garanderen.

Ten behoeve van haar toekomstige digitale handelsovereenkomsten heeft de EU in 2018 alternatieve zogenoemde 'horizontale bepalingen' ontwikkeld inzake grensoverschrijdende gegevensstromen en de bescherming van de persoonlijke levenssfeer en persoonsgegevens ontwikkeld. Sindsdien heeft de EU deze modelclausules in handelsbesprekingen over digitale handel (bijvoorbeeld met Australië, Indonesië, Nieuw-Zeeland, Tunesië en het Verenigd Koninkrijk) op tafel gelegd. Ook heeft de EU deze clausules opgenomen in het EU-voorstel voor de WTO-regels inzake elektronische handel (e-commerce). De voorgestelde modelclausules van de EU bevatten enerzijds een gelimiteerder verbod op beperkingen van grensoverschrijdende gegevensstromen dan de VS voorstaat (dat ten uitvoer is gelegd in de CCTPP, de USMCA en de digitale handelsovereenkomst tussen de VS en Japan), anderzijds een ruimere uitzondering voor binnenlandse privacy- en gegevensbeschermingsregels dan de eerder genoemde algemene uitzondering (die ook in het VS-model is overgenomen).

Tegen deze achtergrond is de primaire onderzoeksvraag die in dit proefschrift wordt beantwoord:

_Hoe kunnen de afspraken inzake grensoverschrijdende gegevensstromen in toekomstige handelsovereenkomsten van de EU juridisch worden verenigd met de bescherming van de fundamentele rechten op privacy en persoonsgegevens?_
Deze onderzoeksvraag valt uiteen in vier subvragen die achtereenvolgens in de hoofdstukken 2-5 worden beantwoord.

In hoofdstuk 2 wordt de belangrijkste kwestie die aan deze stelling ten grondslag ligt, geïdentificeerd en uiteengezet: namelijk de toenemende spanning tussen het beheer van grensoverschrijdende doorgiften van persoonsgegevens door de EU en het internationale handelsrecht. In dit hoofdstuk wordt de stelling ontwikkeld dat de beperkingen van de EU op de doorgifte van persoonsgegevens in strijd zijn met de verbintenissen en verplichtingen die op de EU rusten uit hoofde van de GATS en de post-GATS-handelsovereenkomsten. Volgens deze stelling voldoen dergelijke beperkingen niet aan de handelsnoodzakelijkheidstest, zelfs niet in de meest milde interpretatie ervan, omdat zij de grenzen van de GATS-bepalingen en de algemene uitzondering voor de bescherming van de persoonlijke levenssfeer en persoonsgegevens overschrijden. Tegelijkertijd kunnen, volgens de strikte noodzakelijkheidstoets in het EU-Handvest (zoals geïnterpreteerd door het HvJEU), de juridische mogelijkheden om af te wijken van de bescherming van het recht op privacy en de bescherming van persoonsgegevens onvoldoende zijn om te voldoen aan de internationale handelsverplichtingen waar het gaat om grensoverschrijdend verkeer van persoonsgegevens. De sequentiële toepassing van deze twee 'noodzakelijkheidstests' brengt het risico met zich dat beide met elkaar in conflict komen, waardoor de EU in een catch-22-nalevingsimpasse terecht komt tussen de schending van het handelsrecht en een ongerechtvaardigde afwijking van het recht op bescherming van persoonsgegevens.

