

CONTENTS

<i>Preface</i>	vii
<i>Acknowledgements</i>	ix
<i>List of Cases</i>	xv
<i>List of Legislation and International Instruments</i>	xvii
<i>List of Tables, Figures and Schedules</i>	xix
<i>List of Abbreviations</i>	xxi

Chapter 1. Introduction	1
--------------------------------------	---

PART I. THE PROBLEM

Chapter 2. What is Data Privacy and What is the Role of Consent?	9
---	---

1. The Scope: Personal Data Collection and Use by Service Providers	9
1.1. Data and Information	9
1.2. Individuals and Personal Data Collection	11
1.3. Service Providers, the Use of Personal Data and Authorisation	14
2. Data Privacy	19
2.1. Normative and Non-Normative Accounts of Privacy	19
2.2. Data Privacy as Informational Self-Determination (Autonomy)	21
2.3. The Importance of Privacy Values	24
2.4. Online Privacy as a Process of Controlled Self-Revelation	28
3. Autonomy and Consent in the Privacy Process	29
3.1. Autonomy and Consent	29
3.2. Problems of Consent in Respect of Data Privacy	33
3.3. Autonomous Choice in Respect of Privacy Process	36

Chapter 3. What are the Challenges from Online Services?	41
---	----

1. How Do 'Data Markets' Work?	41
1.1. Control Over Data is a Key Success Factor in Online Markets	41
1.2. Which Activities of Service Providers Pose Privacy Problems?	45
1.2.1. 'Enhanced' Service Model	46
1.2.2. Trading Platform Model	49
1.2.3. Non-Trading Platform Model	50
1.3. The Economic Value of Data	54

2.	What Makes ‘Cyber’ Special?	58
2.1.	The Architecture of the Online Environment	58
2.2.	Information Asymmetry and Individualisation	62
3.	Privacy Problems in Respect of Online Services	66
3.1.	Risk of Tangible Loss to the Individual.....	67
3.2.	Harm to Individual Values: Autonomy and Dignity.....	70
3.3.	Interference with Social Values	74

PART II. PRIVACY MANAGEMENT AS A SOLUTION

Chapter 4. How to Regulate Online Services

1.	Regulating Privacy with the Privacy Management Model	80
1.1.	What Privacy Regulation should Achieve	80
1.2.	Problems of Data Privacy Regulation	82
1.3.	Privacy Management Model.....	87
2.	Why Regulate Privacy with the Privacy Management Model?.....	92
2.1.	Achieving Values-Related Goals	92
2.2.	Correcting Market Failure	95
2.3.	Oiling the Wheels of the Digital Economy.....	99
3.	What is Needed to Regulate for Privacy Management?	105
3.1.	Which Regulatory Tools are Needed to Implement Privacy Management?	106
3.1.1.	Market (or Economic Regulation)	108
3.1.2.	‘Norms’.....	109
3.1.3.	The ‘Code’ (Architecture)	110
3.1.4.	The Fourth Modality: Law.....	113
3.2.	Which Regulatory Regime should Implement PMM?	116

Chapter 5. Economic Regulation of ‘Data Markets’

1.	Could ‘Data Markets’ Introduce Privacy Management by Themselves?... ..	123
1.1.	It may be Too Early to Find Monopoly and Abuse of Market Power.....	124
1.2.	Why Does the ‘Invisible Hand’ of the Market Not Improve Privacy?	130
1.3.	Self-Regulation is Not a Viable Option.....	132
2.	How to Influence ‘Data Markets’ to Improve Informational Self-Determination.....	135
2.1.	Employing Personal Information Administrators.....	136
2.2.	Increasing Competition by Data Portability	144
2.3.	Increasing ‘Data Sensitivity’ by Monitoring and Advice	147
2.4.	Securing Data Subjects from Uncontrolled Tracking.....	149

Chapter 6. The Architecture of Privacy Management 153

- 1. How to Express and Communicate Data Subjects’ Privacy Decisions 154
 - 1.1. Privacy Policies and Policy Languages for PMM 154
 - 1.2. Other Initiatives Allowing Individuals to Express Their Preferences 159
 - 1.2.1. ‘Do Not Track’ Technology 159
 - 1.2.2. One-Stop Shopping Opt-Out Tools 160
 - 1.2.3. Privacy Dashboards 161
- 2. How to Categorise and Present Data and Data Uses 165
 - 2.1. Categorisation of Data and Data Uses. 165
 - 2.1.1. Categories of Data 166
 - 2.1.2. Categories of Data Use. 169
 - 2.2. Presentation of Choices to Data Subjects 170
- 3. How Technology Supports Enforcement and Accountability 174
 - 3.1. Technologies Used to Handle Personal Data in the ICT Systems of Service Providers 174
 - 3.2. Enforcement and Accountability Tools. 176

Chapter 7. How to Construct Laws for Privacy Management. 183

- 1. Marking the Gaps: Privacy Management in the Laws Based on Fair Information Practice Principles 184
 - 1.1. Why there is Little Privacy Management in National Data Privacy Laws 184
 - 1.2. How National Data Privacy Laws Fit into Privacy Management ... 190
 - 1.3. The Deficiencies of a Procedural Approach 197
- 2. Closing the Legal Gaps: Privacy Management on Top of the General Data Protection Regulation. 199
 - 2.1. Closing Gaps in Controlling. 200
 - 2.1.1. Data Subjects should be Able to Decide about the Collection of Particular Data Types and Their Uses 201
 - 2.1.2. Data Subjects should be Able to Delete Their Data 203
 - 2.1.3. Data Subjects should be Able to Change Service Provider and Take All Their Data with Them. 204
 - 2.1.4. Data Subjects should be Able to Monitor the Use of Their Data 206
 - 2.2. Closing Gaps in Organising 208
 - 2.2.1. Data should be Organised in a Way that Enables Visibility of All Data Types and Uses by Data Subjects 211
 - 2.2.2. Data Subjects should be Able to Control Their Data and Policy by Means of a Standardised UI and API 212
 - 2.3. Closing Gaps in Planning 214

2.3.1.	Data Subjects should be Able to Define and Change Their Own Policy	216
2.3.2.	Data Subjects' Policies should be Stable (Preserved and Guaranteed)	217
3.	Closing the Legal Gaps: The Necessary General Legal Requirements.	218
3.1.	Enacting an Overarching Principle of Informational Self-Determination	219
3.1.1.	Why the Right to Informational Self-Determination is Necessary	219
3.1.2.	What the Right to Informational Self-Determination should Look Like	222
3.1.3.	Can it be Developed in Europe?	224
3.2.	Extraterritorial Reach of the Law.	228
3.3.	Keeping PMM within Bounds	234
3.3.1.	Limiting the Scope of Regulation.	234
3.3.2.	Restrictions on PIAs and Their Activities	235
3.3.3.	Restrictions on Binding Up Services with Blanket Consent	235
4.	Conclusion.	237
	<i>Schedules</i>	239
	<i>Bibliography</i>	247
	<i>Index</i>	281