

INDEX

- access devices, 145–7
- access offences; *see also* malware
 - overview, 32–3, 56
 - access, meaning of, 68–80
 - Australia, 56–7, 69–71
 - Canada, 57, 73–5
 - computer, meaning of, 59–67
 - denial of service attacks, 43–4, 130
 - motivations for, 33–4
 - unauthorised access requirement
 - overview, 80–3
 - additional elements, 107–11
 - Australia, 80, 82, 94–5, 105
 - burglary analogy for, 91–3
 - Canada, 80, 82, 93–4, 106
 - contractual limitations, 84–7
 - cookies, 90
 - exceeding of authorised access, 91–104
 - fault requirement, 104–7
 - generally, 83
 - intended function test, 89
 - limitations, importance of, 95–8
 - motives versus authorisation, 91
 - regulation by code, 83–4
 - restricted data, 108–9
 - restricted or denied authorisation, 83
 - spyware, 90
 - ulterior purposes, 95
 - United Kingdom, 81–2, 96–8, 105–6
 - United States, 81–3, 98–104, 106–7, 109–11, 164–7
 - unsolicited communications, 87–9
 - United Kingdom, 57–8, 71–3
 - United States, 59
- accessory liability for copyright infringement, 269
- adjudicative jurisdiction, 481–6
- administrator level hacking, 32
- advance-fee fraud, 209, 214–16
- advertisement of child pornography, 333–5
- aircraft, jurisdiction and, 476
- anonymity
 - overview, 7–8
 - grooming, 379, 388
 - harassment, 418, 434
 - internet, 211
 - spoofing for, 123, 275, 434
- Anonymous (group), 13, 32
- antivirus scams, 213
- apps, number of, 7
- attributed identity, 242
- auction site fraud, 212
- Australia
 - access offences, 56–7, 69–71
 - child pornography
 - accessing, 339
 - causing to transmit, 340
 - defences, 368
 - definition, 302–3, 308, 315
 - making available, 331
 - offences, where found, 296
 - possession, 344, 363
 - procurement, 339
 - production, 325
 - publication, 330
 - solicitation, 344
 - transmission element, 337
 - communication, content versus metadata, 170–1
 - computer, meaning of, 60–4

- Australia (cont.)
 copyright infringement, 260, 266, 270–1
 credit card losses, 231
 credit card skimming, 241
 data interception, 152–3, 158–60, 184–7
 data modification/impairment, 113–14, 117, 124–6
 deceiving machines, 235
 device misuse, 136–8
 fraud in, 229
 grooming, 389–90, 394–6, 403–4
 harassment
 fault requirement, 431
 impact on victim, 433
 offences, 425, 430
 publication, 442
 identity information/theft, 239, 243, 246, 248–50, 252
 jurisdiction, 480
 legislative environment, 50–2
 revenge porn, 446
 sexting, 302
 spam, 279–81, 283
 unauthorised access requirement, 80, 82, 94–5, 105
 US–Australia extradition treaty, 488
 voyeurism, 461, 463, 470
 Australia–US extradition treaty, 488
 authentication features, 244
- backup storage, 202–5
 biographical identity, 242
 biometric identity, 242
 Bitcoin, 211
 BitTorrent client, 258
 BitTorrent protocol, 258
 blended threats, 38
 Bluetooth, 152, 159
 botnets, 41, 274
 bots, 41–2
 broadband, risks of, 5
 browser hijackers, 42
 browswrap agreements, 86
 bullying, 420, 422, 427; *see also*
 harassment
- Canada
 access offences, 57, 73–5
 child pornography
 accessing, 340
 causing to transmit, 340
 defences, 369
 definition, 304, 308, 310, 315
 import/export, 338
 making available, 331
 offences, where found, 296
 possession, 344, 363
 procurement, 339
 production, 325
 publication, 331
 communication, content versus
 metadata, 172–5
 computer, meaning of, 60–4
 copyright infringement, 270
 credit card losses, 231
 credit card skimming, 241
 data interception, 154, 160–2, 187–92
 data modification/impairment, 115, 118–19, 126
 device misuse, 138–41
 electronic commerce, 210
 grooming, 396–9
 harassment
 fault requirement, 431
 impact on victim, 432
 offences, 426, 429
 surveillance, 450
 identity information/theft, 230, 239, 243, 246, 250
 internet use rate, 210
 jurisdiction, 477, 481
 legislative environment, 52–3
 online banking, 210
 spam, 279–81, 283
 unauthorised access requirement, 80, 82, 93–4, 106
 voyeurism
 conduct applied to, 467
 defences, 471
 depictions applied to, 461
 distribution of images, 470
 expectation of privacy, 461
 fault requirement, 468
 up-skirt images, 463

