

CONTENTS

GUIDE TO THE BOOK	xviii
GUIDE TO THE ONLINE RESOURCE CENTRE	xix
TABLE OF CASES	xxi
TABLE OF STATUTES	xxix
<hr/>	
PART I INFORMATION AND SOCIETY	1
<hr/>	
1 The world of bits	2
1.1 An introduction to bits	4
1.1.1 The process of digitisation	5
1.2 Moving from atoms to bits	7
1.2.1 Music goes digital	9
1.2.2 Digital goods and society	10
1.3 Rivalrous and nonrivalrous goods	11
1.4 The legal challenge of the information society	12
<hr/>	
2 The network of networks	15
2.1 Introducing the internet (history)	16
2.1.1 Building the ARPANET	17
2.1.2 Building the internet	18
2.2 How the modern internet functions	21
2.2.1 Net neutrality	25
2.3 Higher-level protocols	32
<hr/>	
3 Digitisation and society	37
3.1 The digitisation of information	38
3.1.1 Information collection, aggregation and exploitation	39
3.1.2 Information disintermediation	41
3.1.3 Information management	44
3.2 Digital convergence	46
3.3 The cross-border challenge of information law	49
3.4 Digitisation and law	51
<hr/>	
PART II GOVERNANCE IN THE INFORMATION SOCIETY	53
<hr/>	
4 Regulating the digital environment	55
4.1 Can we regulate the digital environment?	56

4.1.1 Cyberlibertarianism	56
4.1.2 Cyberpaternalism	60
4.2 Lawrence Lessig's modalities of regulation	61
4.3 Network communitarianism	65
4.4 Regulators in cyberspace: private regulators	70
4.5 Regulators in cyberspace: states and supranational regulation	75
4.5.1 WSIS, the IGF and the ITU	76
4.6 Conclusions	82
<hr/>	
5 Digital ownership	84
5.1 Digital property	85
5.1.1 Information as property	86
5.1.2 Statutory intellectual property rights	87
5.1.3 Confidential information	89
5.2 Digital trespass	91
5.2.1 Trespass to servers	91
5.2.2 Copyright and trespass: indexing and scraping	93
5.2.3 <i>Intel v Hamidi</i>	94
5.2.4 Digital trespass at UK law	95
5.2.5 Adware and spyware	100
5.3 Virtual property	101
5.3.1 Virtual theft	101
5.3.2 Misappropriation of virtual goods	104
5.4 Conclusions	106
<hr/>	
6 Cyber-speech	108
6.1 Introduction	108
6.2 From web 1.0 to web 2.0	109
6.2.1 Web 1.0: internet fora	110
6.2.2 Web 1.0: personal websites	111
6.2.3 Web 1.0: law and society	111
6.2.4 Web 2.0: social media platforms	112
6.3 Freedom of expression and social responsibility	114
6.3.1 Freedom of expression: the 'First Amendment' approach	114
6.3.2 Freedom of expression: the European approach	115
6.3.3 Freedom of expression: the approaches compared	116
6.3.4 <i>Licra et UEJF v Yahoo! Inc. and Yahoo! France</i>	117
6.3.5 Cross-border speech	118
6.3.6 <i>Yahoo! Inc. v LICRA</i>	120
6.3.7 Free expression online	122

6.4 Political speech	123
6.4.1 Political speech: economics and media	124
6.4.2 Online political speech	125
6.5 Hate speech	128
6.5.1 Hate speech and society	128
6.5.2 Inter-state speech	129
6.6 Commercial speech	131
6.6.1 Commercial speech and the First Amendment	131
6.6.2 Commercial speech and the information society	132
6.6.3 Regulating spam in Europe	133
6.7 Conclusions: cyber-speech and free expression	135
<hr/>	
7 Social networking and antisocial conduct	137
7.1 Introduction	137
7.2 Social networking, gossip and privacy	139
7.2.1 The spring of 2011 and the Ryan Giggs affair	143
7.2.2 The Neuberger report and the joint committee on privacy and injunctions	147
7.3 Making criminal threats and organising criminal activity	149
7.3.1 The Paul Chambers case	149
7.3.2 The Facebook riot cases	153
7.4 Cyberbullying, trolling and harassment	157
7.5 YouTube and 'Innocence of Muslims'	160
7.6 Conclusions	162
<hr/>	
8 Defamation	165
8.1 The tort of defamation	166
8.1.1 Statements and publication	167
8.1.2 The Defamation Bill	169
8.1.3 Defences	171
8.2 Digital defamation: publication and republication	172
8.2.1 <i>Dow Jones v Gutnick</i>	173
8.2.2 <i>Loutchansky v Times Newspapers</i> : republication and limitation	176
8.2.3 <i>King v Lewis</i>	178
8.2.4 <i>Jameel v Dow Jones</i>	179
8.2.5 Online defamation post <i>Jameel</i>	181
8.3 Intermediary liability	183
8.3.1 <i>Godfrey v Demon Internet</i>	183
8.3.2 Intermediary defences: the Electronic Commerce Directive and Regulations	185
8.4 Digital defamation and UGC	192
8.4.1 Facebook and Twitter libel	193
8.5 Conclusions	196

