This book looks at transatlantic jurisdictional conflicts in data protection law and how the fundamental right to data protection conditions the EU’s exercise of extraterritorial jurisdiction. Governments, companies and individuals are handling ever more digitised personal data, so it is increasingly important to ensure this data is protected. Meanwhile, the Internet is changing how territory and jurisdiction are realised online. The EU promotes personal data protection as a fundamental right. Especially since the EU General Data Protection Regulation started applying in 2018, the EU’s data protection laws have had strong effects beyond its territory. In contrast, similar US information privacy laws are rooted in the marketplace and carry less normative heft. This has provoked clashes with the EU when their values, interests and laws conflict. This research uses three case studies to suggest ways to mitigate transatlantic jurisdictional tensions over data protection and security, the free flow of information and trade.

Mistale Taylor is Counsel at the Public International Law and Policy Group. Her background lies in public international law and data privacy law. She has published and presented on many subjects, including international law, human rights, ethics, privacy and data protection as they relate to emerging technologies.
Transatlantic Jurisdictional Conflicts in Data Protection Law

FUNDAMENTAL RIGHTS, PRIVACY AND EXTRATERRITORIALITY

MISTALE TAYLOR
# Contents

**Acknowledgements**  
*page xiii*

**Author’s Note**  
*xv*

**Table of Cases**  
*xvii*

1 **Introduction**  
1.1 Background  
1.2 Extraterritoriality  
1.3 Jurisdictional Tensions  
1.4 Towards an Assessment Framework  
1.5 Scope of the Study  
1.6 Relevance of the Study  
1.7 Defining Terms  
1.8 Approach of the Study  

2 **Conceptual Approaches to Data Protection in the European Union and the United States**  
2.1 Introduction  
2.2 The Difference between the Right to Privacy and the Right to Data Protection  
2.3 The Evolution of the Right to Data Protection in the EU Legal Order  
2.3.1 Data Protection in Early International Instruments  
2.3.2 From National Laws to EU Law  
2.4 Data Protection as a Value and Right in the EU  
2.5 Information Privacy in the United States  
2.6 A Global Approach to Data Protection
## Contents

### 3 The European Union’s Obligations to Safeguard the Fundamental Right to Data Protection Extraterritorially

- 3.1 Introduction
- 3.2 The EU Charter’s Scope of Application
- 3.3 Data Protection as a Fundamental Right in the EU
- 3.4 The Nature of the Right to Data Protection and Associated Obligations
  - 3.4.1 Under Public International Law
  - 3.4.2 Under International Human Rights Law
- 3.5 The Extraterritorial Application of Human Rights Instruments
  - 3.5.1 Jurisdiction under International Human Rights Law
  - 3.5.2 Applying Different Models of International Human Rights Law Jurisdiction to European Data Protection Law
- 3.6 Control in International Human Rights Law Jurisdiction
- 3.6.1 The Obligation to Respect
- 3.6.2 The Obligation to Protect
- 3.6.3 The Obligation to Fulfil
- 3.7 The Increased Weight of the Fundamental Right to Data Protection and Consequences for Extraterritoriality
  - 3.7.1 The Free Flow of Information
  - 3.7.2 The Right to Freedom of Expression
  - 3.7.3 Security Interests
  - 3.7.4 A Heavier Right
- 3.8 Interim Conclusion

### 4 Limits That Public International Law Poses on the European Union Safeguarding the Fundamental Right to Data Protection Extraterritorially

- 4.1 Public International Law Approaches to Jurisdiction
- 4.2 Two Approaches to Lawfulness under Public International Law
  - 4.2.1 A Substantial Connection
  - 4.2.2 Permissive Principles
- 4.3 The Scope of EU Data Protection Law
Contents

