Index

accountability 153–8
cloud data ownership, and 153–8
cloud service reliability, and 256–7
definition 152–3
EU governance policy objectives 156–8
purpose 157–8
remediation, and 153, 155–6
transparency, and 152–6
Amazon 14, 57, 111, 242–3
America Online (AOL) 84
American Broadcasting Companies v Aereo 182–3
anonymized data 71, 75–8
anonymization 98–9
browser-generated information 81–2
data combination, and 84–5
data erasure, and 77–8
data fingerprints 82–3
data quality and size 91–2
de-identification, and 79–80, 90–91
definition 78–80, 86–7
EU policy on 77–80
identifiers, and 80–83
judicial rulings 85–8
law reform proposals 90–91
pseudonymous data, and 79–80
re-identification, and 77–80, 83–8, 90–91, 93–4
reuse of data, risk assessments 92–3
technological challenges 75–6
US policy on 91
vs. anonymous data 78–80
anonymous data 71
Big Data technology, and 97–8
Bio-PIN codes 238–9
vs. anonymized data 78–80
Apple 68, 188
Asia-Pacific Economic Cooperation
Cross-Border Privacy Rules (CBPR) 37–8
Australia
cloud policy developments 164–5, 181–2
cloud policy limitations 174–6
Copyright Amendment (Digital Agenda) Act 2000 170
copyright law
Creative Commons licensing 209
fair use doctrine 174–7
government works protection 209
protection gaps 174–6
safe harbor provisions 170
cross-border data flow controls 35
data protection 35
National Strategy for Cloud Computing 164–5
personal data, definition 74
BBC iPlayer 207
big data 71, 95, 97–8
binding corporate rules (BCR) 37, 111, 113
Bio-PIN 238
biomedical information see medical records
biomedical research see also genomic research
EU data protection regime 99–100
Icelandic biobank policy 226–7
medical records, use in 230–33
national biobank proposals 225–6
Boucher, R. 212
broadcasting
cloud streaming copyright challenges 182–3
geographical restrictions 212–13
Privacy and legal issues in cloud computing

definition 8, 12, 47, 118–19
development 8
elasticity 12–13
geraphical restrictions 212–13
justifications for 187–93
negative implications of 193–9
Bronner v Mediaprint 59–60
browser-generated information 81–2
community norms, and 158–9
data ownership 145–50
business applications 1–2
global business strategies 206–8
Cartoon Network et al. v Cablevision 178
Chile
safe harbor provisions 171
China
cloud computing policy development 164
civil liabilities see also safe harbor provisions
applicable law 133–5
centre of interests principle 132
cloud service reliability and accountability 256–7
copyright law
cloud service providers 169–74
cloud users 165–9
court competence 131–3
direct/indirect liabilities 169
deo-determined intent of user 131–3, 135–8
internet, evidence of 135–6
jurisdictional conflicts 127–8
terms of service restrictions 260
cloud computing, generally see also
data processing; data protection;
entertainment content;
jurisdiction; uploading
advantages 1–2, 8–9, 106, 118–19, 161–2, 181, 261
challenges, generally 11
characteristics 12–13
cloud lockers 180
community clouds 15–16
community norms 158–9
consumer protection 123–4, 126–7
data preservation and deletion policies 246–7, 280–81, 288–9
investment trends 178
IP regime applicability to 65–8
legal safeguards
cloud contract limitations 66–7
data protection regime 65
EU National Information Security Directive 63
government/intelligence agencies, cloud access by 64–5
intellectual property regime 65–8
national policy and strategy development 163–5
open system, benefits of 43–4
private clouds 15–16, 27, 272–90
public clouds 15–16, 27
regulatory safeguards
competition law 44–6, 52–63
data portability/interoperability 47, 54–5
e-commerce regime 46–7, 50–52
generally 43–4
information society services 49–50
jurisdiction 52
market definition 53–4
network neutrality 47–9
sector-specific regulation 45–52,
67
technological changes,
implications of 96–7
vertical integration 49–50, 55–63
reliability concerns 242–3, 256
revenue from 1–2, 10
risk vs. flexibility 18–19
sector growth 1–2, 10, 28
security challenges
generally 16–17, 25
Index

