

## INDEX

- absentia
  - trial in 414
- access control
  - access devices 130–2
  - counterfeit/unauthorised 132–3
  - unauthorised access to computers (hacking) and 95–7
- access to computers 5–6
  - unauthorised *see* unauthorised access to computers (hacking)
- accidental possession of child pornography 312
- addressing information 153
- adjudicative jurisdiction 410–13
- advance fee frauds 183, 187–8
- advertising
  - child pornography 291–2
- adware 32, 35, 36, 84
- anonymity 6–7
  - fraud and 185
- AOL 76, 243
- ATMs 86
  - consent by machine 205–6
  - deceiving a machine 204–5
  - skimming cards and 197
- attempt 70
- attributed identity 210
- auctions 82
- Australia
  - access to computers 6
  - child pornography 248
    - accessing 297
    - causing to transmit 298
    - criminalisation 253
    - defences 327
    - making available 288, 289
  - meaning of sexually explicit conduct 262, 263
  - medium of depiction 265
  - possession 301, 302, 315, 319
  - procuring 296
  - producing 282
  - publishing 287
  - receiving 300
  - transmission 294
  - virtual child pornography 273
- classification of cybercrime 10
- copyright infringement 224
  - mens rea* 230
  - penalties 231
- cyberstalking 369, 372
  - impact on victim 374
  - publishing information about victim 380, 381, 382
  - targeting victim's computer 384
- cyberterrorism 13
- extradition 415
- fraud
  - advance fee frauds 187
  - credit card skimming 210
  - electronic funds transfer crime 188
  - fraudulent online sales 185, 186
- grooming 343–5
  - inducing or procuring sexual activity 353–4
  - transmitting indecent or obscene material to minors 338–9
- identity crime (identity theft) 199, 208
  - defining identity information 212
  - manufacturing identity information 219

- possessing identity information 214
- trafficking identity information 216–17
- impairment (modification) of data 112–14
  - conduct causing modification or impairment 106
  - legislative provisions 102–3
- interception of data
  - content *versus* traffic data 154–5
  - legislative framework 138–9
  - live *versus* stored communications 166–9
  - meaning of telecommunication 143–5
- jurisdiction
  - adjudicative 411
  - prescriptive 407–8, 409–10
- legislative environment 43–5
- misuse of devices 123
  - possession or control of data 123–4
  - producing, supply or obtaining data 124
- online marketplace 184
- prevalence of cybercrime 40
- scale of cybercrime problem 14
- spam (unsolicited communications)
  - anti-spam legislation 238, 239, 241
- unauthorised access to computers (hacking) 48–9
  - definition of access 60–2
  - definition of computers 53
  - definition of data held in a computer 61–2
  - definition of unauthorised 71, 72
  - exceeding authorised access 86–8
  - fault element 93
- voyeurism 390, 394
  - legislative responses 395, 397, 401
- authorisation to access computers 78–9
  - exceeding authorised access 85–92
- Back Orifice 2000 (BO2K) 34
- banking 3, 207
  - electronic funds transfer crime 188
  - legal responses 202–4
- biographical identity 211
- biometric identity 210
- bots 35–6
  - spam (unsolicited communications) and 234
- British Telecom 39
- broadband 4
- browser hijackers 36
- bugs 28
- bullying 367
- burglary 85, 86
- calculators 55, 57
- call logging devices 157–9
- cameras 3
- Canada
  - access to computers 6
  - child pornography
    - accessing 297
    - causing to transmit 298
    - criminalisation 252, 253
    - defences 325, 326
    - making available 288
    - meaning of sexually explicit conduct 260
    - medium of depiction 266, 268, 271
    - possession 308, 319, 323
    - procuring 296
    - producing 282
    - publishing 287
    - virtual child pornography 273, 274
  - classification of cybercrime 10
  - Convention on Cybercrime and 22
  - copyright infringement 230
  - cyberstalking 369, 371, 373
    - communicating with the victim 377
    - impact on victim 374
    - surveillance 386
    - targeting victim's computer 384
  - fraud in
    - credit card skimming 210
    - fraudulent online sales 186
  - grooming 345–9
  - identity crime (identity theft) 200, 208
    - defining identity information 211