- carding, 145, 227–8
- card-not-present transactions, 213, 231
- CERT Australia survey, 46
- CFAA: *see* Computer Fraud and Abuse Act of 1986 (CFAA, US)
- child modelling sites, 306
- child pornography
 - overview, 289–94
 - advertisement of, 333–5
 - Australia
 - accessing, 339
 - causing to transmit, 340
 - defences, 368
 - making available, 331
 - offences, where found, 296
 - procurement, 339
 - publication, 330
 - solicitation, 344
 - transmission element, 337
 - Canada
 - accessing, 340
 - causing to transmit, 340
 - defences, 369
 - definition, 304, 308, 310, 315
 - import/export, 338
 - making available, 331
 - offences, where found, 296
 - possession, 344, 363
 - procurement, 339
 - publication, 331
 - criminalisation of, 294–7
 - defences, 368–74
 - definition
 - overview, 297–9
 - age of consent, 299
 - Australia, 302–3, 308, 315
 - Canada, 304, 308, 310, 315
 - medium of depiction, 308–13
 - minor, what constitutes, 299–302
 - morphed images, 314, 320–2
 - sexting, 301–2
 - sexually explicit conduct, 302–8
 - United Kingdom, 303, 311, 315
 - United States, 305, 311–12, 316
 - virtual child pornography, 313–25
 - distribution or transmission, 335–8
 - honey pot websites, 343
 - offering or making available, 330–5
 - possession
 - overview, 344–5
 - access compared, 338
 - actual custody, 345–54
 - Australia, 344, 363
 - Canada, 344, 363
 - de facto custody, 354–5
 - defences, 368–74
 - deleted files, 348, 361–2
 - forgetting of possession, 359–61
 - historically, 294–6
 - ignorance of possession, 357–9
 - inadvertent possession, 356–7, 372
 - intention to possess, 365–8
 - knowledge, 355–65
 - making compared, 329
 - physical possession, 345–55
 - storage devices versus images, 347
 - United Kingdom, 330, 344, 362
 - United States, 344, 364
 - viewing compared, 353
 - virtual images, 309
 - procurement, 338–44
 - production, 325–30
 - United Kingdom
 - advertisement, 333
 - defences, 370, 372
 - definition, 303, 311, 315
 - distribution of images, 336
 - offences, where found, 297
 - possession, 330, 344, 362
 - production, 325
 - United States
 - accessing, 340
 - defences, 371–2
 - definition, 305, 311–12, 316
 - import/export, 338
 - offences, where found, 297
 - possession, 344, 364
 - procurement, 339
 - production, 325
 - receiving, 341
 - transport, 337
- chosen identities, 242
- click-frauds, 216
- clickjacking, 38

