

Contents

1	Introduction	1
1.1	The Digitised Image and Face Recognition Technology	1
1.2	Face Recognition Technology	2
1.3	Face Recognition Technology and Privacy	3
1.4	Face Recognition Technology and Surveillance	5
1.5	Face Recognition Technology and Its Ethical and Legal Implications	5
1.6	Face Recognition Technology and Personal Autonomy	6
1.7	Face Recognition Technology and Big Data	6
	References	7
2	What Is Face Recognition Technology?	9
2.1	Introduction: What Is Face Recognition Technology?	9
2.2	How Does Face Recognition Work?	10
2.3	Face Recognition Algorithms	11
2.4	Other Approaches	14
2.5	Weaknesses and Failures of FRT	15
2.6	Face Recognition Vulnerability	15
2.7	Face Spoofing Counter-Measures	16
2.8	Current Uses of Face Recognition Technology	17
	2.8.1 Passports and Other Government Uses	17
	2.8.2 Law Enforcement	19
	2.8.3 Commerce	20
	2.8.4 Gambling and Banking	22
	References	23
3	Some Ethical and Legal Issues of FRT	27
3.1	Fears and Misconceptions of FRT	27
	3.1.1 Disney World	28
	3.1.2 Driver Licences	28
	3.1.3 New York Domain Awareness System	30

3.2	Some Deeper Issues: FRT, Data Protection and Civil Liberties	31
3.3	Face Recognition: Civil Liberty and Public Disclosure	33
3.3.1	Public Disclosure	34
3.3.2	Public Interest Disclosure and FRT	36
	References	36
4	Privacy and Surveillance Surveyed	39
4.1	Introduction: Privacy and Surveillance	39
4.2	The Data Subject and Surveillance	41
4.3	Biometric Data and Civil Liberties	43
4.4	The Data Subject and Privacy	46
4.5	The Data Subject and Autonomy	46
4.6	Privacy, Informatisation and Photography	49
4.7	The Data Subject and Biometric Data	52
4.8	The Socio-Political Context	53
	References	55
5	Autonomy, Liberty and Privacy	57
5.1	The Concept of Autonomy	57
5.2	Freedom & Privacy	59
5.3	Dworkin's First and Second-Order Autonomy	60
5.4	Autonomy and Freedom	63
5.5	Negative and Positive Liberty	64
5.6	Kafka and Negative Liberty	65
5.7	Foucault's Police and Bentham's Prisoners	66
5.8	Privacy and Autonomy	68
	References	73
6	Compulsory Visibility?	75
6.1	Introduction	75
6.2	Body-Worn Cameras	76
6.3	Compulsory Visibility and Coercion	76
6.4	Compulsory Visibility and Face Recognition	79
6.5	Big Data	80
6.6	Big Data and Face Recognition	81
6.7	Compulsory Visibility and Autonomy	82
	References	84
7	The Law and Data Protection	87
7.1	Introduction	87
7.2	Data Protection and Privacy	89
7.3	Informational Privacy	91
7.4	Data Protection and Privacy: The United States Sectoral Approach	93
7.5	Reconciling US and EU Provisions	96

- 7.6 Data Protection and Face Recognition 97
- 7.7 Biometric Data and the Development of the General Data Protection Regulation 101
- 7.8 Human Rights: Civil Liberty, Privacy and the Law 105
- References 109
- 8 The Law and Surveillance 113**
 - 8.1 Surveillance, Regulatory Power and Rights 113
 - 8.2 Human Rights, Mass Surveillance and UK Case Law 118
 - 8.2.1 Human Rights: Interference 120
 - 8.3 Face Recognition: Accountability and Trust 122
 - 8.4 Face Recognition: Privacy and Image Ownership 122
 - References 123
- 9 State Paternalism and Autonomy 125**
 - 9.1 State Paternalism: Active and Passive 125
 - 9.2 Ethics and State Power 127
 - 9.2.1 Liberty and State Power 128
 - 9.2.2 Ethical State Power 130
 - 9.3 Paternalism and FRT 131
 - 9.4 Control, Paternalism and Autonomy 132
 - 9.5 Citizen and State 134
 - 9.6 Face Recognition and Second-Order Preferences 137
 - 9.7 Preventing Harm and the Effect on Second-Order Preferences 138
 - 9.8 Threats to Privacy 142
 - References 145
- 10 State Paternalism and Data 147**
 - 10.1 Protecting Privacy: Data Protection and the Political Dimension 147
 - 10.2 Protecting Privacy: UK Data Protection and the Face Recognition Paradigm 151
 - 10.3 Data Processing and Second-Order Preferences 154
 - 10.4 The Data Subject and Face Recognition Systems [State Data-Mining Power] 156
 - References 160
- 11 The Future of Face Recognition Technology and Ethico: Legal Issues 163**
 - 11.1 Face Recognition: The Future and Its Implications 163
 - 11.2 Threat Recognition and Securitising Identity 163
 - 11.3 Identity Management 166
 - 11.4 Face Recognition and the Human Interface 168
 - 11.4.1 Data and the Human Interface 170
 - 11.5 Predicting Social Concerns and Reactions 172

11.6	Constitutional Safeguards and Rights	174
11.7	Legal and Regulatory Safeguards	176
11.8	Regulating the Commoditisation of Data	180
	References	181
12	Conclusion	185
12.1	Face Recognition Technology and the Right to Personal Image Ownership	185
12.2	Data Ownership: A New Legal and Moral Rights Framework	186
12.3	Democratisation of Technology Development	189
12.4	Personal Identifiable Images and Street Photography	190
12.5	Recommendations	191
	References	192
	Bibliography and Further Reading	195
	Index	199