- Canada (*cont.*)
  - possessing identity information 214
  - trafficking identity information 217–18
- impairment (modification) of data 114
  - conduct causing modification or impairment 106–7
  - legislative provisions 104
- interception of data
  - content *versus* traffic data 155–7
  - legislative framework 139–40
  - live *versus* stored communications 169–70
  - meaning of telecommunication 145–7
- jurisdiction
  - adjudicative 410
- legislative environment 45
- misuse of devices 124–8
- online marketplace 184
- prevalence of cybercrime 40
- spam (unsolicited communications)
  - anti-spam legislation 238, 240, 241
- unauthorised access to computers (hacking) 49
  - definition of access 63–5
  - definition of computers 53, 54, 55, 56
  - definition of unauthorised 71, 72
  - fault element 94
- voyeurism
  - defences 402
  - legislative responses 395, 396, 399, 400, 401, 402
- causation 118
- cell phones 52, 156
- child grooming *see* grooming
- child pornography 3, 4, 178, 247–51
  - criminalisation 251–4
  - defences 324–8
  - definition 255–6
    - definition of minor 256–9
    - meaning of sexually explicit conduct 259–65
    - medium of depiction 265–71
  - distribution 292–3
    - import/export 295
    - transmission 294
    - transport 294–5
  - hacking and 31
  - malicious software and 34
  - offering or making available 286–7
    - advertising 291–2
    - making available 288–90
    - publishing 287–8
    - showing 290–1
  - possession 301–2
    - accidental 312
    - actual custody 302–9
    - de facto* custody 310–11
    - deletion 317–18
    - forgetfulness 315–17
    - ignorance 312–15
    - intention to possess 320–4
    - knowledge of possession 311–20
    - physical possession 302–11
  - procuring 295–7
    - accessing 297–8
    - causing to transmit 298
    - receiving 298–300
    - requesting 300–1
  - producing 282–6
  - virtual 271–81
- China, copyright infringement in 222
- ChoicePoint 195
- commercial information
  - unauthorised access to computers (hacking) 29, 30, 82
- communication
  - changing nature of telecommunications 135–6
  - impairment of 103
- Computer Crime and Security Survey* 39
- computers 3
  - as target of cybercrime 27–8
  - definition 52–3
    - Australia 53
    - Canada 53, 54, 55, 56
    - United Kingdom 53, 56
    - United States of America 56–8
  - Denial of Service (DoS) attacks 4, 12, 37–9
  - misuse *see* misuse of devices

