## Contents

### Part I  Generic Issues

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>Is Personal Data the Adequate Concept?</td>
<td>9</td>
</tr>
<tr>
<td>1.1.1</td>
<td>New Kinds of Sensitive Data in Our Modern Networks: Identifiers and Contact Data</td>
<td>11</td>
</tr>
<tr>
<td>1.1.2</td>
<td>IP Address, Cookies, Data Generated by RFID, Always “Personal Data”? Why Regulate Them Anyway?</td>
<td>13</td>
</tr>
<tr>
<td>1.1.3</td>
<td>New Data to be Protected: The Profiles</td>
<td>16</td>
</tr>
<tr>
<td>1.2</td>
<td>New Objects and New Actors to be Regulated?</td>
<td>18</td>
</tr>
<tr>
<td>1.2.1</td>
<td>EU Commission’s Support to PETs</td>
<td>20</td>
</tr>
<tr>
<td>1.2.2</td>
<td>Towards a Liability of Terminal Equipments Producers and Information System Designers: The RFID Case</td>
<td>21</td>
</tr>
<tr>
<td>1.2.3</td>
<td>Terminal Equipment as a Virtual Home?</td>
<td>23</td>
</tr>
<tr>
<td>1.2.4</td>
<td>Conclusions of Sect. 1.2</td>
<td>27</td>
</tr>
<tr>
<td>1.3</td>
<td>Final Conclusions</td>
<td>28</td>
</tr>
</tbody>
</table>

### 2  Some Caveats on Profiling

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>Introduction</td>
<td>31</td>
</tr>
<tr>
<td>2.2</td>
<td>What Is It with Profiling?</td>
<td>31</td>
</tr>
<tr>
<td>2.3</td>
<td>From Measurement to Detection</td>
<td>32</td>
</tr>
<tr>
<td>2.4</td>
<td>A Risky Dependence</td>
<td>33</td>
</tr>
<tr>
<td>2.5</td>
<td>Privacy, Fairness (Non-discrimination) and Due Process</td>
<td>34</td>
</tr>
<tr>
<td>2.6</td>
<td>Causality and (Criminal) Liability</td>
<td>35</td>
</tr>
<tr>
<td>2.7</td>
<td>Who Owns My Data; Who Authors the Profiles I Match with?</td>
<td>35</td>
</tr>
<tr>
<td>2.8</td>
<td>Transparency and Anticipation</td>
<td>36</td>
</tr>
<tr>
<td>2.9</td>
<td>Privacy and Data Protection</td>
<td>36</td>
</tr>
<tr>
<td>2.10</td>
<td>From Data Minimisation to Minimal Knowledge Asymmetries?</td>
<td>38</td>
</tr>
</tbody>
</table>
2.11  AmLaw: From Privacy Enhancing Technologies to Transparency Enhancing Tools? ......................................................... 39
2.12  Call for Attention ................................................................................ 39
References ..................................................................................................... 40

3  Levelling up: Data Privacy and the European Court of Human Rights ................................................................. 43
   Gordon Nardell QC
3.1  The Background .................................................................................. 43
3.2  Legality, Necessity, Secrecy ................................................................ 46
3.3  Legality: The Liberty Case ................................................................... 47
3.4  Necessity and Proportionality: The S. and Marper Case ..................... 49
3.5  Where Does It Leave Us? ..................................................................... 51

4  Responding to the Inevitable Outcomes of Profiling: Recent Lessons from Consumer Financial Markets, and Beyond ............................... 53
   Tal Zarsky
4.1  Preface .................................................................................................. 53
4.2  Rethinking the Regulation of Profiling: In a Nutshell ......................... 55
   4.2.1  A Brief Introduction to the Flow of Personal Information ..... 55
   4.2.2  The Limits and Troubles of Regulating Data Collection ........... 57
   4.2.3  The Limits and Troubles of Regulating Data Analysis .......... 57
   4.2.4  Regulating Profiling by Addressing Uses:
          Possibilities, Factors and Limits .............................................. 58
4.3  A Tale of Four Data Miners .................................................................. 61
4.4  Some Conclusions and Summing Up ................................................... 72
References ..................................................................................................... 73

Part II  Specific Issues: Security Breaches, Unsolicited Adjustments, Facebook, Surveillance and Electronic Voting ...... 75