- clickwrap agreements, 86
- cloud computing, copyright infringement and, 259
- commercial copyright infringement, 263–4
- Commission on Crime Prevention and Criminal Justice, 25
- communications: *see* data interception
- composite images, 314
- computer crime, 4
- Computer Crime and Security Survey, 45
- computer support scams, 215
- computer targets; *see also* access offences; data interception; data modification/impairment; device misuse
 - overview, 31–2
 - harassment, 447
 - legislative environment, 47–55
 - malware, 38–43
 - prevalence of, 45–7
- computer-related forgery, 237–8
- computer-supported crimes, 11
- conclusion stage of grooming, 385
- connectivity, 417; *see also* internet; social networking sites
- conspiracy for copyright infringement, 269
- content data, traffic data compared, 169
- contributory infringement, 268
- Convention on Cybercrime: *see* Cybercrime Convention
- cookies, 42, 90, 129, 204
- COPINE Project (Combating Paedophile Information Networks in Europe), 303
- copyright infringement
 - Australia, 260, 266, 270–1
 - Canada, 270
 - commercial infringement, 263–4
 - distribution, 265–9
 - extent and impact of, 256
 - legislative environment, 261–71
 - mens rea*, 269–70
 - penalties, 271
 - prosecutions for, 259
 - theft distinguished, 255–61
 - United Kingdom, 256, 262, 270
 - United States
 - commercial infringement, 263
 - distribution, 265
 - mens rea*, 270
 - numbers of cases, 259
 - value added by copyright industries, 256
- counterfeit devices, 147
- covert surveillance: *see* surveillance; voyeurism
- credit card fraud, 213
- credit card skimmers, 226
- credit card skimming, 225–7, 241
- criminal copyright infringement: *see* copyright infringement
- criminalisation decisions, 18
- Cryptolocker, 225
- cyberbullying, 420, 422, 427; *see also* harassment
- cybercrime
 - challenges of, 5–9
 - cyberterrorism compared, 14
 - defined, 10–11
 - evolution of, 3
 - generations of, 4
 - online/offline consistency, 17–18
 - under-reporting of, 16–17
 - scale of, 15–17, 45–7
 - terminology limitations, 9–10
 - virtual crimes as, 18–23
- Cybercrime Convention
 - overview, 23–7
 - access, meaning of, 68
 - child pornography
 - definition, 298–9, 315
 - distribution and transmission, 335
 - offences, 325
 - offering or making available, 330
 - procurement, 339
 - statutes and, 294
 - computer, meaning of, 59
 - computer system, meaning of, 60
 - copyright infringement, 261, 269
 - data interception, 150–2
 - data modification/impairment, 112, 123–32
 - device misuse, 133–6

- extradition, 486
- forgery, 237
- fraud, 232–3
- harassment, 425
- jurisdiction, 475–7, 485
- sexually explicit conduct, 302
- stored versus live communications, 184
- traffic data, 169
- unauthorised access requirement, 52, 107
- cyber-dependent crimes, 11
- cyber-enabled crimes, 11
- cyberspace, crime in, 19
- cyberstalking, 419, 421, 424; *see also* harassment
- cyberterrorism, 12–15
- daemons, 41
- data access: *see* access offences
- data collection problems, 16–17
- data interception
 - Australia, 152–3, 158–60, 170–1, 184–7
 - Canada, 154, 160–2, 172–5, 187–92
 - communication, content versus metadata, 167–83
 - Cybercrime Convention, 150–2, 184
 - keyloggers, 161, 165–6
 - stored versus live communications, 182
 - surveillance compared, 193
 - telecommunications, 149–50, 158–67
 - United Kingdom, 154, 162–4, 175–8, 192–7
 - United States, 155–7, 164–7, 178–83, 197–8
- data modification/impairment; *see also* access offences
 - overview, 35–6, 112–13
 - Australia, 113–14, 117, 124–6
 - Canada, 115, 118–19, 126
 - conduct causing, 117–23
 - damage element, 129–31
 - legislation, 113–17
 - loss element, 131–2
 - parity with physical damage, 113
 - United Kingdom, 115–16, 119–20, 126–9
 - United States, 116–17, 120–2, 129–32
 - what constitutes, 123–32
- data storage devices, 70
- dating scams, 214–15
- debit card fraud, 213
- deleted files, 348, 361–2
- deletion, 123
- denial of service (DoS) attacks, 43–4, 130
- device misuse
 - overview, 36–8
 - access devices, 145–7
 - Australia, 136–8
 - Canada, 138–41
 - counterfeit devices, 147
 - dual use items, 135, 143–4
 - need for legislation, 133
 - United Kingdom, 141–4
 - United States, 144–8
- Digital Millennium Copyright Act (US), 262, 266
- digital rights management, 262
- digital technology, exploitation of, 3
- directory harvest attacks, 275
- distributed denial of service attacks (DDoS attacks), 44
- DNS-poisoning, 224
- domestic violence, 421; *see also* harassment
- Dotcom, Kim, 260, 488
- down-blouse images, 455
- drive-by-downloads, 38
- drop services, 228
- dual criminality, 487
- dual use items, 135, 143–4
- dumpster diving, 219
- eBay fraud, 212
- electronic commerce, 210
- electronic communication: *see* data interception (ECPA, US), 155
- electronic funds transfer crime, 216–17, 233–5
- emails, 166, 196, 223; *see also* spam

- encryption, as damage, 130
- exclusivity stage of grooming, 383
- expectation of privacy, 173–4
- external perspective on computer access, 68
- external perspective on online conduct, 20
- extortion, 214
- extradition, 486
- extradition treaties, 488