In de context van de lopende handelsbesprekingen over digitale handel die de EU met haar handelspartners voert over grensoverschrijdende gegevensstromen, privacy en gegevensbescherming, is deze stand van zaken niet houdbaar. Volgens het primaire recht van de EU mogen de EU-instellingen niet onderhandelen over internationale handelsregels zo lang die strijdig zijn met het EU-acquis. Tegelijkertijd kan de EU, ondanks het feit dat internationale handelsovereenkomsten, hiërarchisch bezien, onder het primaire recht van de EU staan, niet worden ontheven van haar internationale handelsverplichtingen om de enkele reden dat deze strijdig zijn met het primaire recht van de EU. Daarom moet de EU het EU-Handvest en haar internationale handelsverplichtingen tegelijkertijd naleven. De in dit proefschrift voorgestelde en in de hoofdstukken drie en vier verder uitgewerkte uitweg uit deze impasse is gebaseerd op drie belangrijke overwegingen. Ten eerste is een proactieve houding van de EU te prefereren omdat wachten riskant kan zijn: de EU kan immers door een handelsrechtelijke instantie onder hevige tijdsdruk worden gedwongen om de beperkingen op te heffen. Ten tweede, en daarmee samenhangend, kan de aanhoudende onzekerheid over de rechtmantigheid van de doorgifte van persoonsgegevens buiten de EER enerzijds, en de naleving van de beperkingen op dergelijke doorgiften van de internationale handelsverplichtingen van de EU anderzijds, de handelsrelaties bekoelen, ten nadele van het bedrijfsleven in de EU. Ten derde zou het laten prevaleren van
'doeltreffende en volledige' bescherming van het recht op privacy en op bescherming van persoonsgegevens een totaalverbod op de doorgifte van persoonsgegevens tot gevolg kunnen hebben hetgeen de digitale grensoverschrijdende handel met de EU zou ondermijnen en om die reden onacceptabel is.

**In hoofdstuk 3** wordt een stap terug gedaan en onderzocht wat de term 'protectionisme' inhoudt en of EU-beperkingen op doorgiften van persoonsgegevens buiten de EER protectionistisch zijn. Door de inzichten uit het werk van Michel Foucault over de relatie tussen discours en macht toe te passen, toont dit hoofdstuk aan dat het niet mogelijk is een goede balans te vinden tussen liberalisering van de digitale handel en bescherming van privacy en persoonsgegevens door eenvoudigweg de optie van 'protectionisme' uit te sluiten. Hoofdstuk 3 stelt dan ook dat het onderscheid tussen bescherming en protectionisme niet helder is: het trekken van de grens tussen bescherming en protectionisme is onder de streep arbitrair. Binnen dit spectrum is er een grijs gebied aan maatregelen, waaronder ook binnenlandse maatregelen kunnen vallen, waarbij het onzeker is welk soort reguliersdoel eigenlijk speelt: een vermomde vorm van protectionisme of echte bescherming die incidenteel ook in het voordeel kan zijn van binnenlandse partijen. Of maatregelen in dit grijze gebied onder de noemer 'bescherming' dan wel 'protectionisme' vallen - met andere woorden: of handelsrechtelijke instanties bij hun keuze voor 'bescherming' gaan of voor 'protectionisme' - hangt in wezen af van het discours. Binnen een economisch discours, waar de vrije handel hoog in het vaandel staat, zou een dergelijke regeling als protectionisme zijn uitgesloten. In een pluralistisch discours daarentegen, waarin de vrije handel en de bescherming van privacy en data evenveel waarde krijgen, zou het de voorkeur verdienen om staten eigen beleidsruimte toe te staan om een aantal licht protectionistische maatregelen aan te nemen teneinde beide grondrechten te beschermen.

In het kader van de onderhandelingen over en de interpretatie van het internationale handelsrecht is de keuze van het juiste discours over privacy en de bescherming van persoonsgegevens van cruciaal belang. Bij het opstellen en interpreteren van bepalingen in internationale handelsovereenkomsten bepalen onderliggende waardenstructuren waar de grens ligt tussen legitieme bescherming van privacy en van persoonsgegevens aan de ene kant en onrechtmatig protectionisme aan de andere kant. Tegen deze achtergrond wordt in hoofdstuk 3 gesteld dat landen zich bewust moeten zijn van de waardenstructuren die bij een bepaald discours horen. Landen moeten ervoor zorgen dat zij het eerst eens worden over welke waardenstructuur de voorkeur verdient en vervolgens die structuur leidend te laten zijn bij de keuze van het discours in plaats van andersom. In dit hoofdstuk wordt gesteld dat het onderscheid tussen privacy en bescherming van persoonsgegevens enerzijds en protectionisme anderzijds deels een *morele* kwestie is, dus niet alleen een kwestie van economische efficiëntie. Dit impliceert dat wanneer het debat over grensoverschrijdende
stromen van persoonsgegevens raakt aan niet-economische waarden, zoals individuele rechten, dat debat niet moet worden beperkt tot de handelseconomie maar moet plaatsvinden in een breder normatief kader.