- legislative environment 40–3
  - prevalence 39–40
  - see also* malicious software; unauthorised access to computers (hacking)
  - confidentiality
    - unauthorised access to computers (hacking) and 89, 95
  - consent
    - by machine 205–6
    - implied 79–80
    - spam (unsolicited communications) 241–2
  - conspiracy to defraud 120
  - contracts
    - access to computer regulated by 74–7
  - Convention on Cybercrime *see* Cybercrime Convention
  - cookies 36, 84, 98, 179
  - copyright infringement 3, 4, 221–5
    - legislative provisions 225–7
      - commercial infringement 227–8
      - distribution of files 228–30
      - mens rea* 230–1
      - penalties 231
  - credit cards
    - carding 198–9
    - online fraud 186
    - skimming 196–8, 210
    - verification systems 186
  - criminal damage 101, 102
  - criminal offences
    - child pornography *see* child pornography
    - jurisdiction *see* jurisdiction
    - online communities 18, 20
    - spam (unsolicited communications) 242–4
    - supplying articles to commit offences 129
    - voyeurism 389–93
  - Cummings, Philip 195
  - cyberbullying 367
  - cybercrime
    - challenges of 5
      - absence of capable guardians 7–8
    - accessibility 5–6
    - anonymity 6–7
    - global reach 7
    - portability and transferability 7
    - scale 5
    - cyberterrorism 11–13
    - definition 8–11
    - evolution of 3–4
    - online/offline consistency 15–16
    - scale of problem 13–15
    - virtual crime 16–21
    - see also* individual topics
  - Cybercrime Convention 9, 21–4, 44, 96
    - adjudicative jurisdiction 413
    - on child pornography 255
      - definition of minor 256
    - distribution 292
    - meaning of sexually explicit conduct 259
    - offering or making available 286
    - procuring 296
    - virtual child pornography 281
  - on cookies 84
  - on copyright infringement 225–6
    - definition of access 58
    - definition of computer 52
    - definition of unauthorised 70
  - on fraud 201, 206, 207–10
  - on impairment (modification) of data 101
  - on interception of data 136–8
  - on misuse of devices 120–1
  - prescriptive jurisdiction 406–7
- cyberstalking 365–8
  - forms of 375
    - communicating with the victim 376–9
    - publishing information about victim 379–84
    - surveillance 384–7
    - targeting victim's computer 384
  - legislative responses 368–71
    - conduct element 371–2
    - fault element 373
    - impact on victim 374
- cyberterrorism 11–13

- data
  - definition of data held in a computer
    - Australia 61–2
  - impairment of *see* impairment (modification) of data
  - interception *see* interception of data
  - possession or control of data 123–4
  - trafficking in 124, 133
- deception
  - deceiving a machine 204–5
  - obtaining property by 203, 204
- defences 127
  - child pornography 324–8
  - grooming offences 337
  - voyeurism 402
- deletion of child pornography 317–18
- Denial of Service (DoS) attacks 4, 12, 37–9
- digital number recorders (DNRs) 156
- Digital Rights Management (DRM)
  - protection 226
- digital technology 3
- disabling codes 75
- Distributed Denial of Service (DDoS)
  - attacks 38
- distribution
  - child pornography 292–3
    - import/export 295
    - transmission 294
    - transport 294–5
  - files 228–30
  - voyeuristic images 401–2
- domain names 77
  - pharming 194
- Drew, Lori 75
- dual use systems 122, 129
- dumpster diving 191
- eBay 35, 82
- electromagnetic emissions 137
- electronic funds transfer crime 188
  - legal responses 202–4
- email 3
  - address harvesting 235
  - interception 135, 136, 152, 163, 169, 172, 175
  - Nigerian email frauds 183, 184, 185, 187
  - phishing 192–4
  - ‘store and forward’ delivery 165–6
  - unsolicited communications *see* spam
- encryption technology 6
  - cracking WEP encryption keys 32
- enforcement jurisdiction 413–16
- exceeding authorised access 85–92
- exploits 121
- external storage devices 62, 304–5
- extradition 414–16
- extraterritorial jurisdiction 406, 409–10, 411
- file sharing 3
- forgery 191, 206–7
- fraud 3, 4, 183–5
  - advance fee frauds 183, 187–8
  - conspiracy to defraud 120
  - electronic funds transfer crime 188
    - legal responses 202–4
  - fraudulent investments 188
  - identity crime *see* identity crime
  - legal responses 201–2
    - computer-related forgery 206–7
    - consent by machine 205–6
    - deceiving a machine 204–5
    - electronic funds transfer crime 202–4
  - Nigerian email frauds 183, 184, 185, 187
  - online sales 185–7
  - scale of problem 199–201
  - unauthorised access to computers (hacking) 94, 95, 99
- government information
  - unauthorised access to computers (hacking) 29, 52, 70, 87
- grooming 331–7, 343
  - Australia 343–5
    - inducing or procuring sexual activity 353–4
    - transmitting indecent or obscene material to minors 338–9
  - Canada 345–9
    - inducing or procuring sexual activity 351–2