- Facebook, 34, 216, 221, 225
- false identification documents, 244
- false identification fraud, 218–20
- file-sharing, 257, 334
- filtering software, 272–3, 275
- First Amendment: *see* United States
- flagged ships, jurisdiction and, 476
- forgery, 220, 237–8
- fraud; *see also* copyright infringement; identity theft; phishing; spam
 - overview, 209–12
 - advance-fee fraud, 209, 214–16
 - carding, 227–8
 - click frauds, 216
 - computer-related forgery, 237–8
 - cost of, 231
 - credit card skimming, 225–7
 - deceiving machines, 235–6
 - device misuse and, 144
 - electronic funds transfer crime, 216–17, 233–5
 - identity information/theft, 218–20
 - internet enabling, 210–12
 - investment fraud, 217–18
 - legal responses to, 232–8
 - Nigerian mail fraud, 209, 214–16
 - online sales, 212–14
 - pharming, 223–4
 - scale of, 228–32
- friendship-forming stage of grooming, 380
- funds transfer crime, 216–17, 233–5

- gateway technology, 292
- grooming
 - overview, 377–85
 - anonymity, 379, 388
 - Australia, 389–90, 394–6, 403–4
 - Canada, 396–9
 - defined, 378
 - fantasy defence, 388, 408
 - grooming category, 394–401
 - inducing or procuring category, 402–13
 - internet access enabling, 378
 - legislative response, need for, 385–8
 - prevalence of, 385
 - stages of, 380
 - transmitting indecent or obscene material to minors category, 389–94
 - travelling with intent category, 413–16
 - United Kingdom, 390–2, 399–401, 405, 413–15
 - United States, 392–4, 402, 406–13, 415–16
- guardians, role of, 9

- hacking, 101, 224–5; *see also* computer targets
- hacktivism, 13
- handheld devices, 7–8; *see also* mobile phones
- happy slapping, 445
- harassment
 - overview, 417–20
 - Australia
 - fault requirement, 431
 - impact on victim, 433
 - offences, 425, 430
 - publication, 442
 - Canada
 - fault requirement, 431
 - impact on victim, 432
 - offences, 426, 429
 - surveillance, 450
 - communication with victims, 433–8
 - defined, 417
 - happy slapping, 445
 - indirect harassment, 423
 - legislation, 423–33
 - publication of information, 439–47
 - range of conduct, 419
 - revenge porn, 445

- scale of, 420–3
- sextortion, 447
- stalking compared, 424
- surveillance, 448–53
- targeting victim's computer, 447–8
- trolling, 437–8
- true threats, 434–7, 442
- United Kingdom, 426, 431–2, 447
- United States
 - course of conduct, 428
 - fault requirement, 431
 - free speech issues, 434, 440
 - impact on victim, 432
 - offences, 427
 - publication, 440, 442
- harvesting software, 275
- hijacking, 275
- honey pot websites, 343

- ICMP floods, 44
- identification documents, 244
- identity breeding, 220
- identity crime, 218–20, 230
- identity fabrication, 240
- identity manipulation, 240
- identity theft
 - overview, 238–41
 - Australia, 239, 243, 246, 248–50, 252
 - Canada, 239, 243, 246, 250
 - dealing in identity information, 248–52
 - defined, 218, 239–40
 - identity information defined, 241–5
 - manufacture of identity information, 252–4
 - need for offence, 238
 - possession of identity information, 245–8
 - United Kingdom, 239, 245–6, 250, 253
 - United States, 240, 244, 247, 251, 254
- Identity Theft and Assumption Deterrence Act of 1998 (US), 240
- impairment of data: *see* data modification/impairment

- implied extraterritorial jurisdiction, 479
- indecenty: *see* child pornography; grooming; voyeurism
- indirect harassment, 423
- information gathering, 448
- insiders, 101
- intended function test, 89
- internal perspective on computer access, 68
- internal perspective on online conduct, 20
- international comity, 485–6
- International Telecommunications Regulations, 278
- internet
 - child pornography, 289
 - communication types, 169
 - fraud easier with, 210–12
 - grooming, 378
 - as packet-switched network, 168
 - transformation by, 149
 - use of, 210
- internet access, 6
- internet of things, risks of, 5
- internet protocols, denial of service attacks and, 43
- intimate partner violence, 421; *see also* harassment
- investment fraud, 217–18
- IP addresses, 176, 181
- isanyoneup.com, 446