inherent challenges 17–20
IT management implications 20–21
provider-user relations 20
security responsibility sharing 18–19
threats, types of 17–18
security solutions
  data encryption 23–4
generally 21–2
  hardware-anchored security 24
  sensitive data removal 24–5
service level agreements 22
service delivery models 13–15, 19, 27
service deployment models 15–16, 27
service reliability and accountability 256–7
Terms of Service (ToS) 111
trends 1–2, 10, 160–62
trial periods 273–4
zoning 131–7
cloud lockers 180
community clouds 15–16
community norms 158–9
competition law
  advantages and disadvantages 45
  applicability 45–6
  customer lock-in 54–5
  data portability/interoperability 54–5
downstream/upstream markets 53–4
entertainment content 195–6
general role in 44–6
geographical restrictions 195–6
market definition 53–4
market dominance 54–9
purpose 44–5
refusal to supply 59–63
restrictive agreements 55–6
vertical integration, and 49–50, 55–63
confidential information
  ownership of data generated in cloud 149–50
  ownership of data placed in cloud 144–5
consent
  data processing 35, 87–8, 93–4, 105, 137
EU Data Protection Regulation (proposed) requirements 114–15
medical data transmission 223–4, 228, 230–31
obtained by proxy 231
research use, and 230–33
right to withdraw 114
consumer protection
generally 123–4, 126–7
geo-determined intent of users 137–8
contract law
  Business Associate Contracts 234, 250
  constructive contracts 262
contract law, generally
  balance between parties 265–6
cloud computing challenges 263–6
  legal certainty, and 265
contract terms
  audit rights 277–8
  change control rights 276
  commitments to contract 271–2
  compliance obligations 277–9
customer control rights 276
customers’ data, rights over 281–3
data location 279–80
data retention 288–9
data return or deletion 280–81, 288–9
derived information, rights over 283–4
generally 266–7
implied terms 264–5
information security 280
infringement remedies 285–6
liability limitations 278–9
licensing
  customer understanding of 264
generally 263–6
  implied terms 264–5
  modification 266
  risk implications 265
  subject of license 268–9
minimum term commitments 272–3
modification 266
Privacy and legal issues in cloud computing

- non-infringement warranties/indemnities 284–5
- non-suspension/interruption protection 286–7
- permissible uses 269–70
- personnel continuity 287
- service commitments 271–3
- service continuity protections 286–7
- service level commitments 274–5
- service quality protections 273–6
- technical architecture rights 276
- termination assistance 287–9
- termination clauses 270–71
- testing and acceptance 273–4
- updates, inclusion of 268

Convention on Jurisdiction and Foreign Judgments in Civil and Commercial Matters (proposed)(Hague Conference) 204–5

