

Contents

Foreword by Gary T. Marx: Privacy Is Not Quite Like the Weather . . .	v
Part I Setting the Scene	
1 Introduction to Privacy Impact Assessment	3
David Wright and Paul De Hert	
1.1 Growing Interest	3
1.2 A Few Key Definitions	5
1.3 A PIA Timeline	8
1.4 Why Carry Out a PIA?	10
1.4.1 To Manage Risks	10
1.4.2 To Derive Benefits	16
1.5 Variations in PIA Approaches	17
1.6 Open Issues	23
1.6.1 Scale and Scope of the PIA	24
1.6.2 Who Should Perform the PIA?	25
1.6.3 Should Engaging External Stakeholders Be Part of the PIA Process?	26
1.6.4 Should PIAs Be Published?	27
1.6.5 Should PIAs Be Mandatory?	28
1.6.6 Should the DPA or Privacy Commissioner “Approve” a PIA?	29
1.6.7 Should a PIA Apply to the Development of New Policy?	30
1.6.8 Two or More Organisations Collaborating on a PIA	30
1.6.9 Are Trans-national PIAs Feasible?	31
1.7 Objectives and Scope of This Book	31
2 A Human Rights Perspective on Privacy and Data Protection Impact Assessments	33
Paul De Hert	
2.1 Terminology	33
2.2 Data Protection Impact Assessments	34
2.3 Privacy Impact Assessment: What Is Privacy?	38

- 2.4 Privacy Impact Assessments: Privacy and Permissible Limitations 40
- 2.5 The Technology Should Be Used in Accordance with and as Provided by the Law (First PIA Element) 45
 - 2.5.1 Open Questions About the Transparency and Legality Requirement 48
- 2.6 The Technology or Processing Should Serve a Legitimate Aim (Second PIA Element) 49
- 2.7 The Technology Should Not Violate the Core Aspects of the Privacy Right (Third PIA Element) 51
- 2.8 The Technology Should Be Necessary in a Democratic Society (Fourth PIA Element) 54
 - 2.8.1 Necessity, Evidence and Politics 56
- 2.9 The Technology Should Not Have or Give Unfettered Discretion (Fifth PIA Element) 59
- 2.10 The Technology Should Be Appropriate, Least Intrusive and Proportionate (Sixth PIA Element) 61
 - 2.10.1 Appropriateness and the Least Intrusive Method 63
 - 2.10.2 The Fair Balance Requirement, Evidence and Precaution 66
 - 2.10.3 The Fair Balance Requirement, Stakeholder Participation and Impact Assessments 70
- 2.11 The Technology Should Not Only Respect Privacy Requirements But Also Be Consistent with Other Human Rights (Seventh PIA Element) 72
- 2.12 Conclusion 74
- 3 (Regulatory) Impact Assessment and Better Regulation 77**
 - David Parker
 - 3.1 The Development of (Regulatory) Impact Assessment 79
 - 3.2 Use of RIA/IA in the UK 81
 - 3.3 RIA/IAs and the European Commission 92
 - 3.4 Conclusions 95
- 4 Prior Checking, a Forerunner to Privacy Impact Assessments 97**
 - Gwendal Le Grand and Emilie Barrau
 - 4.1 Introduction 97
 - 4.2 How Prior Checking Has Been Implemented 98
 - 4.2.1 Prior Checking Has Been Transposed in the National Legislation of Most Member States and Is Used by Most Member States 98
 - 4.2.2 Prior Checking Is Limited to Operations Likely to Present Specific Risks in Most Countries 99
 - 4.2.3 Categories of Processing Operations, When They Are Defined, Are Not Homogeneous 100
 - 4.2.4 Exemptions Are Foreseen in Half of the Countries 102