4.3.1 Applicable Law and Jurisdiction 66
4.3.2 Data Controllers and Data Processors 67
4.4 Territoriality 68
  4.4.1 In EU Data Protection Law 73
  4.4.2 Subjective Territoriality 75
  4.4.3 Objective Territoriality 76
    4.4.3.1 In the Context of the Activities of an Establishment in the EU 76
    4.4.3.2 From the Use of Equipment in the EU to Targeting Those in the EU 77
  4.4.3 Public International Law 79
  4.4.4 The Effects Doctrine 80
4.5 Personality 82
  4.5.1 Individuality and Personality 83
  4.5.2 Active and Passive Personality 84
    4.5.2.1 Reconciling Citizenship, Residence and Applicability 85
    4.5.2.2 Reconciling Personality and Territoriality 89
4.6 The Protective Principle 90
4.7 Universal Jurisdiction 91
4.8 Prohibitions in Exercising Jurisdiction 92
4.9 Interim Conclusion 93

5 Ways to Mitigate Problematic Jurisdictional Overreach 95
  5.1 Introduction 95
  5.2 Mitigating Factors as Proxy for Territoriality 96
  5.3 Connection 97
    5.3.1 Connection in EU Data Protection Law 100
      5.3.1.1 Context of the Activities of an Establishment of a Controller or Processor 101
    5.3.2 Targeting 103
    5.3.2 Interim Conclusion on Connection in EU Data Protection Law 107
  5.4 Reasonableness 107
    5.4.1 Comity 108
    5.4.2 The Enduring Appeal of the Third Restatement of US Foreign Relations Law 109
  5.4.3 Interest 110
  5.4.4 Interest-Balancing 111
  5.4.5 Balancing Rights 112
Contents

5.4.6 Reasonableness and a Rule of Reason 114
5.5 Assessment Framework 116
6 The Reach of European Union Data Protection Law in Transatlantic Data Transfers for Counterterrorism Purposes 118
6.1 Introduction 118
6.2 Conceptual Approaches to Privacy in Counterterrorism Agreements 122
6.3 Transatlantic Tensions in Passenger Name Record Agreement Negotiations 124
   6.3.1 The 2004 Agreement and Reactions 124
   6.3.2 The 2006 Annulment 127
   6.3.3 The 2007 Agreement 128
   6.3.4 The 2011 Agreement 129
6.4 Incorporating Interpretations of EU Data Protection Law into Passenger Name Record Agreements 132
6.5 Jurisdictional Assessment 136
   6.5.1 International Human Rights Law Obligations 137
   6.5.2 Territoriality 139
   6.5.3 Personality 142
   6.5.4 Mitigating Factors 145
6.6 Spreading a Global Passenger Name Record Processing Norm 147
6.7 Interim Conclusion 149
7 Data Protection and the Free Flow of Information 150
7.1 Introduction 150
7.2 Framing the Jurisdictional Questions 153
   7.2.1 The Freedom of Expression 154
   7.2.2 The Free Flow of Information 155
   7.2.3 The Freedom of Expression, the Free Flow of Information and the Right to Erasure 156
7.3 The Right to Erasure in the EU 159
   7.3.1 In the Data Protection Directive and the General Data Protection Regulation 159
   7.3.2 In Case Law: Google Spain 160
   7.3.3 Reactions to the Judgment 163
7.4 Implementing the Right to Erasure 165
   7.4.1 Possible Implementation Methods 165
   7.4.2 Applied Implementation Methods 166
7.4.3 Google v CNIL and Proposed Implementation Methods 168
7.4.4 Assessing Reasonableness in Google v CNIL 169
7.5 Exercising the Right to Erasure 172
7.5.1 Concealing Territorial and National Connections 173
7.5.2 The Content of the Request 174
7.6 Analysing the Implementation Methods 175
7.6.1 The Fundamental Right to Data Protection 175
7.6.1.1 Respect 176
7.6.1.2 Protect 176
7.6.1.3 Fulfil 176
7.6.2 Territoriality Issues 177
7.6.3 The Effects Doctrine 178
7.6.4 Personality Issues 178
7.6.5 Degree of Connection 179
7.6.6 Reasonableness 182
7.7 Suggested Solutions to Implementation Issues 184
7.8 Spreading a Global Standard through an EU Court Decision 187
7.9 Interim Conclusion 188