- copyright law
- computer programs 141–2
- copyright gap 173–4
- country of origin challenges 146
- creativity requirement 141–2
- data generated in cloud 145
- data placed in cloud 141–2
- digital copyright exceptions 168–9
- digital works 141
- DVR services 175, 178
- EU law 141–2, 146–7
- fair use/personal use doctrine 168, 176–7, 212
- benefits of 177–8
- safe harbor provisions, and 173–5, 179
- geographical restrictions
- benefits of 187–93, 198–9
- disadvantages of 193–9
- government works, protection of 208–9
- historical development 184–5
- independence of right doctrine 184–5
- jurisdiction
- applicability of protections 185–6
- national law divergence, and 184–5
- under private international law 127
- liabilities
- of cloud service providers 169–74
- of cloud users 165–9
- principles, generally 141
- private copying exemptions 168
- safe harbor provisions 169–73
- terms of use 166–7
- US law 141–2, 146, 168, 172–3
- vs. authors’ rights 141
- country code top level domains (ccTLD) 135–6
- cross-border data flows
- control mechanisms
- binding corporate rules (BCR) 37, 111, 113
- CBPR 37–8
- compensation controls 38
- data portability policies, and 210–12
- data storage risks 36
- digital passports 210–11
- EU National Information Security Directive 63
generally 35–6, 43–4
- international law obligations, and 129–30
- international mechanisms 37–8
- international treaty approaches 203–4
- safe harbor provisions 37, 64, 110–13, 116–17, 169–73, 254
- EU to US flows
- adequacy decisions 109–11
- challenges 116–17
- Data Protection Regulation provisions 106–16
disclosure to third parties 113–16
- EU regime applicability 103–7
- EU regime exclusions 109–10
- EU regime requirements 109–12
- information policies 113–15
- regulatory challenges 96, 99–100
- Safe Harbor Agreement 37, 64, 110–13, 116–17
- transfers to sub-processors 112–13
- regulatory challenges
data portability/interoperability 47
data storage risks 36
<table>
<thead>
<tr>
<th>Data Protection</th>
<th>295</th>
</tr>
</thead>
<tbody>
<tr>
<td>EU regime, in</td>
<td>129–30</td>
</tr>
<tr>
<td>generally</td>
<td>35–6, 43–4, 65</td>
</tr>
<tr>
<td>Cross-Border Privacy Rules (CBPR)(APEC)</td>
<td>37–8</td>
</tr>
<tr>
<td>cybertravel</td>
<td>210</td>
</tr>
<tr>
<td>data, definition</td>
<td>7</td>
</tr>
<tr>
<td>data fingerprints</td>
<td>82–3</td>
</tr>
<tr>
<td>data loss, risks of</td>
<td>17, 67</td>
</tr>
<tr>
<td>data mining</td>
<td>84–5, 149, 158</td>
</tr>
<tr>
<td>data ownership</td>
<td>152–8</td>
</tr>
<tr>
<td>cloud challenges</td>
<td>139</td>
</tr>
<tr>
<td>community norms, role of</td>
<td>158–9</td>
</tr>
<tr>
<td>confidentiality</td>
<td>144–5, 149–50</td>
</tr>
<tr>
<td>contract law influences</td>
<td>145</td>
</tr>
<tr>
<td>copyright</td>
<td>141–2, 145</td>
</tr>
<tr>
<td>country of origin</td>
<td>146</td>
</tr>
<tr>
<td>customer relationships</td>
<td>142–3</td>
</tr>
<tr>
<td>data mining</td>
<td>149</td>
</tr>
<tr>
<td>database rights</td>
<td>142, 146–8</td>
</tr>
<tr>
<td>derived information</td>
<td>148–9, 158–9, 283–4</td>
</tr>
<tr>
<td>encryption</td>
<td>150</td>
</tr>
<tr>
<td>endowment effect</td>
<td>139–40</td>
</tr>
<tr>
<td>information generated in cloud</td>
<td>145–50, 158–9</td>
</tr>
<tr>
<td>information placed in cloud</td>
<td>140–45</td>
</tr>
<tr>
<td>metadata</td>
<td>148–9</td>
</tr>
<tr>
<td>ownership concept</td>
<td>139–40</td>
</tr>
<tr>
<td>privacy rights, and</td>
<td>140</td>
</tr>
<tr>
<td>terms of service</td>
<td>150–51</td>
</tr>
<tr>
<td>transparency</td>
<td>152–6</td>
</tr>
<tr>
<td>TRIPS Agreement protection</td>
<td>143–4</td>
</tr>
<tr>
<td>uploaded data, misconceptions about</td>
<td>262</td>
</tr>
<tr>
<td>use controls</td>
<td>150–52</td>
</tr>
<tr>
<td>data processing</td>
<td>108</td>
</tr>
<tr>
<td>activities, context of</td>
<td>108</td>
</tr>
<tr>
<td>automated data certificates</td>
<td>112</td>
</tr>
<tr>
<td>consent</td>
<td>35, 87–8, 93–4, 105, 137</td>
</tr>
<tr>
<td>right to withdraw</td>
<td>114</td>
</tr>
<tr>
<td>controller representative requirements</td>
<td>106–7</td>
</tr>
<tr>
<td>controller vs. processor distinction</td>
<td>101–3</td>
</tr>
<tr>
<td>data transfers to sub-processors</td>
<td>112–13</td>
</tr>
<tr>
<td>definition</td>
<td>100–101</td>
</tr>
<tr>
<td>disclosure to third parties</td>
<td>113–16</td>
</tr>
<tr>
<td>establishment, classification of</td>
<td>108–9</td>
</tr>
<tr>
<td>EU regime applicability</td>
<td>103–7</td>
</tr>
<tr>
<td>information policies</td>
<td>113–15</td>
</tr>
<tr>
<td>justifications for</td>
<td>104–5</td>
</tr>
<tr>
<td>private international law jurisdiction, and</td>
<td>128</td>
</tr>
<tr>
<td>Safe Harbor Agreements</td>
<td>110–13, 116–17, 254</td>
</tr>
<tr>
<td>safeguard exceptions</td>
<td>110–11</td>
</tr>
<tr>
<td>surveillance, and</td>
<td>115–16</td>
</tr>
<tr>
<td>data protection see also cross-border</td>
<td>33</td>
</tr>
<tr>
<td>data flows; medical records; outsourcing</td>
<td>34</td>
</tr>
<tr>
<td>accountability</td>
<td>32, 34</td>
</tr>
<tr>
<td>best efforts policies</td>
<td>251</td>
</tr>
<tr>
<td>cloud challenges</td>
<td>29, 33–41, 99–100</td>
</tr>
<tr>
<td>collection restrictions</td>
<td>30–31, 34</td>
</tr>
<tr>
<td>compensation controls</td>
<td>38</td>
</tr>
<tr>
<td>consent</td>
<td>137</td>
</tr>
<tr>
<td>controller representative requirement</td>
<td>106–7</td>
</tr>
<tr>
<td>controller vs. processor distinction</td>
<td>101–3</td>
</tr>
<tr>
<td>data breach management</td>
<td>34</td>
</tr>
<tr>
<td>data collection restrictions</td>
<td>30–31</td>
</tr>
<tr>
<td>data erasure/exit policies</td>
<td>31, 33, 77–8, 246–7</td>
</tr>
<tr>
<td>data quality</td>
<td>31</td>
</tr>
<tr>
<td>data storage</td>
<td>36, 246–7</td>
</tr>
<tr>
<td>data transfer restrictions</td>
<td>32</td>
</tr>
<tr>
<td>data use restrictions</td>
<td>34</td>
</tr>
<tr>
<td>data users, and</td>
<td>29, 41–2</td>
</tr>
<tr>
<td>definitions</td>
<td>295</td>
</tr>
<tr>
<td>EU regime</td>
<td>69–70, 72–7, 88–90, 97–100</td>
</tr>
<tr>
<td>personal data</td>
<td>73–4</td>
</tr>
<tr>
<td>processing</td>
<td>100–101</td>
</tr>
<tr>
<td>US regime</td>
<td>74–5, 86–7, 89</td>
</tr>
<tr>
<td>formal contractual relationships, and</td>
<td>39</td>
</tr>
<tr>
<td>identity management/authentication</td>
<td>33</td>
</tr>
<tr>
<td>individual participation</td>
<td>32, 34</td>
</tr>
</tbody>
</table>
international control mechanisms 37–8
ISO information security standards 251
judgment calls, and 40
monitoring activities 107
outsourcing and subcontracting 29, 33–4, 38–41
participation principle 34
principles 29–34
accountability 32, 34
collection restrictions 30–31, 34
data erasure/exit policies 31, 33
data quality 31
data transfer restrictions 32
identity management/authentication 33
individual participation 32, 34
purpose driven 30–31
security safeguards 31
use restrictions 31
privacy awareness, and 40
private international law jurisdiction 128
regulatory challenges
cross-border data flows 35–8
outsourcing 33–4
security/compliance gaps 40
standard terms and conditions 40–41
subcontracting agreements 38–40
technological change, rate of 96–7
verification 40–41
risks 28
security safeguards 31
special data categories 100
verification 40–41
databases
data reutilization or extraction 147–50
EU protection regime 142, 146–7
US protection regime 147–8
Datatium LLC 82
denial of service (DoS) 18, 256
digital passports 210
disclosure
data disclosure/reuse risk assessments 92–3
legal requirements 64–5
medical records 229
to third parties 113–16
discrimination 190–91, 249–50
Doll, R. 214–15
Donner (criminal proceedings) 134
Dropbox 15, 111, 143, 151, 167, 272
due diligence, importance of 289–90
DVD region codes 187–9, 193–4, 197–8
e-commerce
access provider functions 50–51
definition 47
EU internal market provisions 130
hosting providers, and 51–2
service provider liabilities 50–51
eDate Advertising GmbH v X and Olivier Martinez 130, 132
elasticity 12–13
encryption
advantages and disadvantages 71, 150
generally 23
genomic data 247–8
homomorphic encryption 23–4
incremental encryption 24
endowment effect 139–40
entertainment content
anti-piracy policies 192–3
censorship, and 192, 197–8
competition, and 195–6
cultural rights, and 197–8
distribution and licensing 191–2
price discrimination, and 190–91
regulatory standards, national variations in 192–3
sequential distribution 188–9
EU see also cross-border data flows
A4 Cloud Project 156–8
Access Directive 46–7
Index