   Rosa Barcelo and Peter Traung
5.1  Introduction .......................................................................................... 78
   5.1.1  The EU Security Breach Legal Framework:
          The Background ....................................................................... 78
   5.1.2  The Review of the ePrivacy Directive ..................................... 79
   5.1.3  An Overview of the Security Breach Framework
          Under the Revised ePrivacy Directive ..................................... 80
5.2  Purposes and Existing Data Protection Principles Underpinning the New EU Security Breach Framework ........................................... 81
   5.2.1  Preventing and Minimising Adverse Effects for Individuals ... 81
   5.2.2  The Security Principle ............................................................. 82
   5.2.3  The Data Minimisation Principle ............................................. 84
   5.2.4  The Information Principle ......................................................... 84
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.2.5</td>
<td>The Accountability Principle</td>
<td>85</td>
</tr>
<tr>
<td>5.3</td>
<td>Elements of the EU Security Breach Notification Framework</td>
<td>86</td>
</tr>
<tr>
<td>5.4</td>
<td>Scope of the EU Security Breach Notification Framework</td>
<td>86</td>
</tr>
<tr>
<td>5.4.1</td>
<td>Entities Obliged to Notify: Covered Entities</td>
<td>86</td>
</tr>
<tr>
<td>5.4.2</td>
<td>The Application to Information Society Services and Beyond</td>
<td>87</td>
</tr>
<tr>
<td>5.4.3</td>
<td>Definition of ‘Personal Data Breach’</td>
<td>89</td>
</tr>
<tr>
<td>5.5</td>
<td>The Threshold Triggering the Obligation to Notify</td>
<td>90</td>
</tr>
<tr>
<td>5.5.1</td>
<td>Description of the Threshold</td>
<td>90</td>
</tr>
<tr>
<td>5.5.2</td>
<td>“Likely to Adversely Affect the Personal Data and Privacy”</td>
<td>92</td>
</tr>
<tr>
<td>5.5.3</td>
<td>Exceptions Relating to Technological Protection Measures and Law Enforcement</td>
<td>93</td>
</tr>
<tr>
<td>5.6</td>
<td>Means of Providing Notice, Timing and Content</td>
<td>95</td>
</tr>
<tr>
<td>5.6.1</td>
<td>Means of Providing Notice</td>
<td>95</td>
</tr>
<tr>
<td>5.6.2</td>
<td>Timing of the Notification</td>
<td>96</td>
</tr>
<tr>
<td>5.6.3</td>
<td>Content of the Notification</td>
<td>97</td>
</tr>
<tr>
<td>5.7</td>
<td>Enforcement of the Provisions</td>
<td>98</td>
</tr>
<tr>
<td>5.7.1</td>
<td>Audit and Other Tools Available to the Authorities</td>
<td>98</td>
</tr>
<tr>
<td>5.7.2</td>
<td>Selective to be Effective</td>
<td>99</td>
</tr>
<tr>
<td>5.7.3</td>
<td>Damages</td>
<td>100</td>
</tr>
<tr>
<td>5.8</td>
<td>The Next Steps</td>
<td>100</td>
</tr>
<tr>
<td>5.8.1</td>
<td>Technical Implementing Measures Through Comitology</td>
<td>100</td>
</tr>
<tr>
<td>5.8.2</td>
<td>Areas/Subjects Covered by Comitology</td>
<td>101</td>
</tr>
<tr>
<td>5.8.3</td>
<td>Towards the Application of a Security Breach Notification Scheme Across Sectors</td>
<td>102</td>
</tr>
<tr>
<td>5.9</td>
<td>Conclusions</td>
<td>104</td>
</tr>
</tbody>
</table>

6 From Unsolicited Communications to Unsolicited Adjustments          105
Gloria González Fuster, Serge Gutwirth and Paul de Hert
5.1 Protecting the Individual in front of Technology                  105
5.2 The Regulation of Unsolicited Communications                       107
5.3 The Shift Towards Unsolicited Adjustments                          110
6.3.1 Upcoming Practices                                               111
6.3.2 Present Problematic Practices                                    112
6.3.3 The (Other) Limits of Current Legislation                       114
5.4 Concluding Remarks                                                 115
References                                                              116