- stages 333–5
- transmitting indecent or obscene material to minors 337–8
- travelling with intent 361
- United Kingdom 335, 349–51
  - inducing or procuring sexual activity 354
  - transmitting indecent or obscene material to minors 339–41
  - travelling with intent 361–4
- United States of America 331, 333, 334, 335, 336
  - inducing or procuring sexual activity 352, 355–61
  - transmitting indecent or obscene material to minors 341–3
  - travelling with intent 364
- Habbo Hotel 19
- hacking *see* unauthorised access to computers (hacking)
- harassment *see* cyberstalking
- harmonisation between countries 21
- hyperlinks 288
- ICMP floods 38
- identity crime (identity theft) 189–92, 199–201, 206, 207–10
  - carding 198–9
  - credit card skimming 196–8, 210
  - defining identity information 210–13
  - hacking and use of malware 195–6
  - manufacturing identity information 219–20
  - pharming 194
  - phishing 192–4
  - possessing identity information 212, 213–15
  - trafficking identity information 215–19
- impairment (modification) of data 29, 79, 101–2, 111–12
  - Australia 112–14
    - conduct causing modification or impairment 106
    - legislative provisions 102–3
  - Canada 114
    - conduct causing modification or impairment 106–7
    - legislative provisions 104
  - United Kingdom 114–16
    - conduct causing modification or impairment 107–8
    - legislative provisions 104
  - United States of America 117–19
    - conduct causing modification or impairment 108–11
    - damage 117–19
    - harm
    - intentionally accessing protected computer 111
    - legislative provisions 104–6
    - transmission of program/command 108–11
- implied consent 79–80
- implied licences 82
- incitement 120
- indecent material
  - transmitting indecent or obscene material to minors 337–8
    - Australia 338–9
    - United Kingdom 339–41
- injunctions 82
- instant messaging 135
- intellectual property rights *see* copyright infringement
- intended function test 83
- intention
  - copyright infringement 230–1
  - possession of child pornography 320–4
  - unauthorised access to computers (hacking) 50, 64, 84, 92–5, 97–100, 111
- interception of data
  - Australia
    - content *versus* traffic data 154–5
    - legislative framework 138–9
    - live *versus* stored communications 166–9
    - meaning of telecommunication 143–5
  - Canada
    - content *versus* traffic data 155–7
    - legislative framework 139–40

- interception of data (*cont.*)
  - live *versus* stored communications 169–70
  - meaning of telecommunication 145–7
- changing nature of
  - telecommunications 135–6
- content *versus* traffic data 152–4
- Convention on Cybercrime and 136–8
- live *versus* stored communications 164–6
- meaning of telecommunication 143
- United Kingdom
  - content *versus* traffic data 157–61
  - legislative framework 140
  - live *versus* stored communications 170–3
  - meaning of telecommunication 148–9
- United States of America
  - backup storage 177–9
  - content *versus* traffic data 161–4
  - legislative framework 141–3
  - live *versus* stored communications 173–9
  - meaning of telecommunication 149–52
  - under SCA 174
  - temporary storage 174–6
  - under Wiretap Act 173–4
- Internet 135, 138
  - access to 5–6
  - broadband 4
  - child pornography and *see* child pornography
  - cyberterrorism and 12
  - domain names 77
    - pharming 194
  - fraudulent online sales 185–7
  - numbers of people connected to 5
  - online marketplace 184
  - sexual predators *see* grooming
- Internet Corporation for Assigned Names and Numbers (ICANN) 77
- Internet Crime Complaint Centre 185
- investments, fraudulent 188
- Jaynes, Jeremy 244
- junk email *see* spam (unsolicited communications)
- jurisdiction 405–6
  - adjudicative 410–13
  - enforcement 413–16
  - prescriptive 406–10
- Kazaa 223
- Kerr, O. S. 68, 69
- keyloggers 147, 150
- LambdaMOO 16, 18
- legislative environment 40–3
  - Australia 43–5
  - Canada 45
  - United Kingdom 46
  - United States of America 46–7
- legislative (prescriptive) jurisdiction 406–10
- Lessig, L. 8
- licence agreements
  - implied licences 82
  - software 75
- logic bombs 33
- loss of computers and data 191
- Love Bug 414
- McKinnon, Gary 415
- mail bombing 37
- malicious code 125
- malicious software 32–3
  - bots 35–6
  - identity crime and 195–6
  - spam (unsolicited communications) and 234
  - spyware 36–7
  - Trojans 34, 40, 196
  - viruses and worms 33–4, 40
- Maple Story game 18
- media
  - scale of cybercrime problem and 15
- Melissa virus 33
- misuse of devices 120–3
  - Australia 123
  - possession or control of data 123–4