- jurisdiction
 - overview, 475
 - adjudicative, 481–6
 - Australia, 480
 - Canada, 477, 481
 - competing claims to, 483
 - enforcement, 486–8
 - extradition, 486
 - grooming, 415
 - international comity and, 485–6
 - prescriptive, 475–81
 - sovereignty and, 483
 - transnational nature of cybercrime and, 8
 - United Kingdom, 478
 - United States, 479–80

- Kazaa, 334
- KELIHOS, 41
- keyloggers, 42, 161, 165–6
- Kryogeniks, 35

- LambdaMOO, 19
- law enforcement, challenges of, 8–9
- legal identity, 241
- legislative environment; *see also*
 - Australia; Canada; United Kingdom; United States
- analogies lacking, 47–50
- Australia, 50–2
- Canada, 52–3
- existing laws, extensions of, 47, 91–3
- United Kingdom, 53–4
- United States, 54–5
- legislative jurisdiction, 475–81
- lent identities, 240
- LinkedIn, as personal information
 - source, 221
- linking sites, 266
- logic bombs, 39
- Love Bug virus, 487
- LulzSec, 34
- luring; *see* grooming

- mail transfer agents (MTA), 183
- malware; *see also* device misuse
 - overview, 38–43
 - carding, 228
 - computer support scams, 215
 - fraud, 224–5
 - scareware, 213
- man-in-the-middle attacks, 275
- Man-In-The-Browser (MITB) attacks, 40
- means of identification, 244
- media, 17
- Megaupload, 261
- Melissa virus, 39
- metadata, 168
- metering information: *see* data interception
- microfrauds, 211
- Mitchell, Ashley, 22
- mobile phones; *see also* data interception
 - child pornography, 291
 - computer, meaning of, 66
 - malware, 38
 - numbers of, 7
 - online banking, 210
- Model Anti-Stalking Code (US), 427, 430–2, 450
- modification of data: *see* data modification/impairment
- money laundering, 215
- money mules, 215
- morphed images, 314, 320–2
- MTA (mail transfer agents), 183
- mutuality of benefit, 373
- MySpace, 85

- Nationality Principle, 477
- networks, 12, 37–8, 125
- News of the World scandal, 195–6
- Nigerian mail fraud, 209, 214–16
- North American Man-Girl Love Association (NAMGLA), 293

- objective territoriality, 476
- obscenity: *see* child pornography; grooming; voyeurism
- offences against property, 21–2
- offences against the person, 21
- Oliver Scale, 303
- online banking, 210
- online sales, 212–14
- online worlds, 18–23
- online/offline consistency, 17–18
- Operation Buccaneer, 260
- organised crime, 293
- orphan folders, 293
- outside hackers, 101

- packet headers, 168
- packetizing information, 183
- packet-switched network, 168
- paedophilia: *see* child pornography
- participant monitoring, 192
- passing off identity information, 248–52
- passwords: *see* device misuse
- Peeping Toms: *see* voyeurism
- peer-to-peer (p2p) technology

- child pornography, 291, 331, 336
- copyright infringement, 257
- decentralised nature of, 257
- risks of, 5
- Pen Register Act (US), 157, 179
- pen registers, 157
- pharming, 223–4
- phishing, 145, 210, 220–3
- pings, 44
- pop-ups, 213, 327
- pornography: *see* child pornography
- port scanning, 34
- possession of child pornography: *see* child pornography
- possession of identity information, 245–8
- prescriptive jurisdiction, 475–81
- PricewaterhouseCoopers survey, 46
- privacy violations: *see* data interception; voyeurism
- private communications: *see* data interception
- Prosecutorial Remedies and Other Tools to end the Exploitation of Children Today Act (PROTECT, US), 319
- Protection of Children Act 1978 (UK), 332–3
- Protective Principle, 476
- proximity cards, 226
- proxy software, 292
- pseudonymity, 418
- pseudo-photographs, 315
- pump and dump schemes, 217

- Queensland: *see* Australia

- radio transmissions, 152, 159, 163
- ransomware, 225
- recording, 192
- registered aircraft, jurisdiction and, 476
- relationship-forming stage of grooming, 381–3
- remote access to victim's computers, 447
- remote access tools (RATs), 228
- rendered images, 314
- rental scams, 214

