

Contents

1	Introduction	1
1.1	Escalating Technological Threats to Privacy	1
1.2	Core Theme of the Book	3
1.3	Rationale for the Case Studies Selection	5
1.4	Key Questions of Interest	7
1.5	Added Value	8
1.6	Structure and Overview of Chapters	9
	References	10
 Part I Principles of Privacy		
2	Privacy, Liberty and Security	13
2.1	Introduction	13
2.2	The Concept of Privacy	14
2.3	Privacy as an International Human Right	17
2.4	The Merits of Privacy	18
2.5	The Concept of Liberty	19
2.6	Privacy and Liberty	20
2.7	The Concept of Security	21
2.8	Privacy, Liberty and Security	22
	References	25
3	Assessing the Adequacy of a Privacy Legal Framework	27
3.1	Introduction	28
3.2	An Adequate Privacy Legal Framework?	28
3.3	International Consensus in Principle	29
3.4	Purpose and Meaning of Each Principle	31
3.4.1	Choice/Consent	32
3.4.2	Access/Participation	33
3.4.3	Notice/Awareness	34
3.4.4	Integrity/Security	35
3.4.5	Enforcement/Redress	36

- 3.4.6 Purpose Specification 37
- 3.4.7 Use Limitation 38
- 3.4.8 Proportionality 38
- 3.5 The EU Approach Versus the US Approach. 39
- 3.6 Required Legal Characteristics 41
- 3.7 Basic Pre-measures. 42
- 3.8 Legal Criteria Specific to the US and UK 43
- 3.9 Applying the Privacy Principles of the Twentieth Century to the
Technological Advancements of the Twenty-First Century 43
- References 44

Part II Technological Threats to Privacy

- 4 Privacy-Invasive Technologies 49**
 - 4.1 Introduction 49
 - 4.2 A Definition of PITs. 50
 - 4.3 The Growing Deployment and Threat of PITs. 50
 - 4.4 PITs and the Human Body 51
 - 4.5 PITs and the Public Space 53
 - 4.6 Other PITs that May Pose Serious Threats to Privacy and Liberty. 58
 - 4.6.1 Neurotechnology 60
 - 4.6.2 Unmanned Aerial Vehicles 61
 - 4.6.3 Lexid. 63
 - 4.6.4 DNA Analysis. 64
 - 4.6.5 Automatic License Plate Recognition 68
 - References 68
- 5 Body Scanners: A Strip Search by Other Means? 71**
 - 5.1 Introduction 72
 - 5.2 A Strip Search by Other Means? 72
 - 5.3 How Backscatter Body Scanners Work 74
 - 5.4 Security Benefits and Drawbacks. 75
 - 5.5 The Plausibility of the Threat Posed by Plastic Guns,
Ceramic Knives, and Liquid/Chemical and Plastic Explosives 77
 - 5.6 Alternatives to Backscatter Body Scanners 79
 - 5.7 Scope of Deployment in the US. 84
 - 5.8 Laws, Codes, Decisions and Other Legal Instruments
of Special Relevance in the US 86
 - 5.9 Deficiencies and Dilemmas of the US Legal Framework 91
 - 5.10 Policy-Relevant Recommendations 99
 - 5.10.1 Focus on Manufacturer-Level Regulations/Laws. 99
 - 5.10.2 Focus on User-Level Regulations/Laws. 102
 - 5.11 Manufacturer-Level or User-Level Regulation?. 104