- producing, supply or obtaining
  - data 124
  - Canada 124–8
  - United Kingdom 128–30
  - United States of America 130, 133–4
    - access devices 130–2
    - counterfeit/unauthorised access devices 132–3
  - mobile phones 52, 156
  - modification of data *see* impairment (modification) of data
  - money laundering 187
  - Morpheus 223
  - murder
    - online communities 18
- Napster 223, 229
- Nigerian email frauds 183, 184, 185, 187
- obscene material *see* indecent material
- O’Connell, R. 333
- offences *see* criminal offences
- online communities 16–21
- open access 31
- overcriminalisation 53, 54, 69, 137
- paedophilia *see* child pornography; grooming
- participant monitoring 171
- passwords 31, 59, 72, 74, 96, 121, 125, 133
- peeping *see* voyeurism
- peer-to-peer networks 4, 169, 222–3, 227, 228
  - bots and 35
- pen registers 142, 161, 164
- penalties
  - copyright infringement 231
- penetration testing devices 122
- pharming 194
- phishing 192–4
- pings 38
- police
  - scale of cybercrime problem and 14
  - telephone monitoring 171
  - unauthorised access to police records 63, 64, 90
- pop-ups 36
- port scanning 29, 67
- possession of child pornography 301–2
  - intention to possess 320–4
  - knowledge 311–20
    - accidental possession 312
    - deletion 317–18
    - forgetfulness 315–17
    - ignorance 312–15
    - knowledge of nature of thing possessed 318–20
  - physical possession 302–11
    - actual custody 302–9
    - de facto* custody 310–11
- predators *see* grooming
- prescriptive jurisdiction 406–10
- privacy 163, 164, 391–2
  - unauthorised access to private information 4
- procuring
  - child pornography 295–7
    - accessing 297–8
    - causing to transmit 298
    - receiving 298–300
    - requesting 300–1
  - sexual activity with a minor 351–2
- producing child pornography 282–6
- property 41–3
  - intellectual property *see* copyright infringement
  - online communities 19–20
- publishing
  - child pornography 287–8
  - information about victim of cyberstalking 379–84
- pump and dump schemes 189
- radio systems 57, 138
- regulation
  - by contracts 74–7
  - lack of 7–8
  - spam (unsolicited communications) 235–8
- remote attacks 4
- rootkits 120
- Salcedo, Brian 196
- Sankus, John 224