Authorisation Directive 46
Brussels I Regulation 123–5, 131–3, 135–6
Cloud Computing Strategy 10
Cloud Partnership 10
cloud policy development 10, 156–8, 164
Community Trade Mark 200
competition law
  abusive market behaviours 55–63
  harmonization, benefits of 62–3
  market dominance 56–9
  refusal to supply 59–63
  vertical restraints 55–6, 61–3
customer protection 123–4, 126–7
copyright law
  broadcast streaming 182
  country of origin principle 146
database right 146–7
digital works and software 141–2
  national treatment principle 204
  review and reform 200
Data Protection Directive
  applicability of 103–5, 107
  internal market clause 130
  personal data, definition 73–5, 97–100
  processing, definition 100–103
  technological change, challenges of 96–7
data protection regime, generally
  applicability 103–7, 135
  cloud computing, and 28, 96–7, 101–3
  controller vs. processor distinction 101–3
data transfers within EU 105–6
disclosure to third parties 115–16
  establishment, classification of 108–9
European Data Protection Seal 111
  monitoring activities 107
  personal data, interpretation 69–70, 73–5, 78–9, 88–90
  review and reform proposals 76–7, 97, 101–3
Data Protection Regulation
  (proposed)
  applicability of 103–7
  automated data certificates 112
  benefits of 112–13
  consent requirements 114–15
  data transfers between EU and US 106–16
data transfers to sub-processors 112–13
data transfers within EU 105–6
disclosure to third parties 113–16
generally 76–9, 90, 97, 116
  information policies 113–15
  surveillance, and 115–16
Database Directive 142
Digital Agenda for Europe 211
e-commerce
  access provider functions 50–51
  background/generally 46–7
  hosting providers, and 51–2, 115–16
  internal market provisions 130
  service provider liabilities 50–51
electronic communications
  framework
  accountability, and 156–8
  background 46–7
  governance policy objectives 156–8
  information society services, and 50
  transparency, and 48–9, 156–8
European Data Protection Seal 111
  jurisdiction
  applicable international law 125–30
  choice of forum 123–4
  conflicts of law rules 125–8
  court competence 123–5, 131–3
  default rules 125
  substantive international obligations 129–30
Licences for Stakeholders policy proposals 211
National Information Security Directive 63
network neutrality, and 48–9
patents and trademarks 200
Rome I Regulation 126, 133
Privacy and legal issues in cloud computing