- revenge porn, 445
- rights management information (RMI), 262
- risk-assessment stage of grooming, 383
- romance scams, 214–15
- root level access, 32
- routine activity theory, 5

- sales online, 212–14
- scareware, 213
- screen capture software, 166
- Second Life*, 21
- Serious Crime Bill 2014 (UK), 54, 115, 143
- sexting, 301–2
- sextortion, 447
- sexual activity, 22–3
- sexual offences: *see* child pornography; grooming; voyeurism
- Sexual Offences Act 2003 (UK), 390, 399, 405, 413
- sexual stage of grooming, 384
- shared folders, 331
- ships, jurisdiction and, 476
- shoulder surfing, 226
- Simple Mail Transfer Protocol (SMTP), 183
- skimmers, 226
- skimming, 225–7, 241
- Smartnet II system, 66
- SMiShing, 223
- sniffer programs, 42
- social networking sites: *see also* Facebook
 - fraud, 222
 - grooming, 380
 - harassment easy with, 418
 - personal information sources, 221
 - spam, 273
- software applications, number of, 7
- source code, 34
- sovereignty and jurisdiction, 483
- spam
 - overview, 272–5
 - Australia, 279–81, 283
 - Canada, 279–81, 283
 - filtering software, 272–3, 275
 - legislation, 279–86

- spam (cont.)
 - regulation of, 275–9
 - United Kingdom, 279–81, 283–4
 - United States
 - commercial/bulk email, 282
 - consent, 283
 - criminal offences, 284
 - enforcement, 281
 - promotion of businesses, 284
 - statutes, 280–1
 - unsolicited commercial email versus bulk email, 282
- Spamhaus Project, 277
- spear phishing, 221
- Spector-Pro, 166
- Spoofcard, 434
- spoofing, 123, 275
- SpyEye virus, 42
- spyware, 42–3, 90, 447
- stalking, 419, 421, 424; *see also* harassment
- state actors, terrorist groups versus, 13
- store and forward delivery, 183
- Stored Communications Act (SCA, US), 156, 198–205
- streaming, 268
- structured query language injection attacks (SQL attacks), 34
- subject matter jurisdiction, 481–6
- subscriber data, 168
- sucker's lists, 223
- suppression of data, 123
- surveillance, 448–53; *see also* harassment; voyeurism
- swarms, 258
- system commands, 350

- technological protection measures (TPMs), 262
- telecommunications, 149–50; *see also* data interception
- Telecommunications (Interception and Access) Act 1979 (TIA Act, Aus), 152–3, 184–7
- telecommunications data: *see* data interception
- temporary internet files (TIFs), 348
- temporary storage, 198–202

- territorial jurisdiction, 476–81
- terrorism, 14–15
- text messages, 188–92
- torrent files, 258
- trade secrets disclosure, 130
- traffic data
 - content data compared, 169
 - defined, 168–9, 177
 - IP addresses, 181
 - Pen Register Act (US), 179
- trafficking, 136, 228; *see also* device misuse
- trap and trace devices, 157
- trash and cash schemes, 217
- TRIPS agreement (Trade-Related Aspects of Intellectual Property Rights), 262–3, 270–1
- trojans, 40–1, 224
- trolling, 437–8
- true threats, 434–7, 442
- Tšurikov, Sergei, 3
- Twelfth United Nations Congress on Crime Prevention and Criminal Justice, 25

- UBE (unsolicited bulk email), 282
- UCE (unsolicited commercial email), 282
- UGotPosted.com, 446
- under-reporting of crime, 16–17
- United Kingdom
 - access offences
 - access, meaning of, 71–3
 - generally, 57–8
 - unauthorised access requirement, 81–2, 96–8, 105–6
 - child pornography
 - advertisement, 333
 - defences, 370, 372
 - definition, 303, 311, 315
 - distribution of images, 336
 - offences, where found, 297
 - possession, 330, 344, 362
 - production, 325
 - communication, content versus metadata, 175–8
 - computer, meaning of, 60–4
 - copyright, 256, 262, 270

