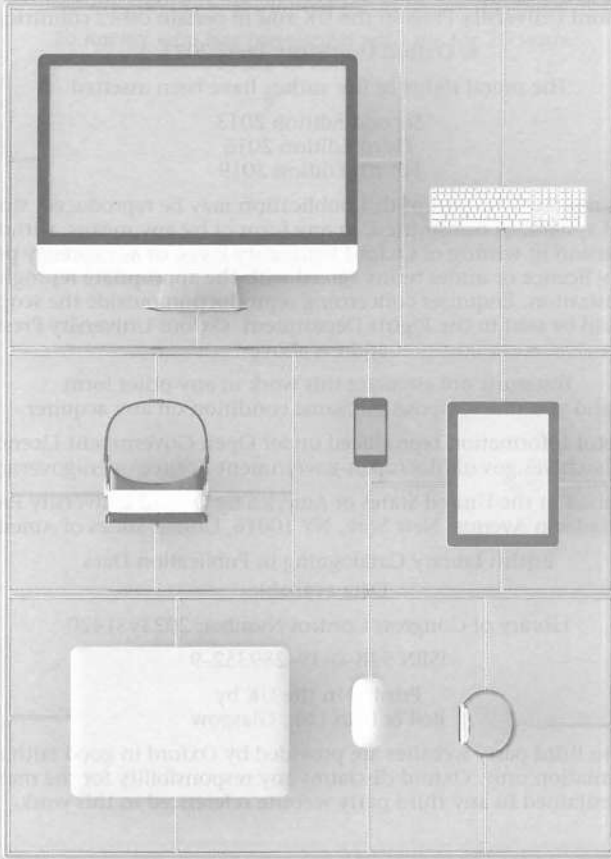


ANDREW MURRAY

PROFESSOR OF LAW, LONDON SCHOOL OF ECONOMICS AND POLITICAL SCIENCE



FIFTH EDITION

INFORMATION TECHNOLOGY LAW

THE LAW AND SOCIETY

OXFORD
UNIVERSITY PRESS

CONTENTS

GUIDE TO THE BOOK	XIX
GUIDE TO THE ONLINE RESOURCES	XX
TABLE OF CASES	XXI
TABLE OF LEGISLATION	XXXIII

PART I THE INFORMATION SOCIETY

1. The world of bits

1.1 An introduction to bits	5
1.1.1 The process of digitization	6
1.2 Moving from atoms to bits	8
1.2.1 Rivalrous and nonrivalrous goods	10
1.2.2 Digital products and society	11
1.3 The legal challenges of the information society	13
1.3.1 Digital convergence	15
1.3.2 The cross-border challenge of information law	17
1.4 Digitization and law	19

2. The network of networks

2.1 Internet history	22
2.1.1 Building the ARPANET	23
2.1.2 Building the internet	24
2.2 How the modern internet functions	27
2.3 Higher-level protocols	31

3. Net neutrality

3.1 Challenges to net neutrality	38
3.2 Regulating net neutrality	42
3.3 The legal framework	45
3.4 Conclusions	56

4. Regulating the information society

4.1 Cyberlibertarianism	59
-------------------------	----

4.2	Cyberpaternalism	64
4.2.1	Lawrence Lessig's modalities of regulation	65
4.3	Network communitarianism	67
4.3.1	Symbiotic regulation	72
4.4	Intermediary and platform regulation	74
4.4.1	Internet intermediaries	75
4.4.2	Platform power and platform regulation	77
4.5	Behavioural regulation	82
4.5.1	Nudging and libertarian paternalism	84
4.6	Algorithmic regulation	86
4.7	Conclusions	89
PART II CONTENT AND THE INFORMATION SOCIETY		93
5.	Cyber-speech	95
5.1	Introduction	95
5.2	Platforms and content hosts	96
5.2.1	Websites and internet fora	97
5.2.2	Social media platforms (SMPs)	98
5.3	Freedom of expression and social responsibility	99
5.3.1	Freedom of expression: the 'First Amendment' approach	99
5.3.2	Freedom of expression: the European approach	100
5.3.3	Freedom of expression: the approaches compared	101
5.3.4	<i>LICRA et UEJF v Yahoo! Inc. and Yahoo! France</i>	102
5.3.5	Cross-border speech	104
5.3.6	<i>Yahoo! Inc. v LICRA</i>	105
5.4	International orders and comity	106
5.5	Political speech	113
5.5.1	Online political speech	114
5.5.2	Astroturfing, #fakenews, and bots	117
5.5.3	Regulating harmful online political speech	121
5.6	Hate speech	126
5.6.1	Hate speech and society	126
5.6.2	Inter-state speech	128
5.7	Conclusions: cyber-speech and free expression	130