PART III	DIGITAL CONTENT AND INTELLECTUAL PROPERTY RIGHTS	199
<hr/>		
9	Intellectual property rights and the information society	201
9.1	An introduction to IPRs	202
9.1.1	Copyright	203
9.1.2	Patents	205
9.1.3	Trade marks	207
9.1.4	The database right	209
9.2	IPRs and digitisation	210
<hr/>		
10	Software	213
10.1	Protecting software: history	213
10.2	Copyright in computer software	216
10.2.1	Obtaining copyright protection	216
10.2.2	The scope of copyright protection	219
10.3	Copyright infringement and software: literal copying	221
10.3.1	Offline piracy	221
10.3.2	Online piracy	223
10.3.3	Employee piracy	223
10.4	Copyright infringement and software: non-literal copying	225
10.4.1	Look and feel infringement	226
10.4.2	Look and feel: <i>Navitaire v easyJet</i>	229
10.4.3	Look and feel: <i>Nova Productions v Mazooma Games</i>	231
10.4.4	Look and feel: <i>SAS Institute v World Programming Ltd</i>	233
10.5	Copyright infringement and software: permitted acts	235
10.6	Software licences	238
10.6.1	End-user licence agreements (EULAs)	238
10.6.2	F(L)OSS	240
10.7	Patent protection for computer software	242
10.7.1	VICOM/computer-related invention	243
10.7.2	The effect of <i>State Street Bank</i>	244
10.7.3	De facto software patents under the European Patent Convention	246
10.7.4	<i>Aerotel Ltd v Telco and Macrossan's Application</i>	248
10.8	Conclusions	249
<hr/>		
11	Copyright in the digital environment	252
11.1	Linking, caching and aggregating	253
11.1.1	Web-linking	253
11.1.2	<i>Google Inc. v Copiepresse SCRL</i>	258
11.2	Peer-to-peer networks	263
11.2.1	Early cases	263

11.2.2	<i>A&M Records, Inc. v Napster, Inc.</i>	266
11.2.3	<i>Post Napster: MGM Studios, Inc. v Grokster, Ltd</i>	271
11.2.4	<i>Sweden v Neij et al. (the Pirate Bay case)</i>	276
11.2.5	Site blocking	279
11.2.6	Three strikes/Digital Economy Act	283
11.2.7	Speculative invoicing	287
11.3	Information and the public domain: the creative commons	291
11.4	Conclusions	293
<hr/>		
12	Databases	296
12.1	Copyright and the database right	296
12.1.1	The listings cases	298
12.1.2	The Database Directive	300
12.2	The database right	303
12.2.1	The <i>Fixtures Marketing</i> cases	306
12.2.2	<i>British Horseracing Board Ltd v William Hill</i>	309
12.2.3	After <i>BHB</i>	314
12.2.4	The <i>Football Dataco</i> decisions	316
12.3	Databases and the information society	318
12.4	Conclusions	320
<hr/>		
PART IV	CRIMINAL ACTIVITY IN THE INFORMATION SOCIETY	323
<hr/>		
13	Computer misuse	324
13.1	Hacking	327
13.1.1	Employee hackers	329
13.1.2	External hackers	334
13.1.3	The McKinnon case	337
13.2	Viruses, criminal damage and mail-bombing	339
13.2.1	Early cases: the Mad Hacker and the Black Baron	339
13.2.2	Later cases: web defacement and mail-bombing	342
13.3	Denial of service and supply of devices	344
13.3.1	Section 3A	348
<hr/>		
14	Pornography and obscenity in the information society	351
14.1	Obscenity	352
14.1.1	The Hicklin principle	353
14.1.2	The Obscene Publications Acts	354
14.2	Pornography	355
14.2.1	The UK standard	355
14.2.2	A global standard?	359
14.2.3	US statutory interventions	361
14.2.4	The decision heard 'round the world'	364