- credit card losses, 231
- data interception, 154, 162–4, 192–7
- data modification/impairment, 115–16, 119–20, 126–9
- device misuse, 141–4
- electronic commerce, 210
- fraud in, 229
- grooming, 390–2, 399–401, 405, 413–15
- harassment, 426, 431–2, 447
- identity crime, 230
- identity information/theft, 239, 245–6, 250, 253
- internet use rate, 210
- jurisdiction, 478
- legislative environment, 53–4
- online banking, 210
- spam, 279–81, 283–4
- voyeurism
 - conduct applied to, 468
 - defences, 471
 - depictions applied to, 460–1
 - distribution of images, 471
 - fault requirement, 469
 - where applicable, 464
- United States
 - access offences
 - generally, 59
 - statutes, 59
 - unauthorised access requirement, 81–3, 98–104, 106–7, 109–11, 164–7
 - Australia–US extradition treaty, 488
 - child pornography
 - accessing, 340
 - defences, 371–2
 - definition, 305, 311–12, 316
 - import/export, 338
 - offences, where found, 297
 - possession, 344, 364
 - procurement, 339
 - production, 325
 - receiving, 341
 - transport, 337
 - computer, meaning of, 64–7
 - copyright infringement
 - commercial infringement, 263
 - Digital Millennium Copyright Act (US), 262
 - distribution, 265
 - mens rea*, 270
 - numbers of cases, 259
 - credit card losses, 231
 - credit card skimming, 241
 - cyberbullying, 428
 - data interception, 155–7, 178–83, 197–8
 - data modification/impairment, 116–17, 120–2, 129–32
 - device misuse, 144–8
 - electronic commerce, 210
 - fraud in, 230
 - grooming, 392–4, 402, 406–13, 415–16
 - harassment
 - course of conduct, 428
 - fault requirement, 431
 - free speech issues, 434, 440
 - impact on victim, 432
 - offences, 427
 - publication, 440, 442
 - identity crime, 230
 - identity information/theft, 240, 244, 247, 251, 254
 - jurisdiction, 479–80
 - legislative environment, 54–5
 - online banking, 210
 - revenge porn, 446
 - spam
 - commercial/bulk email, 282
 - consent, 283
 - criminal offences, 284
 - enforcement, 281
 - promotion of businesses, 284
 - statutes, 280–1
 - value added by copyright industries, 256
 - voyeurism
 - conduct applied to, 467
 - depictions applied to, 460
 - distribution of images, 470
 - fault requirement, 469
 - protected speech, 456
 - where applicable, 464–5
 - unsolicited bulk email (UBE), 282

- unsolicited commercial email (UCE), 282
- unsolicited communications, authorised access and, 87–9
- up-skirt images, 455, 463
- URLs, 176, 181–2
- US Computer Emergency Response Team (US-CERT), 224
- user level hacking, 32

- virtual child pornography: *see* child pornography
- virtual crimes, types of, 21–3
- virtual currencies, 211
- viruses, 38–40, 213
- vishing, 223
- voice over the internet, as telecommunication, 167
- voice phishing, 223
- voicemail, News of the World scandal, 195–6
- voyeurism
 - overview, 454–5
 - Australia, 461, 463, 470
 - Canada
 - conduct applied to, 467
 - defences, 471
 - depictions applied to, 461
 - distribution of images, 470
 - expectation of privacy, 461
 - fault requirement, 468
 - up-skirt images, 463
 - conduct applied to, 467–8
 - criminalisation of, issues with, 455–9
 - defences, 471–2
 - defined, 454
 - depictions applied to, 460–1
 - distribution of images, 470–1
 - fault requirement, 468–9
 - legislation, 459–72
 - prevalence of, 454
 - revenge porn, 446
- United Kingdom
 - conduct applied to, 468
 - defences, 471
 - depictions applied to, 460–1
 - distribution of images, 471
 - fault requirement, 469
 - where applicable, 464
- United States
 - conduct applied to, 467
 - depictions applied to, 460
 - distribution of images, 470
 - fault requirement, 469
 - protected speech, 456
 - where applicable, 464–5
 - where applicable, 461–7
- wardriving, 36
- warez groups, 260
- watering hole attacks, 221
- web addresses, 176, 181–2
- website access, 87
- Wire Fraud statute (US), 234
- wireless hacking, 36
- Wiretap Act (US)
 - contents versus associated data, 178
 - interception, 156, 165, 197–8
 - stored versus live communications, 198–202
- World of Warcraft*, 18
- worms, 40

- ZeroAccess, 41
- zero-day vulnerabilities, 33