Contents

1 Introduction: Subject, Methodology and Structure 1
  1.1 Subject 1
  1.2 Methodology of the Research 5
  1.3 Structure of the Book 9

Part I The Concept of Biometric Data

2 An Introduction into the Use of Biometric Technology 15
  2.1 A Long History of Use of Biometric Characteristics 15
    2.1.1 The Use of Biometric Characteristics in Ancient Times 15
    2.1.2 The Scientific Study of Fingerprint, Anthropometry and Dactyloscopy since the Seventeenth Century 16
    2.1.3 Last Decades of the Twentieth Century: Automated Biometric Techniques Develop 18
  2.2 The Functioning of a Biometric System 19
    2.2.1 Biometric Characteristics Used in Biometric Systems 20
    2.2.2 Use of Biometric Characteristics and Functionalities of a Biometric System 36
    2.2.3 Medical Aspects of Biometrics 63
    2.2.4 Biometric Applications in the Public and Private Sector 64
    2.2.5 Standardization Efforts in the Field of Biometrics 81
  2.3 Preliminary Conclusions 84

3 Biometric Data, Data Protection and the Right to Privacy 87
  3.1 Biometric Data and the Concept of Personal Data 89
    3.1.1 The Emergence of the Data Protection Legislation and the Concept of Personal Data 90
    3.1.2 Are Biometric Data Personal Data? 94
    3.1.3 Are Biometric Data 'Sensitive Personal Data'? 124

3.1.4 Which Personal Data are Biometric Data? 144
3.1.5 Ownership of Biometric Data? 175
3.2 Biological Material and Other Information Relating to Individuals 179
3.2.1 Biological Material 179
3.2.2 Facial Images 190
3.2.3 The Use of Fingerprints in Non-automated Applications 198
3.2.4 Genetic Information and DNA Analysis 199
3.3 Biometric Data, Data Protection and Privacy 224
3.3.1 Biometric Data and the Data Protection Legislation 224
3.3.2 The Fundamental Rights to Data Protection and to Privacy and Biometric Data 228
3.4 Preliminary Conclusions 267
3.5 Preliminary Conclusions for Part I 269

Part II The Processing of Biometric Data and the Proportionality Principle

4 The Risks Involved upon the Use of Biometric Data and Biometric Systems 275
4.1 The Risks which Relate to the Nature Itself of Biometric Data 275
4.1.1 Biometric Data Permit to Identify Individuals 276
4.1.2 Biometric Data can be Used as Universal Unique Identifiers 306
4.1.3 Biometric Data may Reveal Information Relating to Racial or Ethnic Origin and may Concern Health 319
4.1.4 Biometric Data are Vulnerable: Traces, Forgery and Theft 335
4.1.5 Biometric Data and Profiling 349
4.2 The Risks relating to the Architecture and the Specifications of a Biometric System 352
4.2.1 Biometric Data stored in a Central Database versus Biometric Data Locally stored on an Object under the Control of the Data Subject 353
4.2.2 Biometric Systems Only Compare and are Never 100 % Accurate 363
4.2.3 FRR and the FAR depend on Several Factors and are set in Function of the Application 366
4.2.4 Multiple Attack Scenarios and Security Risks 367
4.3 The Risks Relating to the Use of a Biometric System 372
4.3.1 Difficulties during Enrolment 372
4.3.2 The Biometric System may Instigate Discriminatory Effects 374

4.3.3 Biometric Systems shall Not Provide for Automated Decisions 376
4.3.4 Use of Biometric Data for Incompatible Purposes and Re-use of Biometric Data ('Function Creep') 377
4.4 Ethical and Societal Issues 388
4.4.1 Ethical Issues 389
4.4.2 Societal Issues 393
4.5 Preliminary Conclusions 395

5 The Proportionality Principle as a General Principle of Law Applied to Biometric Data Processing 403
5.1 The Proportionality Principle in General 405
5.1.1 Origin of the Proportionality Principle in National Legal Systems 405
5.1.2 The Significance of the Proportionality Principle in Particular Domains 408
5.2 The Proportionality Principle and Directive 95/46/EC 418
5.2.1 Personal Data Must Be 'Adequate, Relevant and Not Excessive (…)' 419
5.2.2 The Personal Data Processing Must Be 'Fairly' and 'Lawfully' and 'For Legitimate Purposes (…)' 426
5.3 The Proportionality Principle and Article 8 ECHR 453
5.3.1 The Proportionality Principle in Combination with the Legality and the Legitimacy Requirement 456
5.3.2 The Margin of Appreciation of the National Authorities 491
5.3.3 Modern Techniques of Identification and Proportionality 494
5.4 New Criteria for the Proportionality Principle under Article 7 and 8 EU Charter and Article 52 EU Charter? 495
5.5 DPAs in Selected Legal Systems and Their Opinions and Decisions Relating to Biometric Applications 499
5.5.1 Belgium 500
5.5.2 France 517
5.5.3 The Netherlands 549
5.6 Preliminary Conclusions 564