8 Enabling Transatlantic Trade and Protecting Privacy through Cross-Border Data Transfer Agreements 189
8.1 Introduction 189
8.2 Balancing International Trade and Privacy 191
8.3 The Need for Adequate Protection 193
8.4 Direct and Indirect Effects of the Adequacy Standard 194
8.5 Transatlantic Data Transfer Agreements 195
8.5.1 Safe Harbour 196
8.5.2 Proceedings in the Schrems Case 197
8.5.3 The Privacy Shield and Subsequent Developments 199
8.5.3.1 The Schrems II Case 202
8.5.3.2 Responses and Further Developments 203
8.6 The Extraterritoriality of Transatlantic Data Transfer Arrangements 204
8.6.1 Effects on Companies 205
8.6.2 Government Reactions 208
8.6.3 Privacy Shield Negotiations and Marginally Successful Legal Diffusion 210
x

Contents

8.6.4 The Failure of EU Law Diffusion in Data Transfer Frameworks 211
8.6.5 Interim Conclusion on Extraterritoriality 214
8.7 Jurisdictional Assessment 214
8.7.1 International Human Rights Law 215
  8.7.1.1 Protecting Individual Interests 215
  8.7.1.2 The Obligation to Respect 216
  8.7.1.3 The Obligations to Protect and Fulfil 217
  8.7.1.4 Interim Conclusion on International Human Rights Law 219
8.7.2 Public International Law 219
  8.7.2.1 Data Localisation as Territoriality 220
  8.7.2.2 Subjective Territoriality 224
  8.7.2.3 Personality 225
  8.7.2.4 Interim Conclusion on Public International Law 226
8.7.3 Mitigating Factors: Interest-Balancing and Reasonableness 227
8.8 Successful Legal Diffusion 231
8.9 Interim Conclusion 232

9 The Normative External Effects of the European Union’s Exercise of Extraterritorial Jurisdiction in Data Protection Law 234
  9.1 Introduction 234
    9.1.1 Global Values 234
    9.1.2 Whom the Law Protects 236
  9.2 Purely Legal Diffusion 238
  9.3 Consequential Norm Diffusion 242
    9.3.1 Data Transfer Arrangements 244
    9.3.1.1 Adequacy Requirements 244
    9.3.1.2 Safe Harbours as Adequacy Decisions 246
    9.3.2 Interim Conclusion 249
  9.4 The EU as Norm Entrepreneur 250
  9.5 Interim Conclusion 253

10 Conclusion: Enduring Territoriality and Fundamental Rights 254
  10.1 Introduction 254
  10.2 Overview of Findings 254
Contents

10.3 Potential Future Directions 257
   10.3.1 Enduring Territorialism 258
   10.3.2 Foregrounding Fundamental Rights 260
10.4 Concluding Remarks 261

Select Bibliography 263
Index 277
Acknowledgements

Amongst his many prodigious observations, Blaise Pascal supposedly observed that ‘the last thing one discovers in composing a work is what to put first’. Indeed, I find myself writing the first page of this book now, more than seven years after the whole outing began. Over these years, so many people have offered inspiration, support, guidance and general camaraderie. To them, I am perpetually grateful. Below are just some of these people.

First and foremost, endless thanks to my brilliant PhD supervisor Cedric Ryngaert from Utrecht University for having the faith in me to make this possible. I am most grateful, too, to my second supervisor John Vervaele. I would like to acknowledge and thank my reading committee for their reflections on a nascent version of this research: Michiel Luchtman, Linda Senden, Christopher Kuner, Paul De Hert and Joe Cannataci. Thank you to my editor at Cambridge University Press, Tom Randall, for his guidance and enduring patience.

I would again like to express my gratitude to Christopher Kuner and Paul De Hert for their collegiality during my research visit to the Brussels Privacy Hub and subsequent stint in Brussels. From my time as a visiting scholar at the University of California, Berkeley, thank you to Chris Hoofnagle, Paul Schwartz and Jim Dempsey for offering their invaluable thoughts on all things American. Marise Cremona and Joanne Scott so kindly took the time to discuss my research during my stay at the European University Institute: thank you. Many thanks, too, to Dan Svantesson for his kindness and support.

