Contents

Foreword vii
Introduction xv
List of Contributors xvii
List of Abbreviations xix
Table of Cases xxiii
Table of Statutes xxxi
Table of Statutory Instruments xli
Table of Conventions, etc xlv
Table of Other Material xlvii

1 Offences Involving Misuse of Computers **1**
1.1 Background to the Computer Misuse Act 1990 1
1.2 Section 1 of the Computer Misuse Act 1990 – unauthorised access to computers 3
1.2.1 Procedure and sentencing 4
1.2.2 Elements of the offence 5
1.2.3 Meaning of 'unauthorised access' 7
1.2.4 Offending behaviour within the scope of section 1 of the Computer Misuse Act 1990 11
1.3 Section 2 of the Computer Misuse Act 1990 – unauthorised access with intent to commit or facilitate further offences 13
1.3.1 Procedure and sentencing 14
1.3.2 Elements of the offence 15
1.3.3 Comparison with the law of criminal attempts 16
1.3.4 Offending behaviour within the scope of section 2 of the Computer Misuse Act 1990 17
1.4 Section 3 of the Computer Misuse Act 1990 – unauthorised acts with intent to impair, or recklessness as to the impairment of, a computer 17
1.4.1 Procedure and sentencing 20
1.4.2 Elements of the offence 26

1.4.3 Offending behaviour within the scope of section 3 of the Computer Misuse Act 1990 or criminal damage 28
1.5 Types of computer misuse and charges under the Computer Misuse Act 1990 31
1.5.1 Alteration or deletion of data 31
1.5.2 Denial of Service attacks 31
1.5.3 Malware 33
1.5.3.1 Viruses 34
1.5.3.2 Trojan Horses 34
1.5.3.3 Worms 35
1.5.3.4 Spyware 35
1.5.4 Blended threats 36
1.5.5 Phishing 36
1.5.6 Pharming 37
1.5.7 Using phishing, pharming and Trojan Horses to harvest information for use in fraud 38
1.6 Section 3ZA of the Computer Misuse Act 1990 – unauthorised acts causing, or creating risk of, serious damage 39
1.6.1 Procedure and sentencing 41
1.6.2 Elements of the offences 41
1.7 Section 3A of the Computer Misuse Act 1990 – making, supplying or obtaining articles for use in offences under section 1 or section 3 42
1.7.1 Procedure and sentencing 43
1.7.2 Elements of the offences 44
1.7.3 Nature of the article 47
1.8 Meaning of 'computer' with regard to offences under the Computer Misuse Act 1990 47
1.9 Jurisdictional issues for offences under the Computer Misuse Act 1990 49

2 Offences Involving Data Protection 53
2.1 Overview 53
2.2 Section 170 of the Data Protection Act 2018 – unlawful obtaining or disclosure of personal data 54
2.2.1 Elements of the offence 55
2.2.2 Procedure and sentencing 57
2.2.3 Personal data 58
2.2.4 Personal data and computer misuse 60

2.2.5 Section 171: re-identification of de-identified personal data 60
2.2.6 Section 173: alteration, etc. of personal data to prevent disclosure to data subject 63
2.3 Access and disclosure of personal data 64
2.3.1 Section 184: prohibition of requirement to produce relevant records 64
2.3.2 Section 119: obstructing the Information Commissioner 66
2.4 Investigatory offences 66
2.4.1 Schedule 15, paragraph 15 to the DPA 2018: powers of entry and inspection 66
2.4.2 Section 144: false statement made in response to an information notice 67
2.4.3 Section 148 of the DPA 2018: destroying or falsifying information and documents 68
2.4.4 Section 132: prohibition placed upon the Information Commissioner and staff 68

3 Offences Relating to Property 71
3.1 Theft under the Theft Act 1968 71
3.1.1 Procedure and sentencing 71
3.1.2 Elements of the offence 72
3.1.3 Intangible property 72
3.1.4 Virtual property and digital currency 73
3.1.5 Confidential information and industrial espionage 74
3.2 Intellectual property theft – infringement of copyright under section 107 of the Copyright, Designs and Patents Act 1988 75
3.2.1 Criminal liability for infringement of copyright 77
3.2.2 Procedure and sentencing 79
3.2.3 Elements of the offence 79
3.2.4 File sharing over the internet 82
3.2.4.1 Data streaming 83
3.2.4.2 Downloading/uploading using a host website 84
3.2.4.3 Criminal liability for streaming and direct downloading 85
3.2.4.4 Peer-to-peer file sharing 85