7 Facebook and Risks of “De-contextualization” of Information          119
Franck Dumortier
7.1 Introduction                                                        119
7.2 The Risks of De-contextualization Deriving from Interactions on Facebook 121
7.2.1 The Simplification of Social Relations on OSNS                   122
7.2.2 The Large Information Dissemination Implied by Interactions on Facebook 123
### 7.2.3 The Globalization and Normalization Effects of Facebook

- Page 126

### 7.3 Consequences of the Threat of De-contextualization on the Rights to Privacy and to Data Protection

- Page 127

#### 7.3.1 Consequences of the Threat of De-contextualization on Privacy as a Right of the Human Being

- Page 128

#### 7.3.2 Consequences of the Threat of De-contextualization on Data Protection as a Right of Data Subjects

- Page 132

### 7.4 Conclusion

- Page 135

### 8 Surveillance in Germany: Strategies and Counterstrategies

**Gerrit Hornung, Ralf Bendrath and Andreas Pfitzmann**

#### 8.1 Introduction

- Page 139

#### 8.2 The Online Searching Judgement of February 27th, 2008

- Page 140

##### 8.2.1 Background of the Case

- Page 140

##### 8.2.2 Other Fundamental Rights

- Page 141

##### 8.2.3 Content of the “New” Fundamental Right

- Page 142

##### 8.2.4 Interferences

- Page 143

##### 8.2.5 Further Developments

- Page 143

#### 8.3 The German Federal Constitutional Court: Closer to ICT and Technology Assessment than German Politicians

- Page 144

##### 8.3.1 Actors and Their Knowledge

- Page 144

##### 8.3.2 Strategies Working Against Privacy and Appropriate Counterstrategies Working Towards Privacy

- Page 147

##### 8.3.3 Summing up: Government vs. Court

- Page 148

#### 8.4 The Rise of the Anti-Surveillance Movement 2.0

- Page 148

##### 8.4.1 Data Retention and the Participatory Resistance Against Surveillance

- Page 149

##### 8.4.2 From the Internet to the Streets and into Pop Culture

- Page 151

##### 8.4.3 Putting Privacy on the Political Agenda

- Page 152

##### 8.4.4 Lessons Learned

- Page 154

### References

- Page 155

### 9 Verifiability of Electronic Voting: Between Confidence and Trust

**Wolter Pieters**

#### 9.1 Introduction

- Page 157

#### 9.2 Trust

- Page 158

##### 9.2.1 Good and Bad Trust

- Page 158

##### 9.2.2 Confidence and Trust

- Page 159

##### 9.2.3 Trust in E-voting

- Page 161

#### 9.3 Verifiability

- Page 163

##### 9.3.1 Voter-Verifiable Elections

- Page 163

##### 9.3.2 Verifiability and Receipt-Freeness

- Page 165

##### 9.3.3 Variants of Verifiability

- Page 166

#### 9.4 Verifiability and Trust

- Page 168

##### 9.4.1 The Politics of Voting Technology

- Page 169

##### 9.4.2 What Proof Do We Prefer?

- Page 169
10 Electronic Voting in Germany ............................................................... 177

Melanie Volkamer

10.1 Introduction .................................................................................... 177
10.2 Approaches Applied in Germany ................................................... 178
10.2.1 Mechanical Voting Machines ..................................................... 178
10.2.2 Direct Recording Electronic (DRE) Voting Computers ............ 179
10.2.3 Paper-Based Electronic Voting Systems ................................... 180
10.2.4 Internet Voting Systems ............................................................ 183
10.3 Requirement Documents ............................................................... 184
10.3.1 German Federal Ordinance for Voting Machines .................... 184
10.3.2 Protection Profile for the Digital Voting Pen ............................ 184
10.3.3 Online-Voting System Requirements for Non-parliamentary Elections .................................................... 185
10.3.4 Catalogue of the German Society of Computer Scientists ....... 185
10.3.5 GI/BSI/DFKI Protection Profile ............................................... 185
10.4 Activists’ Activities ........................................................................ 186
10.5 The Federal Constitutional Court Judgment .................................. 186
10.6 Future of Electronic Voting in Germany ........................................ 187
References ............................................................................................. 188

Part III Third Pillar Issues .......................................................................... 191