14.3	Child-abuse images and pseudo images	366
14.3.1	Policing pseudo-images in the UK	368
14.3.2	Non-photographic pornographic images of children	371
14.3.3	Policing pseudo-images internationally	373
14.4	Extreme pornography	375
14.5	Private regulation of pornographic imagery	380
14.6	Conclusions	383
<hr/>		
15	Crime and law enforcement in the information society	385
15.1	Fraud and identity theft	386
15.1.1	Fraud	386
15.1.2	Identity theft and identity fraud	390
15.2	Grooming, harassment and cyberstalking	393
15.2.1	Grooming	393
15.2.2	Harassment and stalking	396
15.3	Cyberterrorism	397
15.4	Bandwidth theft	403
15.5	The Convention on Cybercrime	404
15.6	Conclusions	406
<hr/>		
PART V	E-COMMERCE	409
<hr/>		
16	Branding and trade marks in the information society	410
16.1	Trade marks and branding	410
16.2	Trade marks in the global business environment	412
16.2.1	Registered and unregistered trade marks	412
16.2.2	Trade mark characteristics	414
16.3	Domain names as badges of identity	415
16.3.1	Sex.com	417
16.4	Early trade mark/domain name disputes	418
16.4.1	Cybersquatting before the UK courts	420
16.5	The ICANN UDRP	424
16.6	The Nominet DRS	428
16.6.1	Reviewing the Nominet DRS	432
16.7	Brand identities, search engines and secondary markets	433
16.7.1	Search engines	433
16.7.2	Secondary markets	439
16.8	Conclusions	442
<hr/>		
17	Electronic contracts	444
17.1	Contracting informally	444
17.1.1	Contract formation	445

17.2	Regulating offer and acceptance	447
17.2.1	Articles 9–11 of the Electronic Commerce Directive	447
17.2.2	Communicating acceptance	449
17.3	Contractual terms	451
17.3.1	Express terms	451
17.3.2	Terms incorporated by reference	452
17.3.3	Implied terms	453
17.3.4	Enforcing terms: consumer protection laws	453
17.4	Formal contracts	456
17.5	Electronic signatures	459
17.5.1	Formalising electronic signatures	461
17.5.2	Advanced electronic signatures	462
17.6	Conclusions	466
<hr/>		
18	Electronic payments	469
18.1	Electronic payments	469
18.1.1	Token payments	469
18.1.2	Alternative payment systems	470
18.1.3	Early e-money	472
18.2	The Electronic Money Directive 2000	474
18.3	Review of the Electronic Money Directive and the 2009 Electronic Money Directive	477
18.4	Conclusions	482
<hr/>		
PART VI	PRIVACY IN THE INFORMATION SOCIETY	485
<hr/>		
19	Data protection	486
19.1	Digitisation, personal data and the data industry	487
19.2	Data Protection Act 1998: background and structure	488
19.2.1	The Data Protection Act 1984	489
19.2.2	The Data Protection Directive	490
19.3	The Data Protection Act 1998	491
19.3.1	Forms of data	491
19.3.2	Processing and use of data	493
19.3.3	Personnel of the Data Protection Act	496
19.4	The data protection principles, processing and fairness	497
19.4.1	Processing data: <i>Bodil Lindqvist</i>	498
19.4.2	Processing data: <i>Johnson v Medical Defence Union</i>	500
19.5	Conditions for processing of personal data	502
19.5.1	Consent	504
19.5.2	Processing sensitive personal data	506
19.6	Supervision of data controllers: data subject rights	507
19.6.1	Subject access: <i>Durant v The Financial Services Authority</i>	508
19.6.2	Correcting and managing data	513

19.7	State supervision of data controllers	514
19.7.1	The Information Commissioner as regulator	515
19.8	Developments in data protection law	517
19.9	Conclusions	520
<hr/>		
20	Data and personal privacy	522
20.1	Enhanced CCTV	522
20.1.1	Pattern recognition: ANPR	524
20.1.2	Pattern recognition: biometrics	525
20.1.3	Regulating CCTV: the code of practice	526
20.2	RFID tracking	532
20.2.1	Regulating RFID	534
20.2.2	The EU action plan	537
20.3	Location and data retention	538
20.3.1	The Regulation of Investigatory Powers Act	539
20.3.2	Data retention	540
20.4	Conclusions	543
<hr/>		
PART VII	FUTURE CHALLENGES FOR INFORMATION LAW	547
<hr/>		
21	The digital public sphere	548
21.1	E-government	550
21.1.1	UK e-government	551
21.1.2	The ministerial declaration and transformational government	555
21.2	The digital divide	557
21.2.1	The global divide	557
21.2.2	The social divide	558
21.2.3	The social divide: opening competition in products and services	560
21.3	The democratic divide	563
21.3.1	The democratic divide and the blogosphere	563
21.3.2	Anonymity and free speech	567
21.4	Conclusions	570
<hr/>		
22	What way next?	572
22.1	Future developments	573
22.1.1	Greater connectivity, greater control	573
22.1.2	Greater connectivity, greater freedom	577
22.1.3	Developing technologies and legal responses	578
22.2	Web 3.0	579
22.3	Law 2.0	581
<hr/>		
INDEX		587