5.12 International Deployment, Developments and Responses 105

5.13 Concluding Remarks 108

References 109

6 Public Space CCTV Microphones and Loudspeakers:

The Ears and Mouth of “Big Brother” 113

6.1 Introduction 114

6.2 The Privacy-Intrusive Evolution of CCTV Surveillance
Technology 114

6.3 The Ears and Mouth of “Big Brother” 116

6.3.1 The Ears (CCTV Microphones) 118

6.3.2 The Mouth (CCTV Loudspeakers) 120

6.4 Scope of Deployment in the UK 121

6.4.1 CCTV Microphones 121

6.4.2 CCTV Loudspeakers 122

6.5 Security Gains 125

6.5.1 CCTV Microphones 125

6.5.2 CCTV Loudspeakers 127

6.6 Alternatives to CCTV Microphones and Loudspeakers 128

6.6.1 Alternatives to CCTV Microphones 128

6.6.2 Alternatives to CCTV Loudspeakers 129

6.7 Laws, Codes, Decisions and other Legal Instruments
of Special Relevance in the UK 130

6.7.1 CCTV Microphones 135

6.7.2 CCTV Loudspeakers 136

6.8 Deficiencies and Dilemmas of the UK Legal Framework 137

6.8.1 CCTV Microphones 137

6.8.2 CCTV Loudspeakers 144

6.9 Policy-Relevant Recommendations 146

6.9.1 CCTV Microphones 147

6.9.2 CCTV Loudspeakers 149

6.10 Concluding Remarks 154

References 154

**7 Human-Implantable Microchips: Location-Awareness
and the Dawn of an “Internet of Persons” 157**

7.1 Introduction 158

7.2 RFID/GPS Implants and the Technology Behind Them 160

7.2.1 RFID Implants 160

7.2.2 GPS Implants 162

7.3 Location-Awareness and the Dawn of an
“Internet of Persons” 164

7.3.1 The Capabilities of HIMs 164

7.3.2 Location Information 168

7.3.3	Social and Privacy Implications	170
7.3.4	A Means of Control	171
7.3.5	An “Internet of Persons”: A Possible Dystopian Future?	172
7.3.6	Are We Nearly There?	178
7.4	Potential Security and Well-Being Benefits	180
7.5	Security Risks and Drawbacks	183
7.6	Scope of Deployment	187
7.6.1	Actual Deployment in the US	187
7.6.2	Potential Deployment	190
7.6.3	Actual and Potential International Deployment	198
7.7	Alternatives to HIMs	199
7.8	Laws, Codes, Decisions and Other Legal Instruments of Special Relevance in the US	201
7.8.1	Constitutionally Protected Rights	201
7.8.2	Federal Statutory Laws	201
7.8.3	Tort Law	204
7.8.4	Case Law	204
7.8.5	State Statutory Laws	206
7.8.6	Administrative Decisions	207
7.8.7	Standards, Guidelines and Self-regulations	208
7.9	Deficiencies and Dilemmas of the US Legal Framework	209
7.10	Policy-Relevant Recommendations	226
7.10.1	Consent	229
7.10.2	Proportionality	231
7.10.3	Purpose Specification	232
7.10.4	Use Limitation	235
7.10.5	Enforcement, Accountability and Redress	236
7.10.6	Access and Participation	238
7.10.7	Notice and Awareness	239
7.10.8	Security	241
7.10.9	Privacy Impact Assessment	242
7.10.10	Definitions	243
7.10.11	Constitutional and Case Law Considerations	244
7.10.12	The International Dimension	245
7.11	Concluding Remarks	246
	References	246
8	New Privacy Threats, Old Legal Approaches:	
	Conclusions of Part II	251
8.1	The New Threats to Privacy	251
8.2	Beyond Privacy and Data Protection	253
8.3	Deficiencies of the Existing Privacy Legal Frameworks	255
	Reference	256

Part III New Approach to Protecting Privacy

9 The Value, Role and Challenges of Privacy by Design 259

9.1 Introduction 260

9.2 Concept, Theory and Origins of PBD 260

9.3 PBD Methodology 266

9.4 PBD Solutions for: Body Scanners, HIMs, CCTV
Microphones and Loudspeakers 268

9.5 PBD Versus PETs 270

9.6 PBD in the Current US and UK/EU Legal Frameworks 272

9.6.1 US Legal Framework 272

9.6.2 EU Legal Framework 273

9.7 Growing Widespread Recognition 274

9.8 Potentially Growing Application 278

9.9 A Unique Selling Point and Source of Value Creation 279

9.10 The Growing Lack of Trust 281

9.11 Potential Criticism 282

9.12 Practical Challenges of Implementing PBD 283

9.13 Concluding Remarks 285

References 286

Part IV Research Results

10 Conclusions and Policy Implications 291

10.1 Introduction 292

10.2 Keeping Up with the Technology 292

10.3 PBD: Critical Combination of Technology and Law 293

10.4 Not a Substitute for Law 299

10.5 Flexibility vs. Specificity 300

10.6 Radical Changes for Radical Capabilities 301

10.7 Implementation, Enforcement, Monitoring and Evaluation 306

10.8 Accountability, Sanctions and Recalls 307

10.9 Certified Privacy-Friendly 309

10.10 Designing for Privacy 311

10.11 Adequate PBD Solutions 312

10.12 Avoiding Overregulation 313

10.13 Furthering Deployment and Innovation 316

10.14 Safeguarding Privacy, Liberty and Security 318

10.15 Using Privacy-Friendly Alternatives 320

10.16 Countering Potential Criticism of PBD 320

10.17 Overcoming Some of the Challenges 321

10.18 Engaging Relevant Stakeholders 322

10.19	Not a Panacea: The Limitations and Constraints of PBD	323
10.20	Final Conclusions.	328
	References	329
	Appendix A: A3-Report	331
	Appendix B: Summary Table.	333
	Index.	337



<http://www.springer.com/978-94-6265-025-1>

Privacy-Invasive Technologies and Privacy by Design
Safeguarding Privacy, Liberty and Security in the 21st
Century

Klitou, D.

2014, XIX, 338 p. 8 illus., Hardcover

ISBN: 978-94-6265-025-1

A product of T.M.C. Asser Press