Diana Alonso Blas

11.1 Introduction .................................................................................... 193
11.2 Amendments with Data Protection Relevance ............................... 195
11.2.1 Preservation of the Specificity of the Eurojust Data Protection Regime .................................................... 195
11.2.2 Clear Definition of National Competences ................................. 196
11.2.3 Extension of the Categories of Personal Data which Eurojust may Legally Process ................................ 196
11.2.4 Improvement of the Information Provision from Member States .................................................................. 198
11.2.5 CMS-Related Issues and Secure Communication with Member States .................................................. 200
11.2.6 Time Limits ............................................................................. 203
11.2.7 Relations with Third Parties .................................................... 205
11.2.8 EU Classified Information ..................................................... 208
11.3 Amendments with Relevance to the Joint Supervisory Body of Eurojust (JSB) .................................................... 208
11.4 Concluding Remarks ...................................................................... 210
<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>The Case of the 2008 German–US Agreement on Data Exchange: An</td>
<td>211</td>
</tr>
<tr>
<td></td>
<td>Opportunity to Reshape Power Relations?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Rocco Bellanova</td>
<td></td>
</tr>
<tr>
<td></td>
<td>12.1 Introduction</td>
<td>211</td>
</tr>
<tr>
<td></td>
<td>12.2 Towards a “Prüm Model”?</td>
<td>212</td>
</tr>
<tr>
<td></td>
<td>12.3 Context: Transitional Periods?</td>
<td>213</td>
</tr>
<tr>
<td></td>
<td>12.5 Memberships and Actors</td>
<td>216</td>
</tr>
<tr>
<td></td>
<td>12.6 Divergences Among Provisions of Prüm Instruments</td>
<td>218</td>
</tr>
<tr>
<td></td>
<td>12.7 Resistance to the “Prüm Model”?</td>
<td>220</td>
</tr>
<tr>
<td></td>
<td>12.8 Final Considerations</td>
<td>222</td>
</tr>
<tr>
<td></td>
<td>References</td>
<td>223</td>
</tr>
<tr>
<td>13</td>
<td>DNA Data Exchange: Germany Flexed Its Muscle</td>
<td>227</td>
</tr>
<tr>
<td></td>
<td>Sylvia Kierkegaard</td>
<td></td>
</tr>
<tr>
<td></td>
<td>13.1 Introduction</td>
<td>227</td>
</tr>
<tr>
<td></td>
<td>13.2 Background</td>
<td>228</td>
</tr>
<tr>
<td></td>
<td>13.3 Substantive Law</td>
<td>232</td>
</tr>
<tr>
<td></td>
<td>13.4 German Hegemony &amp; Democratic Deficit</td>
<td>233</td>
</tr>
<tr>
<td></td>
<td>13.5 Innocent ‘Lambs for Slaughter’</td>
<td>236</td>
</tr>
<tr>
<td></td>
<td>13.6 Data Protection</td>
<td>238</td>
</tr>
<tr>
<td></td>
<td>13.7 Conclusion</td>
<td>240</td>
</tr>
<tr>
<td></td>
<td>References</td>
<td>241</td>
</tr>
<tr>
<td>Part IV</td>
<td>Technology Assessment Views</td>
<td>245</td>
</tr>
<tr>
<td>14</td>
<td>Information Privacy in Europe from a TA Perspective</td>
<td>247</td>
</tr>
<tr>
<td></td>
<td>Walter Peissl</td>
<td></td>
</tr>
<tr>
<td></td>
<td>14.1 Introduction</td>
<td>247</td>
</tr>
<tr>
<td></td>
<td>14.2 About EPTA</td>
<td>248</td>
</tr>
<tr>
<td></td>
<td>14.3 ICT and Privacy in Europe: The First Common EPTA Project ...</td>
<td>249</td>
</tr>
<tr>
<td></td>
<td>14.3.1 Methodology of the Project</td>
<td>250</td>
</tr>
<tr>
<td></td>
<td>14.3.2 Outcome</td>
<td>251</td>
</tr>
<tr>
<td></td>
<td>14.3.3 Some Findings</td>
<td>252</td>
</tr>
<tr>
<td></td>
<td>14.3.4 The Challenges: and How to Deal with Them</td>
<td>253</td>
</tr>
<tr>
<td></td>
<td>References</td>
<td>254</td>
</tr>
<tr>
<td>15</td>
<td>Privacy and Security: A Brief Synopsis of the Results of the</td>
<td>257</td>
</tr>
<tr>
<td></td>
<td>European TA-Project PRISE</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Johann Čas</td>
<td></td>
</tr>
<tr>
<td></td>
<td>15.1 Introduction</td>
<td>257</td>
</tr>
<tr>
<td></td>
<td>15.2 Background and Objectives of PRISE</td>
<td>258</td>
</tr>
<tr>
<td></td>
<td>15.3 Project Methods</td>
<td>259</td>
</tr>
</tbody>
</table>
Part V  Legal Practitioner’s Views  ................................................................. 263