- 4.2.5 Prior Checking in the Context of National Legislative Measures and Regulations is Carried Out in Half of the Countries 103
- 4.3 How Prior Checking Has Worked in Practice 105
 - 4.3.1 Prior Checking Takes Different Forms at National Level; Data Protection Authorities Use Several Tools 105
 - 4.3.2 The Format and Publicity of the Data Protection Authorities’ Decisions Are Not Harmonised Across Europe 106
 - 4.3.3 Data Protection Authorities Usually Set a Time Limit to Complete Prior Checking 107
 - 4.3.4 In the Context of Prior Checking, Notifications by the Controller Usually Do Not Include More Information than Notifications for Other Types of Processing 108
 - 4.3.5 Data Protection Authorities Have Developed Specific Instruments or Procedures for Processing Operations Subject to Prior Checking 109
 - 4.3.6 Decisions of the Data Protection Authorities Can Generally Be Appealed Before an Administrative Court 110
 - 4.3.7 Data Controllers Who Start Processing Operations Without Notifying the Data Protection Authority Most Likely Get Fined 110
- 4.4 Lessons Learned from Prior Checking 111
 - 4.4.1 Assessment of the Current Prior Checking System and Potential Evolutions 111
 - 4.4.2 Data Protection Authorities Use Tools to Complement Prior Checking 112
 - 4.4.3 What Role for Privacy Impact Assessments? 112
- 4.5 Conclusion 115

Part II Five Countries Lead the Way

- 5 PIAs in Australia: A Work-In-Progress Report 119**
 - Roger Clarke
 - 5.1 Introduction 119
 - 5.2 The Nature of PIAs 120
 - 5.3 The History and Status of PIAs in Australia 120
 - 5.3.1 Pre-2000 122
 - 5.3.2 Post-2000 123
 - 5.3.3 The 10 Contexts 124
 - 5.4 PIA Guidance Documents 137
 - 5.4.1 Evaluation Criteria 137

- 5.4.2 The Victorian Privacy Commissioner’s Guide 138
- 5.4.3 The Australian Privacy Commissioner’s Guide 139
- 5.5 Future Developments 142
 - 5.5.1 The States and Territories 142
 - 5.5.2 The OAPC/ICO 144
 - 5.5.3 The ALRC’s Recommendations 144
 - 5.5.4 The Government’s Response 146
- 5.6 Conclusions 147
- 6 Privacy Impact Assessment – Great Potential Not Often Realised 149**
 - Nigel Waters
 - 6.1 Introduction 149
 - 6.2 A Useful Analogy? 150
 - 6.3 What Is PIA? 150
 - 6.4 PIA and Privacy by Design 150
 - 6.5 PIA and Privacy Auditing 151
 - 6.6 Who Should Be the Client? 152
 - 6.7 In an Ideal World 153
 - 6.8 Using PIA Findings to Effect Change 153
 - 6.9 Some Examples of PIA 155
 - 6.9.1 Online Authentication for e-Government
in New Zealand 155
 - 6.9.2 Retention and Linkage of Australian Census Data 156
 - 6.9.3 The Australian Financial Reporting Regime 156
 - 6.9.4 Individual Identifiers for e-Health in Australia 157
 - 6.9.5 Hong Kong Smart Identity Card 158
 - 6.10 Conclusion 160
- 7 Privacy Impact Assessments in Canada 161**
 - Robin M. Bayley and Colin J. Bennett
 - 7.1 Introduction 161
 - 7.1.1 The Canadian Privacy Legislative Framework 162
 - 7.2 The Conduct of PIAs in Canada 164
 - 7.2.1 The Legal Basis for Privacy Impact Assessments 164
 - 7.2.2 Who Conducts PIAs? 166
 - 7.2.3 Private Sector PIAs 168
 - 7.2.4 When PIAs Are Required 169
 - 7.2.5 PIAs Involving State Security, Law
Enforcement and International Projects
and Agreements 171
 - 7.2.6 PIA Characteristics and Methodology 172
 - 7.2.7 The Audit and Review of PIAs 175
 - 7.2.8 The Publication of PIAs 180
 - 7.3 Conclusions 182