6. Social networking and antisocial conduct	133
6.1 Introduction	133
6.2 Social networking, gossip, and privacy	135
6.2.1 Spring 2011 and the Ryan Giggs affair	139
6.2.2 <i>PJS v News Group Newspapers</i>	142
6.3 Harmful communications	146
6.3.1 <i>Chambers v DPP</i>	146
6.3.2 Harmful communications post <i>Chambers</i>	149
6.4 Cyberbullying, trolling, and harassment	154
6.5 Reforming the communications offences	159
6.6 Conclusions	165
7. Defamation	167
7.1 The tort of defamation	168
7.1.1 Statements and publication	169
7.1.2 Taking jurisdiction in claims against non-UK respondents	171
7.1.3 Defences	172
7.2 Digital defamation: publication and republication	180
7.2.1 <i>Dow Jones v Gutnick</i>	180
7.2.2 Multiple publication and jurisdiction	183
7.3 Intermediary liability	186
7.3.1 <i>Godfrey v Demon Internet</i>	186
7.3.2 Intermediary defences: the e-Commerce regulations	187
7.3.3 The operators of websites defence	193
7.3.4 Intermediary liability and Article 10 ECHR	194
7.4 Social media defamation	199
7.5 Conclusions	204
PART III DIGITAL CONTENT AND INTELLECTUAL PROPERTY RIGHTS	207
8. Intellectual property rights and the information society	209
8.1 An introduction to IPRs	210
8.1.1 Copyright	211
8.1.2 Patents	213
8.1.3 Trade marks	215

8.1.4 The database right	216
8.2 IPRs and digitization	218
9. Software	221
9.1 Protecting software: history	221
9.2 Copyright in computer software	224
9.2.1 Obtaining copyright protection	224
9.2.2 The scope of copyright protection	227
9.3 Copyright infringement and software: literal copying	229
9.3.1 Offline and online piracy	230
9.3.2 Employee piracy	231
9.4 Copyright infringement and software: non-literal copying	233
9.4.1 Look and feel infringement	234
9.4.2 Look and feel: <i>Navitaire v easyJet</i>	237
9.4.3 Look and feel: <i>Nova Productions v Mazooma Games</i>	239
9.4.4 Look and feel: <i>SAS Institute v World Programming Ltd</i>	241
9.5 Copyright infringement and software: permitted acts	243
9.6 Patent protection for computer software	246
9.6.1 VICOM/computer-related invention	248
9.6.2 The effect of <i>State Street Bank</i>	249
9.6.3 <i>De facto</i> software patents under the European Patent Convention	251
9.6.4 <i>Aerotel Ltd v Telco and Macrossan's Application</i>	252
9.7 Conclusions	256
10. Digital creativity and copyright law	259
10.1 Content, creativity, and creation	259
10.2 Copyright law, characters, and re-using content	260
10.2.1 Fair dealing	265
10.2.2 Remixing and sampling	268
10.2.3 <i>Paramount Pictures v Axanar Productions</i>	271
10.3 Computer-generated works	273
10.3.1 AI authors	273
10.3.2 AI-generated infringement	279
10.4 Conclusions	281