In hoofdstuk 3 wordt voorts gesteld dat beperkingen van het grensoverschrijdend verkeer van persoonsgegevens noodzakelijk zijn. Tenzij de aanpak van gegevensbescherming en privacy wordt geharmoniseerd, hebben landen meer beleidsruimte nodig om eigen gegevensbeschermingsregelingen op te stellen. Juist omdat het gegevensbeschermingsniveau in sommige landen laag kan zijn (misschien strategisch laag), zouden landen met een hoger beschermingsniveau de doorgifte van persoonsgegevens moeten beperken.

In hoofdstuk 4 wordt ingegaan op enkele specifieke aspecten van het internationaal handelsrecht die in hoofdstuk 2 aan de orde kwamen. Het bestaat uit drie delen. In het eerste deel wordt de vraag gesteld of de door de Europese Commissie in 2018 voorgestelde modelclausules inzake grensoverschrijdende gegevensstromen en de bescherming van de persoonlijke levensfeer en persoonsgegevens de EU in staat stellen om de potentiële catch-22-nalevingsimpasse in toekomstige handelsovereenkomsten te doorbreken en tegelijkertijd de doelstellingen na te streven van het versoepelen van handel in grensoverschrijdende gegevensstromen en het bevorderen van een op regels gebaseerd multilateraal handelsstelsel. Het wordt gesteld dat de 2018-clausules op het eerste gezicht enerzijds ruime autonomie geven om privacy en persoonsgegevens als grondrechten te beschermen en anderzijds beperking van grensoverschrijdende gegevensstromen verbieden. Vergeleken met het Amerikaanse model is het verbod op beperkingen van grensoverschrijdende gegevensstromen nauwer geformuleerd. Voorts wordt in de voorgestelde clausules gesteld dat de bescherming van persoonsgegevens en van de persoonlijke levensfeer en persoonsgegevens de EU heeft. Bovendien waarborgt de ruime formulering van de voorgestelde uitzondering voor de bescherming van de persoonlijke levensfeer en persoonsgegevens (de zogenaamde 'digitale handelsuitzondering'), die is gemodelleerd naar de nationale veiligheidsuitzonderingen in de WTO-overeenkomsten, de mogelijkheid voor de EU om beperkingen op de doorgifte van persoonsgegevens buiten de EER in het kader van de AVG te handhaven. De voorgestelde uitzondering voor de digitale handel erkent expliciet de regels voor grensoverschrijdende doorgiften van persoonsgegevens als voorbeeld van maatregelen die in het kader van de uitzondering zouden moeten worden toegestaan.