8 Privacy Impact Assessment in New Zealand – A Practitioner’s Perspective 187
 John Edwards

8.1 Introduction 187

8.2 Background 188

8.3 A Short History of Privacy Impact Assessment in New Zealand 188

8.4 Undertaking Privacy Impact Assessments 193

8.5 Timing 194

8.6 The Cost of Privacy Impact Assessment 195

8.7 For Whom Is the Report Prepared? 196

8.8 Problems with Privacy 196

8.9 Independence 199

8.10 Givens 199

8.11 Scope Constraints 200

8.12 Legal Professional Privilege Applies 201

8.13 After the Assessment? 202

8.14 Conclusion 203

9 Privacy Impact Assessment in the UK 205
 Adam Warren and Andrew Charlesworth

9.1 Introduction 205

9.2 Legislative and Policy Framework 207

9.2.1 Legislation 208

9.2.2 Policy 210

9.3 The UK PIA Process 211

9.4 Case Study: Office for National Statistics (ONS), 2011 Census 214

9.5 Lessons Learnt 216

9.6 Future Developments 221

9.7 Conclusion 223

10 PIA Requirements and Privacy Decision-Making in US Government Agencies 225
 Kenneth A. Bamberger and Deirdre K. Mulligan

10.1 Introduction 225

10.2 The US PIA Requirement and Its Implementation 228

10.3 Challenges Inherent in the PIA Model 230

10.3.1 Limits of Process 230

10.3.2 Substantive Barriers to Oversight 231

10.4 Seeking Ways to Overcome Barriers to PIA Success: Learning from the US Experience 235

10.4.1 Lessons from NEPA 236

10.5 Suggestions from the US PIA Experience: The RFID Cases 237

10.5.1 The Cases in Brief 238

10.5.2 Possible Elements of Variance 240

10.6 Status and Independence of Embedded Privacy Experts 241

10.7 Expert Personnel, Integrated Structure and the PIA Tool 245

- 10.7.1 Creating Accountability in the Absence of Oversight: The Privacy and Integrity Advisory Committee 248
- 10.8 Directions for Further Inquiry 249

Part III PIA in the Private Sector: Three Examples

- 11 PIA: Cornerstone of Privacy Compliance in Nokia 253**
 - Tobias Bräutigam
 - 11.1 Introduction 253
 - 11.2 Definitions 255
 - 11.2.1 Privacy 255
 - 11.2.2 Personal Data 256
 - 11.2.3 PCI DSS 256
 - 11.2.4 PIA, PISA 256
 - 11.2.5 Nokia 256
 - 11.3 Nokia’s Approach to Privacy 256
 - 11.3.1 Governance Model 257
 - 11.3.2 Other Measures in Support of Privacy 259
 - 11.3.3 Reasons for Conducting Privacy Assessments 260
 - 11.4 The Process, or How Privacy Assessments Are Conducted 261
 - 11.4.1 Two Kinds of Privacy Assessments 261
 - 11.4.2 Undertaking a PISA 261
 - 11.4.3 The PIA Process – Deviations from PISA 263
 - 11.5 The Content of Privacy Assessments 264
 - 11.5.1 The PISA Template 264
 - 11.5.2 The PIA Template 267
 - 11.6 Areas for Improvement 269
 - 11.6.1 Quality of the Requirements That Are Assessed 269
 - 11.6.2 Resources 270
 - 11.6.3 Awareness 270
 - 11.6.4 Evaluating Findings 271
 - 11.6.5 Information Not Available 271
 - 11.6.6 Corrective Actions 271
 - 11.6.7 Speed of Execution 271
 - 11.7 Conclusion and Summary: 10 Recommendations 271
 - 11.7.1 Start Small, But Start 272
 - 11.7.2 Awareness 272
 - 11.7.3 Privacy Assessments Need to Be Supported by a Governance Model 272
 - 11.7.4 Definitions of Requirements Must be as Self-Explanatory as Possible 273
 - 11.7.5 Include Open Questions in the Assessments 273
 - 11.7.6 Specialisation 273
 - 11.7.7 Cultivate a Culture of Continuous Improvement and Open Communication 273