Rome II Regulation 126–7
Universal Service Directive 46
European Commission v Federal Republic of Germany 60–61
European Convention on Human Rights 128–30
European Genome-Phenome Archive 238
ex-ante regulation see sector-specific regulation
ex-post regulation see competition law

Facebook 15, 82–3
Beacon 154–5
biometric identification 99–100
data mining 149
data ownership 143–5, 152, 154–5
data transfers, EU regime
applicability 110
terms of service 152, 154–5, 272
transparency policies 154–6, 159
fair use doctrine see copyright law
Flickr 116
Football Dataco v Sportradar 134, 147–8
France Telecom 58–9
France v Turkey (Lotus case) 120–21

genomic research
accountability conflicts 256–7
best efforts policies 251
big data challenges 238
Bio-PIN codes 238–9
Business Associate Contracts 234, 250
Cancer Genome Consortium 238
cloud benefits 239–42, 257–8
cloud concerns 242–3, 257–8
cloud contract types 241
cloud reliability, and 242–3, 256
cloud service deployment
characteristics 240–41
confidentiality 248–53
data controls 245–8
data encryption 247–8, 258
data location and transfer 253–6
data monitoring 247–8, 258
data privacy 223–57
data security 242, 248–53
data set size 237–9
data storage and deletion policies 246–7
ethical issues 258–9
genetic discrimination, and 249–50
genome sequences 237–8
Global Alliance for Genomics and Health 258
jurisdictional influences 255–6
multi-stakeholders in 258
safe harbor provisions 254
sample donor anonymity 238
terms of service amendments 245–6, 256–7
transparency, importance of 257–8
geraphical restrictions
anti-piracy policies, and 192–3
censorship, and 192, 197–8
competition, and 195–6
consmption patterns 194–5
cultural rights, and 197–8
disadvantages of 193–9, 212–13
distribution and licensing 191–2
DVD region codes 187–9, 193–4, 197–8
justifications for 187–93, 198–9, 212–13
price discrimination, and 190–91
regulatory standards, national variations in 192–3
sequential distribution 188–9
German Telekom 58–9
Germany
copyright law 141–2, 168
data protection law 251