16 The Role of Private Lawyers in the Data Protection World  .......... 265
    Christopher Kuner
    16.1 The Roles of Data Protection Lawyers  .......................................... 265
        16.1.1 Legal Practice ................................................................. 265
        16.1.2 Speaking, Writing, and Other Pro Bono Activities .......... 267
    16.2 The Challenges of Practicing Data Protection Law ............... 267
    16.3 Outlook for Data Protection Law Practice ............................. 268
    16.4 Conclusions ................................................................. 269

17 Transfer and Monitoring: Two Key Words in the Current
    Data Protection Private Practice: A Legal Practitioner’s View ........ 271
    Tanguy Van Overstraeten, Sylvie Rousseau and Guillaume Couneson
    17.1 Introduction ........................................................................... 271
    17.2 International Data Flows: The Issue of Transfer .................. 272
        17.2.1 Unambiguous Consent: A Subsidiary Solution? .......... 273
        17.2.2 Standard Contractual Clauses: A Solution to be
            Further Harmonised ...................................................... 274
        17.2.3 Binding Corporate Rules: The Way Forward ............. 275
        17.2.4 No One Size Fits-All Solution to the Data Transfer .... 277
    17.3 Big Brother Is Watching You: the Issue of Monitoring ........ 277
        17.3.1 Monitoring by Private Companies ................................. 278
        17.3.2 Monitoring by Public Authorities ............................... 283
        17.3.3 Monitoring by Individuals ........................................... 285
    17.4 Conclusion ........................................................................... 285

Part VI  Technologist’s Views ................................................................. 287

18 Architecture Is Politics: Security and Privacy Issues in
    Transport and Beyond ................................................................ 289
    Bart Jacobs
    18.1 Architectural Issues .............................................................. 289
    18.2 What Went Wrong: Smart Cards in Public Transport .......... 291
    18.3 What Can Still Go Right: Road Pricing ............................... 295
    18.4 Privacy and Trust for Business .............................................. 297
    References ................................................................................. 298
19 PETs in the Surveillance Society: A Critical Review of the Potentials and Limitations of the Privacy as Confidentiality Paradigm.......................... 301
  Seda Gürses and Bettina Berendt
  19.1 Introduction ................................................................. 301
  19.2 Privacy as Data Confidentiality and Anonymity .................. 303
    19.2.1 Personal Data as the Focus of PETs ...................... 303
    19.2.2 Anonymity as a Privacy Enhancing Mechanism ....... 305
    19.2.3 Anonymity and Confidentiality in the Internet: Assumptions of PETs .................. 306
  19.3 Surveillance Society and Its Effects on PETs .................... 308
    19.3.1 The Daily Perspective on Surveillance ..................... 308
    19.3.2 The Marketing Perspective on Surveillance .............. 309
    19.3.3 The Political Perspective on Surveillance ............... 309
    19.3.4 The Performative Perspective on Surveillance ......... 310
  19.4 The Information Perspective on Surveillance .................... 311
  19.5 Revisiting the Assumptions ......................................... 313
  19.6 Conclusion .................................................................. 316
References ......................................................................... 319

20 Privacy by Design: A Matter of Choice ........................................... 323
  Daniel Le Métayer
  20.1 Introduction ................................................................. 323
  20.2 What Do We Mean by Privacy by Design? ....................... 323
  20.3 A Matter of Choice ....................................................... 326
  20.4 From a Vicious Cycle to a Virtuous Cycle ...................... 328
    20.4.1 Lawyers and Legislators ....................................... 329
    20.4.2 Computer Scientists .............................................. 331
    20.4.3 A Virtuous Cycle .................................................. 332
References ......................................................................... 332
Data Protection in a Profiled World
Gutwirth, S.; Poullet, Y.; de Hert, P. (Eds.)
2010, XXIII, 334 p., Hardcover