- 11.7.8 Prioritisation 274
- 11.7.9 Effective Resource Management 274
- 11.7.10 Inclusion of PIA and PISA When Managing Projects 274
- 12 How Siemens Assesses Privacy Impacts 275**
 Florian Thoma
 - 12.1 Siemens at a Glance 275
 - 12.2 Terminology 276
 - 12.3 Some Challenges 276
 - 12.4 The Data Protection Officer’s Tasks 277
 - 12.5 Prior Checking 278
 - 12.6 Processor Audits 279
 - 12.7 Group IT System Assessment: Inter-company Agreements . . 280
 - 12.8 Assessment of Offshoring and Outsourcing Projects 281
 - 12.9 Advantages of Privacy Impact Assessments 282
 - 12.10 Involvement of Data Protection Authorities 283
 - 12.11 Moving Forward 283
- 13 Vodafone’s Approach to Privacy Impact Assessments 285**
 Stephen Deadman and Amanda Chandler
 - 13.1 Introduction 285
 - 13.2 Vodafone’s Core Business Operations 286
 - 13.3 The External and Industry Environment 287
 - 13.4 Vodafone’s Policy and Approach to Privacy Risk Management 287
 - 13.4.1 Governance and Accountability 288
 - 13.4.2 Principles 288
 - 13.5 Privacy Impact Assessments 289
 - 13.6 Vodafone’s Privacy Programme 289
 - 13.7 The Role of the PIA in the Vodafone Privacy Programme . . . 290
 - 13.7.1 Strategic Privacy Impact Assessment 290
 - 13.7.2 Case Study – Location Services 291
 - 13.8 PIA and the Privacy Risk Management System (PRMS) 295
 - 13.8.1 Strategic Aims and Objectives of the PRMS 295
 - 13.8.2 Key Operational Controls in the PRMS 296
 - 13.9 The Role of the Privacy Officer 301
 - 13.10 The Role of Privacy Impact Assessment in the PRMS 302
 - 13.11 Conclusion – The Value of Privacy Impact Assessments 303
- Part IV Specialised PIA: The Cases of the Financial Services Industry and the RFID PIA Framework**
- 14 The ISO PIA Standard for Financial Services 307**
 John Martin Ferris
 - 14.1 Introduction 307
 - 14.2 Overview of the ISO 22307:2008 Voluntary Consensus Standard 308

- 14.2.1 A PIA Is Useful During Any Phase of a System’s Life Cycle 308
- 14.2.2 A PIA Requires a Process Including a Plan 309
- 14.2.3 A PIA Needs an Adequate Description of the System 310
- 14.2.4 A PIA Standard Should Be Neutral on Frameworks That Support a PIA Development . . . 310
- 14.2.5 A PIA Is Not a Privacy Audit 313
- 14.3 History of ISO 22307:2008 313
- 14.4 Voluntary Consensus Standards 315
 - 14.4.1 ISO TC 68 316
 - 14.4.2 Business Challenges of ISO TC 68 and Voluntary Consensus Standards 316
 - 14.4.3 ISO TC 68 Security and Privacy Work 319
 - 14.4.4 Choosing Voluntary Consensus Standards 319
- 14.5 Summary 321
- 15 The RFID PIA – Developed by Industry, Endorsed by Regulators 323**
 - Sarah Spiekermann
 - 15.1 Introduction – The History of the RFID PIA 323
 - 15.2 Preliminary Considerations Before Engaging in a PIA 327
 - 15.3 Initial Analysis to Determine the Scope of PIA 329
 - 15.4 PIA Risk Assessment Process 333
 - 15.4.1 How Is the Risk Assessment Done Step By Step? . . 334
 - 15.5 PIA Reporting 344
 - 15.6 Conclusion 344
- 16 Double-Take: Getting to the RFID PIA Framework 347**
 - Laurent Beslay and Anne-Christine Lacoste
 - 16.1 An Introduction to the RFID Recommendation 347
 - 16.2 Conditions of Involvement of the Art. 29 WP 348
 - 16.3 The Different Actors Involved in the Recommendation 349
 - 16.3.1 The European Data Protection Supervisor 349
 - 16.3.2 The European Network and Information Security Agency 349
 - 16.3.3 Industry 350
 - 16.3.4 National Authorities and Agencies 350
 - 16.4 From a Negative Opinion of the WP29 to a Positive One 350
 - 16.4.1 The July 2010 Opinion of the Art. 29 WP and the Issue of Risk Analysis 350
 - 16.5 Endorsement of the Art. 29 WP: Consequences and Further Steps 354
 - 16.6 PIA in Perspective 356
 - 16.6.1 PIA for RFID Applications and Impact Assessments in a Regulatory Process 356