4 Offences Involving Communications **93**
4.1 Introduction 93
4.2 Section 127 of the Communications Act 2003 – improper use of public electronic communications network 93
4.2.1 Procedure and sentencing 94
4.2.2 Elements of the offence 96
4.2.3 Grossly offensive, menacing, etc. character of the communication 97
4.2.4 Public electronic communications network 101
4.3 Section 1 of the Malicious Communications Act 1988 – sending letters, etc. with intent to cause distress or anxiety 103
4.3.1 Procedure and sentencing 105
4.3.2 Elements of the offence 105
4.4 Applicability of section 127 of the Communications Act 2003 and section 1 of the Malicious Communications Act 1988 to computer communications 107
4.4.1 Internet communications, social media and trolling 107
4.4.2 Director of Public Prosecutions' guidelines regarding internet communications 110
4.5 Unlawful interception of communications 115
4.5.1 Fundamentals of interception 116
4.5.2 Procedure and sentencing 121
4.5.3 Monetary penalties for unintentional interception 122
4.5.4 Elements of the offence 124
4.5.5 Period of transmission and 'hacking' of communications 130
4.5.6 Business practices and interception 133
4.5.7 Unlawful interception, equipment interference or computer misuse 136

5 Offences Relating to Internet or Computer Content **137**
5.1 Introduction 137
5.2 Section 1 of the Protection of Children Act 1978 and section 160 of the Criminal Justice Act 1988 – making, possession, publication and distribution of indecent images of children 138
5.2.1 Procedure and sentencing 140
5.2.2 Elements of the offences 144

5.2.3 Downloading indecent images of children/ child-abuse images 148
5.2.4 Possession of indecent images of children/ child-abuse images in electronic format 151
5.2.5 Sexual Harm Prevention Orders 155
5.3 Section 62 of the Coroners and Justice Act 2009 and section 63 of the Criminal Justice and Immigration Act 2008 – possession of prohibited images of children and possession of extreme pornographic images 158
5.4 Section 2 of the Obscene Publications Act 1959 – publishing an obscene article or having an obscene article for gain 159
5.4.1 Procedure and sentencing 161
5.4.2 Elements of the offence 164
5.4.3 Refinement of the test for obscenity 166
5.4.4 Obscenity and publications over the internet 167
5.4.5 Jurisdiction in which internet publications take place 171
5.4.6 Obscenity and communications via the internet 173
5.5 Section 53 of the Regulation of Investigatory Powers Act 2000 – ancillary offence of failing to disclose access to computers 174
5.5.1 Procedure and sentencing 177
5.5.2 Computers and disclosure notices 179

6 Cyber Harassment and Cyber Stalking 183
6.1 Offences Against the Person 183
6.2 Sections 2 and 2A of the Protection from Harassment Act 1997 – harassment and stalking 183
6.2.1 Procedure and sentencing 187
6.2.2 Elements of the offence 189
6.2.3 Harassment and stalking 192
6.2.4 'Cyber harassment' and 'cyber stalking' 193

7 Contempt of Court, the Internet and Court Reporting 201
7.1 Criminal contempt of court 201
7.1.1 Elements of the offence 202
7.1.2 Sentencing of contempts of court 203
7.1.3 Open justice and reporting of proceedings over the internet 204
7.1.4 Juries and internet misuse 208

8 Criminal Evidence and Computer Technology **215**
8.1 General background to the rules of criminal evidence 215
8.1.1 Default position on admissibility 215
8.1.2 Stay of proceedings 216
8.1.3 Exclusion of evidence in course of proceedings 220
8.1.4 Discretion to exclude evidence at common law 220
8.1.5 Statutory discretion to exclude evidence under section 78 of the Police and Criminal Evidence Act 1984 223
8.2 Hearsay and computer-derived evidence 227
8.2.1 Prohibition against hearsay and admissible hearsay 227
8.2.2 Hearsay and computer evidence 232
8.2.3 Section 117: business and other documents 241
8.3 Police powers of seizure of computer evidence 242

Appendices
A1 Criminal Procedure Rules 2015 247
A2 New Social Media Guidelines CPS 249

Index 267