11. Copyright in the digital environment	283
11.1 Linking, caching, and the temporary reproduction right	284
11.1.1 Linking, framing, and caching	284
11.1.2 The temporary reproduction right	289
11.1.3 The temporary reproduction right after <i>PRCA</i>	296
11.2 The communication to the public right	297
11.2.1 A communication: <i>SGAE</i> and <i>TVCatchup</i>	298
11.2.2 A new public: <i>Svensson</i> , <i>GS Media</i> and <i>Stichting Brein</i>	300
11.2.3 A return to linking and framing: <i>VG Bild Kunst</i> and <i>Tuneln</i>	305
11.3 The copyright in the Digital Single Market Directive	310
11.4 Conclusions	313
12. Copyright infringement in the digital environment	316
12.1 Early cases: <i>Napster</i> and <i>Grokster</i>	316
12.2 <i>Sweden v Neij et al. (The Pirate Bay case)</i>	324
12.3 Site blocking (s.97A)	327
12.3.1 <i>Cartier International AG v British Telecommunications</i>	332
12.4 Speculative invoicing	336
12.5 Conclusions	341
13. Databases	343
13.1 Copyright and the database right	343
13.1.1 The listings cases	345
13.1.2 The Database Directive	346
13.2 The database right	350
13.2.1 The <i>Fixtures Marketing</i> cases	353
13.2.2 <i>British Horseracing Board Ltd v William Hill</i>	356
13.2.3 Post <i>BSB/Fixtures Marketing</i> decisions	360
13.3 Databases and the information society	365
13.4 Conclusions	370
14. Branding, trade marks, and domain names	372
14.1 Trade marks in the global business environment	373
14.1.1 Registered and unregistered trade marks	374
14.1.2 Trade mark characteristics	375

14.2 Domain names as badges of identity	376
14.3 Trade mark/domain name disputes	379
14.3.1 Early cases on cybersquatting before the UK courts	380
14.3.2 Cybersquatting, the CJEU, and later cases	383
14.4 The ICANN UDRP	386
14.5 The new gTLD process and dispute resolution	391
14.6 The Nominet DRS	394
14.6.1 Reviewing the Nominet DRS	398
14.7 Conclusions	399
15. Brand identities, search engines, and secondary markets	401
15.1 Jurisdiction and online trade mark disputes	401
15.2 Search engines	407
15.3 Secondary markets	416
15.4 Conclusions	420
PART IV E-COMMERCE	423
16. Electronic contracts	425
16.1 Contracting informally	425
16.1.1 Contract formation	426
16.2 Regulating offer and acceptance	428
16.2.1 Articles 9–11 of the Electronic Commerce Directive	428
16.2.2 Communicating acceptance	430
16.3 Contractual terms	432
16.3.1 Express terms	432
16.3.2 Terms incorporated by reference	432
16.3.3 Implied terms	433
16.4 Formal contracts	434
16.5 Electronic signatures	435
16.5.1 Identity and electronic signatures	437
16.5.2 Qualified electronic signatures	439
16.6 Smart contracts	442
16.6.1 Smart contracts and legal fallibility	447
16.7 Conclusions	451

17. Payments, cryptocurrency, and cryptoassets	453
17.1 Payments	453
17.1.1 Token payments	453
17.1.2 Alternative payment systems	454
17.2 Online payments, e-money, and e-payments	456
17.2.1 PSD II and EMD II	456
17.3 Cryptocurrency	459
17.3.1 Blockchain (distributed ledger) technology	461
17.3.2 Regulating cryptocurrency	463
17.4 Cryptoassets (or digital assets)	469
17.4.1 The UK jurisdiction task force	469
17.4.2 Cryptoassets and the courts	472
17.4.3 The Law Commission consultation on digital assets	474
17.5 Conclusions	477
18. Consumer protection	480
18.1 Distance and online selling	480
18.1.1 Jurisdiction, choice of law, and consumer disputes	481
18.1.2 Consumer rights in distance contracts	485
18.2 The Consumer Rights Act 2015	488
18.3 Regulation of spam	490
18.3.1 Regulating spam	491
18.3.2 <i>Microsoft v McDonald; Mansfield v John Lewis</i>	493
18.3.3 Regulating spam: GDPR and the ICO	494
18.4 Conclusions	496
PART V CRIMINAL ACTIVITY IN THE INFORMATION SOCIETY	499
19. Computer misuse	501
19.1 Hacking	503
19.1.1 Employee hackers	505
19.1.2 External hackers	511
19.1.3 Extradition cases	513
19.2 Viruses, criminal damage, and mail-bombing	518
19.3 Denial of service and supply of devices	522