Google
AdSense 94
AdWords 132
App Engine 14
data mining 149
data quality and size, implications of 91
data sensitivity challenges 94
Flu Trends 91
Health 243
Maps 15
Index

market dominance 57
personal data use litigation 81–2, 87–8
safe harbor provisions, and 174
Street View 128
terms of service 151
Gurry, F. 203–4

hackers 18
Handelskwekerij GI Bier BV v Mines de potasse d’Alsace SA 131–2
hardware-anchored security 24
Hargreaves Review of Intellectual Property and Growth 208
healthcare information see medical records
hijacking 17–18
HIV/AIDS 232
Hong Kong
cross-border data flow controls 35
personal data, definition 74
hosting providers 51–2, 115–16
Hotel Alpenhof GesmbH v Oliver Heller 131
hybrid clouds 15–16, 244, 272–90

Iceland
National Biobank policy 226–7
iCloud 68
ICT, generally
law, and
applicability to 158–9
challenges of 2–3
technological change
extraterritorial extension
mechanisms 210–12
rate of 96–7
regulatory safeguards, and 96–7
vulnerability and risk 18, 243
indemnities, for non-infringement 284–5
independence of right doctrine 184–5
information and communication technology see ICT
information security 2
CSP encryption 23–4
hardware-anchored security 24

importance 11
responsibility sharing 18–19
sensitive date removal 24–5
Infrastructure-as-a-service (IaaS) model 14, 27, 166–7
intellectual property, generally 2 see also copyright law; data ownership; databases
choice of law principles
developments 204–6
cloud computing, and
contract law influences 66, 145
customers’ data, rights over 281–3
derived information 148–9, 158–9, 283–4
regime applicability to 65–8
cultural rights protection 197
EU Community Trade Mark 200
treaty developments 199–204
TRIPS Agreement protection 143–4, 201–2
intelligence agencies, cloud data access by 64–5
International Cancer Genome Consortium 238
Internet, generally 261
advantages 118–19, 221–2
misconceptions about 262
search engines, role of 221–2
internet piracy 207–8
Io Group Inc. v Veoh Networks Inc. 173
ISO information security standards 252
IT governance
EU regime
background 46–7
information society services, and 50
transparency, and 48–9, 156–8
Itar-Tass Russian News Agency v Russian Kurier, Inc. 204
iTunes 188
ITV Broadcasting Ltd v TV Catch Up Ltd 182
Japan
Smart Cloud Strategy 163

Anne S.Y. Cheung and Rolf H. Weber - 9781783477074
Downloaded from Elgar Online at 02/09/2019 06:04:33AM
via free access
jurisdiction
adjudicative jurisdiction 120
cloud computing, and
applicable law 133–5, 185–6
bordered services 131–7
centre of interests principle 132
consumer protection issues 137
contract restrictions 66–7
copyright challenges 146, 181–6
country code top level domains (ccTLD) 135–6
country of origin 146
court competence 131–3
extraterritorial extension, benefits of 186, 199–213
geo-determined intent of users 131–2, 135–8
geographical restrictions, and 187–93
geolocation blocking 136
internet, evidence of 135–6
location independence 12–13
multiple infringements, and 186
monitoring targeting 131–3
technology, relevance of 121–2, 125
territorial anchoring 121
definition 119–20
enforcement powers, and 120–22
extraterritorial extension
mechanisms
by business practice 206–8
choice of law principles, and 204–6
by contract law 206–8
cross-border data portability 210–12
digital passports 210
enforcement of judgments focus 205–6
EU policies 200–201
exhaustion of rights, policy development challenges 201–2
by government policy 208–10
government works, copyright protections on 208–10
by law 204–6
potential benefits of 199
by technological development 210–12
by treaty 199–204
unitary rights, development challenges 200–201
US policies 204–5, 255–6
interpretation, importance of 120
location independence 12–13
prescriptive jurisdiction 120–21
private international law, and 119–20
applicable law 125–30
choice of forum 123–4, 204–6
conflict of laws rules 125–8, 204
copyright law 127
court competence 123–5, 131–3
data protection 128
privacy laws 127–8
reform proposals 204–5
substantive international obligations 129–30
third party jurisdictions 124
public international law, and 120–21

Kirtsaeng v John Wiley & Sons, Inc. 202

Lansley, A. 216
law, and technological development
applicability 158–9
challenges 2–3
licensing see also contract terms
in Australia 209
contract law challenges 262–6
Creative Commons licensing 209
customer owned data 262–3
entertainment content, of 191–2
essential terms 266–89
government works 209
implied contracts 263
legal certainty 265
proprietary software 262
service providers owned/licensed data 263
terms, identification difficulties 263–6
LinkedIn 144–5
location independence 12–13
Index