In hoofdstuk 4 wordt echter ook beargumenteerd dat de voorgestelde modelclausules ten minste drie essentiële gebreken vertonen die ertoe kunnen leiden dat zij het fundamentele recht op privacy en op bescherming van persoonsgegevens niet kunnen garanderen en de doelstellingen van het digitale handelsbeleid van de EU ondermijnen.
Ten eerste leidt de onduidelijke verhouding tussen de voorgestelde digitale handelsvrijstelling voor privacy en gegevensbescherming (bedoeld voor de digitale hoofdstukken van handelsovereenkomsten) en de algemene uitzondering (die doorgaans is opgenomen in het hoofdstuk over uitzonderingen van dezelfde voorgestelde handelsovereenkomsten) tot rechtsonzekerheid over de materiële werkingssfeer van de voorgestelde uitzondering. Ten tweede is de voorgestelde digitale uitzondering voor de bescherming van de persoonlijke levenssfeer en persoonsgegevens zodanig ruim geformuleerd dat die het effect van de voorgestelde bepaling op grensoverschrijdende gegevensstromen in dezelfde modelclausules teniet doet. Meer in het algemeen wordt in hoofdstuk 4 gesteld dat de stabiliteit die de op regels gebaseerde internationale handelsorde kenmerkt, verder zou kunnen worden ondermijnd wanneer, zoals in de 2018-clausules wordt voorgesteld, de zeer lage drempel die de uitzondering van 'nationale veiligheid' kent, gebruikt wordt als model voor de digitale handelsuitzondering. Ten derde zijn de voorgestelde modelclausules te EU-gericht in die zin dat zij een erkenning van de bescherming van de persoonlijke levenssfeer en persoonsgegevens als fundamentele rechten vereisen - een verbintenis die wellicht niet alle handelspartners van de EU bereid zijn te aanvaarden of in de praktijk ten uitvoer te leggen.

In het tweede deel van hoofdstuk 4 worden drie manieren voorgesteld om de modelclausules te verbeteren. Ten eerste zouden toekomstige handelsovereenkomsten ofwel een bepaling moeten bevatten die de relatie tussen de algemene en de digitale handelsuitzonderingen voor privacy en gegevensbescherming verduidelijkt, ofwel één enkele uitzondering voor privacy en gegevensbescherming moeten bevatten die voor de hele overeenkomst zou gelden (waarbij wordt erkend dat deze laatste in de praktijk problematisch zou kunnen zijn). Ten tweede zou de EU moeten overwegen om een drempel voor de digitale handelsuitzondering te formuleren die het midden houdt tussen de door de EU voorgestelde 'die het passend acht' drempel en de noodzakelijkheidstoetsing van de algemene uitzondering. Ten derde moet de bepaling op grond waarvan partijen erkennen dat de bescherming van persoonsgegevens en de persoonlijke levenssfeer een grondrecht is, zodanig worden geherformuleerd dat enerzijds de autonomie van de EU om haar grondrechten te beschermen is gewaarborgd maar dat anderzijds andere handelspartners desgewenst een lager beschermingsniveau (binnen de grenzen van de internationale mensenrechtenwetgeving) kunnen hanteren.

In het derde en laatste deel van hoofdstuk 4 wordt ingegaan op andere drempels dan de 'die het passend acht' toets, waarop de EU zou kunnen terugvallen zonder afbreuk te doen aan de fundamentele rechten op privacy en gegevensbescherming. Er wordt gekeken naar alternatieven uit WTO-overeenkomsten en bilaterale en regionale handelsovereenkomsten die zich bevinden op het continuüm tussen de 'noodzaak' in de algemene uitzondering (de huidige test voor privacy en gegevensbescherming) en de 'die
het passend acht'-drempel uit het voorstel. Als haalbare alternatieven worden genoemd de tests inzake 'niet-omzeiling', 'niet-vermijding' en 'redelijkheid', mits zij vergezeld gaan van mechanismen die de discretionaire bevoegdheid van de handelsrechtelijke instanties beperken en dat zij op een genuanceerde manier worden toegepast.