19.3.1	Section 3ZA	526
19.3.2	Section 3A	528
19.4	CMA review and update	530
20.	Obscenity in the information society	533
20.1	Obscenity	534
20.1.1	The <i>Hicklin</i> principle	535
20.1.2	The Obscene Publications Acts	535
20.2	Pornography	537
20.2.1	The UK standard	537
20.2.2	A global standard?	540
20.2.3	US statutory interventions	542
20.2.4	The decision heard 'round the world'	545
20.2.5	Age verification	546
20.3	Child abuse images and pseudo-images	548
20.3.1	Policing images and pseudo-images in the UK	551
20.3.2	Non-photographic pornographic images of children	554
20.4	Extreme pornography	556
20.5	Non-consensual disclosure of private sexual images	560
20.6	Private regulation of pornographic imagery	562
20.7	Conclusions	564
21.	Crime and law enforcement in the information society	566
21.1	Fraud and identity theft	566
21.1.1	Fraud	566
21.1.2	Identity theft and identity fraud	571
21.2	Grooming, harassment, and cyberstalking	574
21.2.1	Grooming	574
21.2.2	Sexual communication with a child	576
21.2.3	Harassment and stalking	578
21.3	Cyberterrorism	579
21.4	The Convention on cybercrime	587
21.5	Conclusions	588

PART VI DATA PRIVACY	591
22. Data protection: the legal framework	593
22.1 Digitization, data, and the regulation of data industries	594
22.1.1 The changing face of data protection laws in Europe	595
22.1.2 GDPR and Brexit	596
22.1.3 The territorial scope of EU GDPR and UK GDPR	598
22.2 Data and data processing	607
22.2.1 Data subjects, data controllers, and processors	612
22.2.2 Data processing and the data protection principles	614
22.2.3 The domestic purposes exception	617
22.2.4 Fairness and lawfulness	620
22.3 Conditions for the processing of personal data	622
22.3.1 Consent	623
22.3.2 Other conditions for the processing of data	626
22.4 Conclusions	628
23. Data protection: rights and obligations	631
23.1 Data subject rights	631
23.1.1 Subject access: <i>Durant v The Financial Services Authority</i>	635
23.1.2 Revising subject access	639
23.1.3 Correcting and managing data	643
23.2 The right to be forgotten (right to erasure)	646
23.3 Supervising data controllers	652
23.4 Conclusions	654
24. The international trade in personal data	657
24.1 Transfers of personal data to third countries from the EU	658
24.1.1 The data exportation framework	660
24.2 Challenging the safe harbor: <i>Schrems I</i>	665
24.3 Challenging privacy shield: <i>Schrems II</i>	668
24.4 Challenging standard contractual clauses	672
24.5 Data transfers to and from the UK post Brexit	675
24.6 Conclusions	678

25. State surveillance and data retention	680
25.1 State surveillance	680
25.1.1 The UK legal framework for interception	681
25.1.2 Targeted interception warrants	684
25.1.3 Bulk interception warrants	689
25.1.4 State surveillance: Five Eyes, Upstream, and Tempora	691
25.1.5 <i>Liberty & Privacy International v GCHQ</i>	695
25.1.6 The European Court of Human Rights and bulk interception	698
25.2 Data retention	703
25.2.1 <i>Digital Rights Ireland</i> and <i>Seitlinger & Ors</i>	704
25.2.2 The Data Retention and Investigatory Powers Act 2014 (DRIPA) (now repealed)	706
25.2.3 Data retention under the Investigatory Powers Act 2016	711
25.3 Conclusions	718
INDEX	721