- 16.6.2 The Issue of Representativeness of the Industry Group 356
- 16.6.3 PIA Procedure: A Voluntary Action 357
- 16.6.4 The PIA Framework for RFID: An Example for Other Technological Fields? 358
- 16.7 Conclusion: Efficiency of PIA and Residual Risk: A Difficult Compromise 358

Part V Specific Issues

- 17 Surveillance: Extending the Limits of Privacy Impact Assessment 363**
Charles Raab and David Wright
- 17.1 Introduction 363
- 17.2 Objections to Subjecting Surveillance to PIA 364
 - 17.2.1 A Brake on Technical Progress 364
 - 17.2.2 Some Surveillance Involves Central Functions of the State 365
 - 17.2.3 Some Surveillance Involves Commercial Sensitivity 366
 - 17.2.4 Some Surveillance Involves More Than One Country 367
 - 17.2.5 Ineffectiveness Would Be Revealed by a PIA 368
 - 17.2.6 PIA Is Too Narrowly Focused 369
- 17.3 Types of Surveillance 369
 - 17.3.1 Watching 370
 - 17.3.2 Listening 370
 - 17.3.3 Locating 370
 - 17.3.4 Detecting 371
 - 17.3.5 Dataveillance 372
 - 17.3.6 Assemblages 372
 - 17.3.7 Surveillance: Causes of Concern 373
- 17.4 Who Are the Surveillants, and Why Do They Use Surveillance? 374
 - 17.4.1 Public Sector 374
 - 17.4.2 Private Sector 375
 - 17.4.3 Society 375
- 17.5 Assessing Surveillance Effects: Privacy and Beyond 376
- 17.6 Conclusion 382
- 18 The Madrid Resolution and Prospects for Transnational PIAs 385**
Artemi Rallo Lombarte
- 18.1 The Madrid Resolution 385
 - 18.1.1 Origin of the Document 385
 - 18.1.2 The Contents of the Madrid Resolution 387
- 18.2 Privacy Impact Assessments in the Madrid Resolution 390
- 18.3 Reception of the Madrid Resolution 392
 - 18.3.1 Towards a Binding International Instrument 392

- 18.3.2 Mexico: First Country to Incorporate the Resolution into Its Legal System 394
- 18.3.3 Europe: Influence of the Madrid Resolution on the “Future of Privacy” 394
- 18.4 Conclusions 395
- 19 Privacy and Ethical Impact Assessment 397**
- David Wright and Emilio Mordini
- 19.1 Introduction 397
- 19.2 Governance Issues in the Practice of an Ethical Impact Assessment 401
 - 19.2.1 The Role of Ethics 401
 - 19.2.2 Consulting and Engaging Stakeholders 402
 - 19.2.3 Accountability 404
 - 19.2.4 Providing More Information, Responding to Complaints and Third Party Ethical Review 405
 - 19.2.5 Good Practice 406
- 19.3 Ethical Principles 406
 - 19.3.1 Respect for Autonomy 407
 - 19.3.2 Dignity 407
 - 19.3.3 Informed Consent 408
 - 19.3.4 Justice 409
- 19.4 Social Cohesion 410
 - 19.4.1 Nonmaleficence (Avoiding Harm) 410
 - 19.4.2 Beneficence 412
 - 19.4.3 Social Solidarity, Inclusion and Exclusion 415
 - 19.4.4 Sustainability 415
- 19.5 Conclusions 416
- 20 Auditing Privacy Impact Assessments: The Canadian Experience . 419**
- Jennifer Stoddart
- 20.1 Introduction 419
- 20.2 Supporting the Performance of PIAs 421
 - 20.2.1 PIAs Are Only as Good as the Processes That Support Them 422
 - 20.2.2 Frameworks Lacking Critical Control Elements Are More Likely to Fail 425
- 20.3 Improving PIA Processes 429
 - 20.3.1 PIAs Should Be Integrated with Other Risk Management Processes 430
 - 20.3.2 PIA Requirements Need To Be Streamlined 430
- 20.4 Need for Strategic Privacy Impact Assessment 432
- 20.5 Enhancing Public Reporting Requirements to Improve PIAs . 433
- 20.6 Conclusion: Evaluating the Effects of Our Audit 434