L’Oréal SA and Others v eBay
International AG and Others
133–4

measured services 12–13
medical records
analogue to electronic data conversion
consolidation and conflation 220–21, 230–31
database design difficulties 217–19
diagnostic images, samples and charts 219
maintenance of old records requirements 219
methods 214
new uses for data, and 222–7
privacy conflicts 228–30
process complexity 217–19
purpose and data uses 219–20
standardisation, lack of 217–19
anonymized data 74–5, 80–81, 85–95
Business Associate Contracts 234, 250
data fragmentation 235
data privacy conflicts 94, 223–4
cloud computing, and 232–6
consent 223–4, 228
control 232
data conversion process, and 223–4, 228
data disclosure requirements 229
genetic testing, and 229–30, 249–50
historical influences 227–8
insurance companies, and 229
privacy assumptions 227–30
relational information, and 230–31
third party rights 229–30
digitisation policies
background 214–15
UK policies 215–16, 219–20, 222, 225, 233
longitudinal electronic medical records/databases 222–5, 230, 232–4
profile of disease and healthcare patterns 222–5
metadata 148–9
Microsoft 14, 57, 60
Microsoft v Commission 60
Moben v 335 LLC 146
multi-tenancy 12–13

National Rugby League Investments Pty Ltd v Singtel Opus 175
Netfix 84–5
network access 12–13
network neutrality 47–9
Nirvanix 243
Northwestern Memorial Hospital v Ashcroft 85–6

OECD data protection and privacy guidelines 30
on-demand self-service 12–13
Open Web Application Security Project (OWASP) 11
outsourcing and subcontracting see also contract terms
data breach management 34
data erasure/exit policies 33, 246–7
data location 279–80
data protection challenges 29, 33–4, 38–9
data use restrictions 34
identity management/authentication 33
judgment calls, and 40
participation principle 34
privacy awareness, and 40
ownership see data ownership

Peter Pammer v Reederei Karl Schlüter GmbH & Co KG 104, 131
personal data, generally see also anonymized data; anonymous data; data ownership; medical records; pseudonymous data
accountability 93–4
big data 71, 95, 97–8
cloud computing, and accountability, and 93–4
challenges 99–100
data disclosure and reuse risk assessments 92–3
data quality and size 91–2
de-identification, and 90–91
genewly 88–90 reidentification, need for 95
consent, 35, 87–8, 93–4, 105, 137
right to withdraw 114
data fingerprints 82–3
data quality and size 91–2
definition 69–71
direct vs. indirect data 76–7
EU regime 69–70, 72–7, 88–90, 97–100
identified vs. identifiable data 69–70, 72–80
realistic risk of identification 89–90
reidentification, need for 95
special data categories 100
US regime 74–5, 86–7, 89
identifiers
browser-generated information 81–2
nature of 80–83
linkable data fields 82–3
ownership, attitudes to 70–71
profiling 82–3, 92–3
reidentification 77–80, 83–8, 90–91, 93–4
technology influences on 72
Peter Pinckney v KDG Mediatech AG 132–3
plaintext 23
Platform-as-a-service (PaaS) model 14, 19, 27, 166
price discrimination 190–91
privacy 2
data ownership, and 140
data users, of 29
definition 71–2
private international law
jurisdiction 127–8
substantive law obligations 129–30
responsibility sharing 18–19
private clouds 15–16, 27, 272–90
profiling 82–3, 92–3
medical records, and 222–4
pseudonymous data 71, 78–80, 90–91, 93
public clouds 15–16, 27
Quality King Distributors, Inc. v L’Anza Research International, Inc. 202
Rackspace 14
Ragnhildur Guðmundsdóttir v The State of Iceland 226–7, 230
reidentification 77–80, 83–8
data combination, and 84–5, 93–4
legal challenges 85–8
Reding, V. 80
remediation 153
resource pooling 12–13
restrictive agreements 55–6
risk
data breaches 17
data loss 17, 67
data storage 36
denial of service (DoS) 18
diligence, inadequacy of 18
hackers and hijackers 17–18
malicious insiders 18
outage 242–3
technological vulnerability 18, 243
Safe Harbor Agreement (US-EU) 64, 110–13
background 37
data transfers to sub-processors 112–13
protection beyond scope of 115–17
surveillance activities, and 115–16
Terms of Service, and 111
US judicial interpretation 172–3
safe harbor provisions
background 169–70
data location and transfer 254
fair use doctrine, and 173–7, 179
purpose 169–70
US judicial interpretation 172–3
US-style free-trade agreements, development of 170–72
search engines, importance of 221–2
sector-specific regulation
advantages and disadvantages 45, 67
applicability 45–6
data portability/interoperability, and 47
e-commerce regime 46–7, 50–52
network neutrality 47–9
vertical integration 49–50
sensitive data see also medical records
discrimination, and 94, 249–50
service delivery models
copyright liabilities 166
data protection responsibilities 27
generally 13–14, 19
Infrastructure-as-a-service (IaaS)
model 14, 27, 166–7
Platform-as-a-service (PaaS) model
14, 19, 27, 166
Software-as-a-service (SaaS) model
15, 19, 27, 34, 112, 166
Service Level Agreements (SLAs) 22
Shapiro, A. 212
_Fiona Shevell and Others v Presse Alliance SA_ 132
Singapore
safe harbor provisions 171–2
Snowden, E. 110
Software-as-a-service (SaaS) model 15,
19, 27, 34, 112, 166
Spain
Google privacy litigation 87
standard terms and conditions see contract terms
Statement on Standards for Attestation
Engagements (SSAE) 251
Subafilms, Ltd v MGM-Pathe
Communications Co. 185
subcontracting see outsourcing and
subcontracting
surveillance
EU data processing restrictions
115–16
EU to US data transfers, and 115–16
US jurisdictional reach 64, 115–16,
255–6