Voortbouwend op de conclusies van hoofdstukken 2 t/m 4 wordt in hoofdstuk 5 het probleem aan de orde gesteld van de 'twee noodzakelijkheden' uit hoofdstuk 2. Dit gebeurt zowel vanuit het perspectief van het EU-Handvest als vanuit dat van de EU-regelgeving inzake gegevensbescherming. De analyse in dit hoofdstuk is gestructureerd aan de hand van drie algemene kwesties: (1) de grondwettelijke grenzen die het EU-Handvest stelt aan het secundaire EU-recht inzake gegevensbescherming en met name de mate waarin het EU-kader voor de doorgifte van persoonsgegevens buiten de EER in de AVG binnen die grenzen kan worden gewijzigd; (2) het vermogen van dit EU-kader om zijn constitutionele functie te vervullen teneinde te voorkomen dat het hoge niveau van bescherming van persoonsgegevens in de EU wordt omzeild en uiteindelijk te zorgen voor een 'doeltreffende en volledige' bescherming van grondrechten; en (3) het hervormingsvoorstel voor een dergelijk kader als reactie op de veranderde politieke, geopolitieke en economische omstandigheden.

Wat het eerste punt betreft, wordt in hoofdstuk 5 betoogd dat er een dynamisch verband bestaat tussen de AVG (als secundair EU-rechtsinstrument) en het EU-Handvest (als primair rechtsinstrument). Tegelijkertijd toont dit hoofdstuk aan dat het kader voor de doorgifte van persoonsgegevens buiten de EER in hoofdstuk V van de AVG slechts één mogelijke opzet van een dergelijk kader in het licht van de vereisten van het EU-Handvest is. Alleen de aanwezigheid van enkele beperkingen en enkele aspecten van dergelijke beperkingen, vormen de essentie van de grondrechte, op privacy, bescherming van persoonsgegevens en het recht op effectieve rechtsbescherming (in de context van de eerste twee rechten) en kunnen daarom niet worden gewijzigd door het afgeleide recht van de EU. Andere elementen van een dergelijk kader kunnen door de secundaire wetgever van de EU worden vastgesteld op basis van een strikte noodzakelijkheids- en evenredigheidstoetsing, waarvan het doel zou zijn de grondwettelijke functie ervan, namelijk het voorkomen van omzeiling van het hoge niveau van bescherming van persoonsgegevens in de EU, te waarborgen. Het begrip 'passend beschermingsniveau', dat volgens het Schrems II-arrest van het HvJEU kan worden beschouwd als het constitutionele ijpunt voor het secundaire rechtskader voor de doorgifte van persoonsgegevens, maakt geen deel uit van de essentie van de bovengenoemde grondrechten. In plaats daarvan regelt het de afweging van de bovengenoemde grondrechten tegen concurrerende beleidsdoelstellingen: aan de ene kant de economische voordelen die inherent zijn aan onbeperkte grensoverschrijdende stromen van persoonsgegevens en aan de andere kant de nationale veiligheidsbelangen van het
buitenland. In hoofdstuk 5 wordt dan ook gesteld dat de EU-wetgever voldoende speelruimte heeft om de opzet van de thans in hoofdstuk V van de AVG gecodificeerde regels te wijzigen.

In het tweede deel van hoofdstuk 5 worden vier gebreken in het EU-kader vastgesteld. Het eerste zwakke punt is dat er, ondanks het recente Schrems II-arrest een hardnekkige kwalitatieve kloof bestaat tussen de adequaatheidsbesluiten enerzijds en de passende waarborgen op grond van artikel 46 van de AVG anderzijds (die beide dienen als mechanismen voor systematische doorgiften). De EU moet het probleem van het buitenlands toezicht op internationaal niveau aanpakken in plaats van via haar eigen secundaire recht. Het buitenlands toezicht was de voornaamste reden waarom kwesties in verband met de doorgifte van persoonsgegevens naar het HvJEU worden verwezen. Het tweede gebrek is dat adequaatheidsbesluiten vatbaar zijn voor politieke druk in het kader van het EU-handelsbeleid. Het derde gebrek houdt in dat adequaatheidsbesluiten niet in staat zijn hun grondwettelijke functie te vervullen omdat de beoordeling waarop de besluiten inzake gepastheid zijn gebaseerd, niet regelmatig wordt herzien (het 'snapshot'-probleem) omdat het moeilijk is individuele rechten in andere jurisdicties af te dwingen (het 'zware last'-probleem) en omdat het mechanisme voor verdere doorgifte dat in de besluiten inzake gepastheid is opgenomen, ondoorlatend is (het 'doorgifte'-probleem). Het vierde en laatste zwakke punt is, op een meer abstract niveau, de beperkte schaalbaarheid van de huidige regeling voor de doorgifte van persoonsgegevens in hoofdstuk V van de AVG in het licht van de technologische ontwikkelingen die zich hebben voorgedaan sinds de jaren negentig, toen de kern van het kader voor het eerst werd ontworpen.