For their academic illumination and friendship, I am indebted to my colleagues past and present: Brianne, Julie, Sander, Natalie, Arron, Nelson, Friederycke, Lucas, Mark, Marieke K, Otto, Machiko, Tony, Christophe, Marieke d H, Ilina, Marco, Rocco, Amy, Bart, Filippo, Julia and Katrina. A special thank you to Alice and Irina, who have been wonderful as colleagues, friends and paranymphs.

xiii
My friends have been incredible throughout all these years, so I’d like to express my heartfelt gratitude to Adrien, Aisha, Alex, Aviv, Alexia, Bárbara, Coen, Daan, Dan, Darshan, Dubbs, Emma, Eoin, Fabian, Flipo, Freddie, George, Gussie, Hayley, Helen, Kroefie, Liselotte, Luca, Max, Merel, Mol, Nick, Patrick, Quirijn, Sarah, Severin, Susy, Teo, Tymon and Willem. For his support and affection, I am especially grateful to Peter. To my parents, and Safira and Caspian: thank you for everything, always. And with that, I believe I’ve discovered the first and last thing to put into this book.
Author’s Note

It has become something of a cliché to say that technology is changing rapidly and the law struggles to keep up. Acknowledging the accuracy of this cliché in most instances, it follows that scholarship tends to lag behind legal developments. This complicated race is especially evident in the field of data privacy law. This book aims to make general statements about public international law and uses data privacy law as a lens through which to do this. I hope, therefore, that the pronouncements it makes stand the test of time and are useful and interesting to readers, acknowledging full well that much of the law and policy mentioned will continue to evolve swiftly.
Table of Cases

Permanent Court of International Justice
SS Lotus (France v Turkey) [1927] PCIJ Rep Series A No 10.

International Court of Justice
Barcelona Traction, Light and Power Co Ltd (Belgium v Spain) (Separate
Military and Paramilitary Activities in and against Nicaragua (Nicaragua v
Arrest Warrant of 11 April 2000 (Democratic Republic of the Congo v
Belgium) [2002] ICJ 1.

Court of Justice of the European Union
Case 167/73 Commission of the European Communities v French
Joined Cases 3, 4 and 6/76 Cornelis Kramer and others [1976] ECLI:EU:
Case C-214/94 Ingrid Bouthalifa v Federal Republic of Germany [1996]
Case C-569/98 The Queen v Minister of Agriculture, Fisheries and Food,
ex parte Trevor Robert Fisher and Penny Fisher [2000] ECLI:EU:
Joined Cases C-465/00, C-138/01 and C-139/01 Österreichischer Rundfunk
Table of Cases

Joined Cases C-293/12 and C-594/12 Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others [2014] ECLI:EU:C:2014:2538.
Table of Cases

Joined Cases C-511/18, La Quadrature du Net and Others, C-512/18, French Data Network and Others, and C-520/18, Ordre des barreaux francophones et germanophone and Others [2020] ECLI:EU:C:2020:791.

European Court of Human Rights
Soering v United Kingdom App no 14038/88 (7 July 1989).
Banković and Others v Belgium and 16 Other Contracting States App no 52207/99 (12 December 2001).
S and Marper v the United Kingdom App nos 30562/04 and 30566/04 (4 December 2008).
Axel Springer AG v Germany App no 39954/08 (7 February 2012).
Von Hannover v Germany (No 2) App nos 40660/08 and 60641/08 (7 February 2012).

National Judgments

Belgium
Rechtbank van Eerste Aanleg Brussel, Voorzitter van de Belgische Commissie voor de bescherming van de persoonlijke levenssfeer v Facebook Ireland Limited, 26 February 2018, AR/2016/153-A.
**Table of Cases**

### France


### Ireland

Schrems v Data Protection Commissioner [2014] IEHC 310, 2 ILRM 441.

Schrems v Data Protection Commissioner (No 2) [2014] IEHC 351, 2 ILRM 506.


### United Kingdom


### United States

Strassheim v Daily, 221 US 280 (1911).

United States v Aluminum Co of America, 148 F 2d 416 (2d Cir, 1945).


In the Matter of a Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corporation, No 14-2985, 2016 WL 3770056 (2d Cir, 2016).