_Telecom Italia_ 62
terms of service see also contract terms
amendment protocols 245–6, 256–7,
260
data ownership, and 151–2, 167
data storage and transfer 260
IaaS service models 167
liability limitations 260
transparency
benefits of 154–5, 257–8
cloud data ownership, and 152–6
definition 153–4
EU governance policy objectives
156–8
network neutrality, and 48–9
Treaty on Audiovisual Performance
(2012) 203
Treaty to Facilitate Access to Published
Works for Persons who are Blind
(2013) 203
Trimble, M. 210
TRIPS Agreement 143–4, 201–2
Twitter 82

UK
Biobank Project 225–6
cloud policy development 164
contract law restrictions 66–7
database rights 147
medical records digitisation 215–16,
225–6, 232–3
National Programme for IT 215–16,
219–20, 222, 233
UMG Recordings Inc. v Veoh Networks
Inc. 173
uploading content
constructive contracts, and 262
data ownership misconceptions 262
US court copyright interpretations
172–3

US
see also cross-border data flows
censorship 192, 198
Children’s Online Privacy Protection
Act 74
copyright law
broadcast streaming 182–3
choice of law provisions 204–5
country of origin conflicts 146
digital works 141–2, 168
exceptions 168
exhaustion of rights 202
fair use doctrine 168, 176–9, 212
first sale doctrine 202, 212
government works protection 208–9
jurisdiction 185–6
uploading, judicial rulings 172–3
Digital Media Consumers’ Rights Act 212
Digital Millennium Copyright Act 168, 170, 172–3
Federal Cloud Computing Strategy 163
Foreign Intelligence Surveillance Act 64, 115
medical records
Business Associate Contracts 234, 250
digitisation policies 233–5
Health Information Technology for Economic and Clinical Health Act 234–5
Health Insurance Portability Act 74–5, 80–81, 85–95, 233–4
privacy conflicts 233–5
Patriot Act 115, 255
personal data
data ownership 146
de-identification, and 80, 91
definition 69–70, 74–5, 86–7, 89
disclosure to third parties 115–16
government/intelligence agency
data access 64
re-identification 85–6
surveillance, and 64, 115–16
safe harbor provisions 37, 64, 110–13, 116–17
free trade agreements 170–72
Notice and Takedown regime 170–71
Video Privacy Protection Act 74
vertical integration
abusive market behaviour 56–63
information society services, and 49–50
market dominance 56–9
refusal to supply 59–63
restrictive agreements 55–6
Viacom International Inc. et al. v YouTube Inc. et al. 173
Vidal-Hall v Google Inc. 81–2
virtual machines (VMs) 9
Wannadoo 58
warranties, for non-infringement 284–5
Wintersteiger AG v Products 4U Sondermaschinenbau GmbH 132
WIPO Internet Treaties 169, 203–4
YouTube 15, 188
zoning 131–7