In het derde en laatste deel van hoofdstuk 5 worden drie denkrichtingen voorgesteld om het kader van hoofdstuk V van de AVG binnen de door het EU-Handvest vastgestelde grenzen te verbeteren waarbij mogelijke korte-, middellange- en langetermijnstrategieën voor de EU op dit gebied in aanmerking worden genomen.

De eerste en meest gematigde denkrichting stelt voor om specifieke elementen van de mechanismen voor de overdracht van persoonsgegevens te verbeteren zonder de opzet en de inhoud van het kader te wijzigen. Zo wordt bijvoorbeeld voorgesteld een transparante procedure goed te gebruiken die de mate waarin het adequaatheidsmechanisme vatbaar is voor politieke beïnvloeding aanpak en de beoordeling van de adequaatheid overzet van een eenzijdig instrument naar een wederkerige overeenkomst. In een tweede denkrichting wordt voorgesteld om het kader meer schaalbaarheid te geven en tegelijkertijd de bijzonderheden ervan te verbeteren. Dit vereist een substantiële herziening van de AVG en zou daarom realistisch gezien pas op middellange termijn kunnen worden aangepakt - bijvoorbeeld bij de volgende herziening van hoofdstuk V van de AVG op grond van artikel 97 van de AVG in 2024. Naast de in de eerste denkrichting geschetste
hervormingsvoorstellen worden in de tweede denkrichting twee principiële aanpassingen van hoofdstuk V van de AVG voorgesteld: (1) soepeler regels voor de overdracht van niet-gevoelige gepseudonimiseerde gegevens en (2) het geven van juridische betekenis aan technologische middelen voor de bescherming van persoonsgegevens. In de derde denkrichting wordt een meer fundamentele herziening van het EU-kader voor de doorgifte van persoonsgegevens voorgesteld. Een manier om dit te doen, zou zijn de huidige 'one-size-fits-all'-aanpak, waarbij de verschillende mechanismen voor de doorgifte van persoonsgegevens die geen rekening houden met de context en de parameters van de doorgifte, te vervangen door regels die zijn ontworpen op basis van een *risicogebaseerde aanpak*, die al in sommige AVG-bepalingen ten uitvoer is opgenomen.

**In Hoofdstuk 6 wordt de hoofd onderzoeksvraag beantwoord aan de hand van**

een overzicht van de antwoorden op de hiervoor beschreven subvragen. Het proefschrift concludeert dat, om grensoverschrijdende gegevensstromen te verenigen met gegevensbescherming en privacy zonder de grondrechten te ondermijnen, een hervorming van de handelsrechtelijke regels in de toekomstige handelsovereenkomsten van de EU en de AVG-regels voor de overdracht van persoonsgegevens buiten de EER noodzakelijk is. Dit hoofdstuk voorziet tevens in richtingen voor verder onderzoek dat nodig is om een volwaardig hervormingsvoorstel van het EU-kader voor de doorgifte van persoonsgegevens buiten de EER op te stellen. Daarnaast stelt hoofdstuk 6 een onderzoek voor naar de kwesties van sociale rechtvaardigheid in de context van commercieel gebruik van persoonsgegevens en van de steeds meer met elkaar verweven relatie tussen nationale veiligheid, staatstoezicht, gegevensbescherming en internationale handel.