6 Strengths and Weaknesses of the Proportionality Principle for Biometric Applications 569
6.1 General 569
6.1.1 A Double Review of the Proportionality of Biometric Data Processing 570
6.1.2 The Proportionality Review under Article 8 §2 ECHR remains Applicable in case the Directive 95/46/EC Does Not Apply 572
6.1.3 The Proportionality Principle Permits to Tackle Fundamental Issues of Society 574

6.2 The Proportionality Principle and the Criteria Used by the DPAs 574
6.2.1 The Processing of Biometric Data for Legitimate Purposes 575
6.2.2 The Biometric Data Processing shall be Adequate, Relevant and Not Excessive 581
6.2.3 The Fair Processing of Biometric Data 584
6.2.4 About the Interference with Fundamental Rights and the Proportionality Thereof 587
6.2.5 Other Criteria put forward by the DPAs for the Evaluation of Biometric Systems 597
6.3 Evaluation 599
6.3.1 Strengths 599
6.3.2 Limits 604
6.4 Absence of Sufficient Protective Measures in Legislation Endangers the Application of the Proportionality Principle and the Balancing of Interests 614
6.4.1 Positive Obligation of States to Protect an Individual's Right to Respect for Private Life 614
6.4.2 The Directive 95/46/EC Refers to Additional Exemptions for Sensitive Data Processing 'For Reasons of Substantial Public Interest' 617
6.4.3 Lack of Legal Criteria for the Use of Biometric Data Endangers the Application of the Proportionality Principle and the Balancing 618
6.5 Preliminary Conclusions 619
6.6 Preliminary Conclusions for Part II 623

Part III Assessment and Recommendations for Strengthening the Data Protection Framework for Biometric Data

7 The Criteria for the Correct 'Balancing of Rights' 631
7.1 General 631
7.1.1 Necessity and Proportionality 631
7.1.2 Balancing of Rights? 634
7.1.3 The Principle of Availability in Conflict with the Principle of Proportionality? 639
7.1.4 Reform of the Directive and the Need for a Comprehensive Framework 643
7.2 The Criteria which Are Relevant for Limiting Interference and as Safeguards for the Use of Biometrics 644
7.2.1 The Use of Templates versus the Use of Samples 646
7.2.2 Verification Versus Identification and Place of Storage 647
7.2.3 Distinction between Biometric Characteristics which Leave Traces and Characteristics which do Not is Outdated 654

7.2.4 Control by the Data Subject ... 657
7.2.5 Revocability and Measures Protecting against Identity Theft and Misuse ... 673
7.2.6 Use of Biometric Data in an Anonymous or Pseudonymous Way ... 674
7.2.7 Accuracy, Efficiency and Reliability ... 689
7.3 Interest and Practical Cases of Biometric Data Processing in the Private Sector ... 692
7.3.1 Biometric Systems in the Employment Context ... 696
7.3.2 Biometric Access Control to Private Clubs and Private Places Open to the Public ... 705
7.3.3 Schools and Biometric Access Control Systems ... 708
7.3.4 Biometric Access Control for Customers ... 712
7.3.5 The Use of Facial Images on Social Networks Sites ... 716
7.3.6 Use of Biometric Systems at Public Events or Places ... 721
7.3.7 The Use of Biometric Data for Testing and Research Purposes ... 724
7.3.8 Biometric Systems for Purely Personal or Household Activities ... 729
7.3.9 Special Case Study: Biometric Identifiers in Passports and Travel Documents ... 730
7.3.10 Comparison: The case of the Body Scanners and Relevant Criteria ... 740
7.4 Preliminary Conclusions ... 742