21 Privacy Impact Assessment: Optimising the Regulator’s Role 437
 Blair Stewart

21.1 Introduction 437

21.2 Approach 438

21.3 Part A: Getting Started 440

21.4 Part B: Getting Through 441

21.5 Part C: Getting Results 441

21.6 Part D: Getting Value 443

21.7 Closing Comments 444

22 Findings and Recommendations 445
 David Wright and Paul De Hert

22.1 PIA Policy Issues: Recommendations for a Better Framework on PIA 446

22.1.1 PIAs Should Be Conducted by Any Organisation Impacting Privacy 446

22.1.2 PIA Needs Champions, High Level Support and an Embedded Privacy Culture 446

22.1.3 A PIA Should Be “Signed Off” by a High-Level Official and Tied to Funding Submissions 448

22.1.4 Risk Management Should Be a Part of PIA, and PIA Should Be Part of Risk Management 448

22.1.5 Privacy Commissioners Should Play a Key Role in PIA 449

22.1.6 Prior Checking and PIA Should Be Complementary, But Their Mutual Relationship Needs More Study 450

22.1.7 Transparency Contributes to the Success of a PIA 452

22.1.8 Publish the Results of the PIA and Communicate with Stakeholders, Including the Public 453

22.1.9 Guard Against Conflicts of Interest 454

22.1.10 Ensure Third-Party Review and Audit of PIAs 455

22.1.11 Common Standards and Good Practice Need To Be Better Identified 456

22.1.12 Create a Central Registry of PIAs 457

22.1.13 Multi-agency and Transnational Projects Should Be Subject to PIA 458

22.1.14 Should PIAs Be Mandatory? 459

22.2 PIA Practice: Guidance for Individual PIAs 462

22.2.1 When Is a PIA Necessary? 462

22.2.2 Determine the Objectives, Scale and Scope of the PIA 463

22.2.3 Initiate a PIA Early, When It Is Possible to Influence Decision-Making 465

- 22.2.4 Who Should Initiate and Conduct the PIA? 465
- 22.2.5 Describe the Proposed Project and Map
the Information Flows 466
- 22.2.6 Identify and Engage Stakeholders 466
- 22.2.7 A Compliance Check Is Only Part of a PIA 470
- 22.2.8 A PIA Should Address All Types of Privacy 471
- 22.2.9 . . . and Other Values Too 472
- 22.2.10 With Stakeholders, Identify the Risks and
Impacts of the Project 473
- 22.2.11 Questions 473
- 22.2.12 Identify Options (Controls) for Avoiding or
Mitigating Negative Privacy Impacts 474
- 22.2.13 Justify the Business Case for the Residual
Risk and Maintain a Risk Register 474
- 22.2.14 Review and Update the PIA as the Project
Progresses 475
- 22.2.15 Prepare the PIA Report and Implement the
Recommendations 476
- 22.2.16 Training and Raising Awareness 476
- 22.2.17 PIA Has Value – Get It! 477
- 22.3 Room for Improvement and Concluding Remarks 478
- About the Authors 483**
- References 493**
- Index 519**