- scareware 187
- Second Life 19, 20
- sexual offences
  - online communities 18, 20
  - sexual predators *see* grooming
  - voyeurism as 392–3
- Shadowcrew 198
- shares
  - pump and dump schemes 189
- skimming credit cards 196–8, 210
- SMS messaging 3, 135, 159
  - SMiShing 192
- sniffer programs 36
- social network sites 385
- software
  - adware 32, 35, 36, 84
  - bugs 28
  - fraud and 187
  - licence agreements 75
  - malicious *see* malicious software
  - scareware 187
  - spyware 32, 36–7, 83
- spam (unsolicited communications)
  - 67, 77, 79–80, 81, 232–5
  - anti-spam legislation 237, 238–9
  - civil or criminal enforcement 239–40
  - commercial and/or bulk email 240–1
  - consent 241–2
  - criminal offences 242–4
  - spam-related conduct 242
  - regulation 235–8
- spear phishing 192
- spyware 32, 36–7, 83
- stalking *see* cyberstalking
- storage devices 62, 304–5
- ‘store and forward’ delivery 165–6
- subject matter (prescriptive)
  - jurisdiction 406–10
- supplying articles to commit offences 129
- surveillance *see* cyberstalking; interception of data; voyeurism
- tapping *see* interception of data
- telecommunications
  - interception *see* interception of data
- telephones 152
  - call logging devices 157–9
  - digital number recorders (DNRs) 156
  - malicious 156
  - mobile phones 52, 156
  - monitoring *see* interception of data
  - VoIP systems 135, 152, 154
- territorial jurisdiction 406–7, 408, 409–10, 411
- terrorism 11–13
- theft 27, 41, 203
  - identity *see* identity crime
- Townshend, Pete 325
- trade secrets 118
- trafficking 122, 125
  - in data 124, 133
  - identity information 215–19
- trap and trace devices 142, 161
- trash and cash schemes 189
- trespass 85–6
  - computer trespass 59, 66, 73, 81, 87
- Trojans 34, 40, 196
- unauthorised access to computers
  - (hacking) 27–8, 48
  - access to information 29, 31
  - additional elements 95–100
  - Australia 48–9
    - definition of access 60–2
    - definition of computers 53
    - definition of data held in a computer 61–2
    - definition of unauthorised 71, 72
    - exceeding authorised access 86–8
    - fault element 93
  - Canada 49
    - definition of access 63–5
    - definition of computers 53, 54, 55, 56
    - definition of unauthorised 71, 72
    - fault element 94
  - definition of access 58–60
  - definition of computers 52–3
  - definition of unauthorised 70–92
  - exceeding authorised access 85–92
  - fault element 92–5
  - identity crime and 195–6

- impairment (modification) of data
  - 29, 79, 101–2
- United Kingdom 49–51
  - definition of access 62–3
  - definition of computers 53, 56
  - definition of unauthorised 71, 72
  - exceeding authorised access 89–91
  - fault element 93, 95
- United States of America 51, 151
  - definition of access 65–70
  - definition of computers 56–8
  - definition of unauthorised 72, 76
  - exceeding authorised access 88–9, 91
  - fault element 94
  - intention and 97–100
  - spam (unsolicited communications) 67, 81
  - use of computer 30–2
- United Kingdom
  - access to computers 6
  - child pornography 248, 249
    - advertising 291
    - criminalisation 251, 253, 254
    - defences 325, 327
    - definition of minor 258
    - distribution 293
    - ignorance of possession 313
    - meaning of sexually explicit conduct 263
    - medium of depiction 268, 269
    - possession 301, 315, 318
    - procuring 296
    - producing 282–3, 285–6
    - publishing 288
    - showing 290–1
    - virtual child pornography 271, 273
  - classification of cybercrime 10
  - Convention on Cybercrime and 22
  - copyright infringement 222, 224
    - mens rea* 230
  - cyberstalking 369, 371, 373
    - impact on victim 374
    - publishing information about victim 380
  - cyberterrorism 13
  - Denial of Service (DoS) attacks 37
  - grooming 335, 349–51
    - inducing or procuring sexual activity 354
    - transmitting indecent or obscene material to minors 339–41
    - travelling with intent 361–4
  - identity crime (identity theft) 200, 209
    - defining identity information 211
    - manufacturing identity information 219
    - possessing identity information 214
  - impairment (modification) of data 114–16
    - conduct causing modification or impairment 107–8
    - legislative provisions 104
  - interception of data
    - content *versus* traffic data 157–61
    - legislative framework 140
    - live *versus* stored communications 170–3
    - meaning of telecommunication 148–9
  - jurisdiction 408
  - legislative environment 46
  - misuse of devices 128–30
  - online marketplace 184
  - scale of cybercrime problem 13
  - spam (unsolicited communications) 233
    - anti-spam legislation 239, 240, 241, 242
  - unauthorised access to computers (hacking) 49–51
    - definition of access 62–3
    - definition of computers 53, 56
    - definition of unauthorised 71, 72
    - exceeding authorised access 89–91
    - fault element 93, 95
  - voyeurism
    - legislative responses 394, 397, 399, 400, 401