8 The Need for a Consistent Legal Regulation of Biometric Data ... 745
8.1 The Deficiencies in the Existing Data Protection Legislation ... 747
8.1.1 The Existing Data Protection Legislation Disregards the Specific Nature of Biometric Data ... 747
8.1.2 The Supervision and the Enforcement of the Data Protection Legislation is Different from Country to Country ... 750
8.1.3 Legislation should be Technology Neutral ... 752
8.1.4 Towards More Precise Conditions for the Processing of Biometric Data in Legislation ... 754
8.2 Evaluation of Previous Initiatives ... 758
8.2.1 Self-Regulation/Co-Regulation ... 758
8.2.2 Privacy by Design, Privacy Enhancing Technologies (PETs) and Best Available Techniques ... 766
8.2.3 Legislative Measures ... 779
8.3 Additional Recommendations ... 791
8.3.1 Use of Privacy-Enhancing Practices and Technologies for the Processing of Biometric Data ... 792

8.3.2 Security and Organizational Aspects of Biometric Systems 808
8.3.3 Transparency for the Data Subject and Role of Certification 819
8.3.4 Adoption of appropriate Legislation 822
8.4 Preliminary Conclusions 829

9 A Legal Model for the Use of Biometric Data in the Private Sector 831
9.1 General Principles 836
9.1.1 General Principle #1: Consent for the Use of Facial Images in Biometric Systems 836
9.1.2 General Principle #2: An Alternative System shall be provided if the Processing of Biometric Data Relies upon Consent 838
9.1.3 General Principle #3: No Hidden or Secret Collection of Biometric Data 839
9.1.4 General Principle #4: General Prohibition to Use Biometric Systems for Identification Purposes Without Explicit Law 839
9.1.5 General Principle #5: Limitation of the Use of Biometric Data as Unique Identifier 842
9.1.6 General Principle #6: Prohibition to Use Biometric Data for Racial or Ethnic Origin or Health Information and Confirmation of Prohibition to Discriminate 844
9.1.7 General Principle #7: Respect for Human Dignity Shall Prevail at All Times 847
9.2 Biometric Data Shall in Principle Not be Stored in Central Databases and Only be Used for Verification 848
9.2.1 An Explicit Prohibition to Store Biometric Data in Central Databases 848
9.2.2 Limited Exceptions Determined by Law 851
9.3 Prohibition to Store Biometric Samples and Use of Privacy-Enhancing Technologies 855
9.3.1 Storage of only (Protected) Templates 855
9.3.2 The Use of Privacy-Enhancing Technologies 856
9.3.3 Semi-anonymous and Anonymous Biometric Verification 859
9.4 Distinct Use by the Private and Public Sector 860
9.4.1 Access to Biometric Data Held in the Private Sector by Public Authorities Requires a Legal Basis 860
9.4.2 Private Public Partnerships 862

9.5 Processing of Biometric Data shall be under the Control of the Data Subject 863
9.5.1 Storage on a Device under the Control of the Data Subject 864
9.5.2 Other Means for Processing Under the Control of the Data Subject? 866
9.6 Enhanced Rights for the Data Subjects 866
9.6.1 Transparency of the Biometric Data Processing: Data Subjects shall receive Additional Information 867
9.6.2 Right of Appeal 871
9.6.3 Data Subjects shall be entitled to Multiple Revocable Biometric Pseudonymous Identities and Anonymity as much as Possible 872
9.7 Security Criteria for Biometric Systems 873
9.7.1 Security Measures for the Deployment of Biometric Applications in General 873
9.7.2 Specific Security Measures for the Processing of Biometric Data 876
9.7.3 The Enrolment Phase: Additional Safeguards Needed 877
9.7.4 Data Breach Notification for Biometric Data? 879
9.8 Organizational Measures 880
9.8.1 Specification of the Fall Back Procedures in Case of Failure of a Biometric System 881
9.8.2 Obligation to Detail Duration of Storage, Usage, Access and Procedures for (Automated) Erasure and Destruction 882
9.8.3 Adoption of Security and Revocation Procedures 883
9.8.4 Organization of Alternative Measures in case the Data Subject Refuses Consent or Objects and Right to Appeal 883
9.9 Certification 885
9.9.1 Content of Certification Programs 885
9.9.2 Measures Against Possible Discriminatory Effects 887
9.9.3 Certification of Services and Test Centers 887
9.10 Liability and Remedies 887
9.10.1 Contractual Liability in Relation with Biometric Systems 888
9.10.2 Liability and Remedies in Case of Security Breach and/or Abuse of Biometric Data 891
9.10.3 Liability for the Designers of Biometric Systems? 894
9.11 Preliminary Conclusions 896
9.12 General Conclusions 898

Bibliography 909
I Legislation 909
II Standardization 923
III Case Law 923
IV Doctrine 927
V Reports and studies 950
VI Papers, policy documents and conference proceedings 956
VII Miscellaneous 962

Index 965