- United States of America
  - access to computers 6
  - child pornography 247, 248
    - advertising 291–2
    - criminalisation 253
    - defences 326, 328
    - ignorance of possession 313–15
    - making available 288
    - meaning of sexually explicit
      - conduct 259, 261, 264
    - medium of depiction 266, 267, 268, 269, 270
    - offering or making available 287
    - possession 301, 303–4, 306, 318, 319, 324
    - procuring 296, 297
    - producing 283
    - receiving 298, 300
    - transport 294–5
    - virtual child pornography 271, 273, 274–81
  - Convention on Cybercrime and 22
  - copyright infringement 224
    - commercial infringement 227
    - distribution of files 229
    - legislative provisions 226
    - mens rea* 230
  - cyberstalking 370, 371, 372, 373
    - communicating with the victim 377–9
    - impact on victim 374
    - publishing information about victim 380, 381, 382
    - surveillance 386, 387
  - extradition 415
  - fraud in 202
    - credit card skimming 210
    - electronic funds transfer crime 188, 203
    - fraudulent online sales 186
    - legal responses 203
  - grooming 331, 333, 334, 335, 336
    - inducing or procuring sexual activity 352, 355–61
  - transmitting indecent or obscene material to minors 341–3
  - travelling with intent 364
  - identity crime (identity theft) 199, 208
    - defining identity information 212
    - manufacturing identity information 220
    - possessing identity information 215
    - trafficking identity information 218–19
  - impairment (modification) of data 117–19
    - conduct causing modification or impairment 108–11
    - damage 117–19
    - harm
    - intentionally accessing protected computer 111
    - legislative provisions 104–6
    - transmission of
      - program/command 108–11
  - interception of data
    - backup storage 177–9
    - content *versus* traffic data 161–4
    - legislative framework 141–3
    - live *versus* stored communications 173–9
    - meaning of telecommunication 149–52
    - under SCA 174
    - temporary storage 174–6
    - under Wiretap Act 173–4
  - jurisdiction 405
    - adjudicative 410, 412
    - prescriptive 409
  - legislative environment 46–7
  - misuse of devices 130, 133–4
    - access devices 130–2
    - counterfeit/unauthorised access devices 132–3
  - online marketplace 184
  - prevalence of cybercrime 39
  - scale of cybercrime problem 14
  - spam (unsolicited communications) 67, 81, 233
    - anti-spam legislation 239, 240, 241, 242, 243–4
    - regulation 235, 238

- unauthorised access to computers
  - (hacking) 51, 151
  - definition of access 65–70
  - definition of computers 56–8
  - definition of unauthorised 72, 76
  - exceeding authorised access 88–9, 91
  - fault element 94
  - intention and 97–100
- voyeurism
  - legislative responses 394, 397–9, 400, 401
- unsolicited communications *see* spam
- use of computer
  - unauthorised 30–2
- VDUs 137
- verification systems for credit cards 186
- virtual child pornography 271–81
- virtual crime 16–21
- viruses 33, 40
- voice phishing 193
- VoIP systems 135, 152, 154
- voyeurism 388–9
  - criminalisation 389–93
  - legislative responses 393–4
    - application 394–5
    - conduct it applies to 399–400
  - defences 402
  - distribution of images 401–2
  - fault element 400–1
  - where it applies 395–9
- Wales, Timothy 331
- wardriving 30–2
- warez groups 224
- weaving 30
- web bugs 36
- web crawlers 36
- wireless hacking 30–2
- wireless networks 144, 148, 149
- wiretapping *see* interception of data
- worms 33, 40
- zombies *see* bots