

Index

- access, to data
 - in government cloud computing, 45–46
 - for Government Cloud system, limitations on, 24
 - by intelligence agencies, 84–89
 - under Executive Order 123333, 85–86
 - under Foreign Intelligence Surveillance Act, 85–86
 - limitations for, 88–89
 - PRISM program, 86–88
 - remedies for, 88–89
 - UPSTREAM program, 87–88
 - law enforcement agencies and, 3–4
 - security services on, 3–4
- accountability
 - in government cloud computing, 44–45, 57–58
 - Health Insurance Portability and Accountability Act of 1996, 148
- accountability principle, data protection and, 110
- agreements. *See* framework agreements; master services agreement; service level agreement; *specific agreements*
- AstraZeneca v International Business Machines Corporation*, 225–26
- audits
 - for data processors, obligations of, 119–20
 - in standardization of cloud computing contracts, 243–44
 - transparency in, 43
- B2B agreements. *See* Business-to-Business agreements
- B2C agreements. *See* Business-to-Consumer agreements
- B2G agreements. *See* Business-to-Government agreements
- back-to-back contracts, 187–88
- binding corporate rules (BCRs), 134
- blockchain contracts, 248
- breach, of cloud computing contracts, 209–11
- Brexit, 7, 100
- Business-to-Business agreements (B2B agreements), 14–15, 205
- Business-to-Consumer agreements (B2C agreements), 14–15
- Business-to-Government agreements (B2G agreements), 14–15
- CaaS. *See* Communications as a Service
- call-off contracts, 171–77
- carbon footprint, of cloud computing, xi–xii
- Carpenter v. US*, 146–48
- Charter of Fundamental Rights of the European Union, 92
- CIA. *See* Confidentiality, Integrity, and Availability of data
- Clarifying Lawful Overseas Use of Data Act (CLOUD Act), US (2018)
 - for cloud service providers, 80–84, 90
 - in *Microsoft* warrant case, 76–77
 - mutual legal assistance treaties and, 81, 83
- cloud barriers, to government cloud computing, 47–50
- cloud clients
 - Business-to-Consumer agreements, 14–15
 - definition, 11
 - government as, 42–46
 - accessibility and, 45–46
 - accountability in, 44–45, 57–58
 - availability and, 45–46
 - legitimacy and, 45, 57–58
 - loss of competence and, 46
 - transparency for, 43–44, 57–58
- cloud computing. *See also* cloud computing contracts; cloud service providers; data controllers; data processors; government cloud

- computing; United Kingdom; United States
- carbon footprint of, xi–xii
- concepts for, 9–14
- copyright laws and, 4
- during COVID-19 pandemic, xii
- critiques of, 8
- definitions in, 9–14
 - for services, 19–20
- deployment models, 23–25
 - community clouds, 24
 - hybrid clouds, 25
 - private clouds, 24
 - public clouds, 24–25
- environmental impact of, xi–xii
- historical development of, 3–4
- in information and communications technology, 3
 - outsourcing of, 4
- law of the parties applicable to, 159
- legal requirements for, 7–8
 - in contracts, 14–15
 - identification of, 15
 - limitations of, 15
 - theoretical approach to, 14–15
- long-term impact of, 8–9
- public debate over, xi–xii
- security issues for, 25–28
 - Confidentiality, Integrity, and Availability of data, 25–26
 - logical protections, 27
 - transparency in, 27
- subcontracting and, 120–22
- subprocessing and, 120–22
- cloud computing contracts, 159–60. *See also* service level agreements; standardization, of cloud computing contracts
 - applicable law for, 220–22
 - breach of, 209–11
 - call-off contracts, 171–77
 - characteristics of, 170–77
 - Cloud Legal Project, 159–60
 - compliance mechanisms, 233–37
 - confidentiality in, 196–203
 - discovery requirements and, 200–1
 - in Government Cloud system, 197–98
 - law enforcement access and, limitations on, 202–3
 - non-disclosure agreements, 196–98
 - in US, 198
 - contract damages, 209–11
 - consequential, 210–11
 - direct, 210, 213
 - limitations in sum, 217
 - liquidated, 214
 - UK approach to, 211–13, 214–17
 - US approach to, 213–17
- data portability, 226–32
 - data hostage clauses, 227
 - under General Data Protection Regulation, 228–30
 - in US states, variability between, 230–32
- Data Protection by Design and by Default obligations in, 176
- disclosure in, 196–203
 - discovery requirements and, 200–1
 - under Freedom of Information Acts, 198–200
 - LEA access and, limitations on, 202–3
 - non-disclosure agreements, 196–98
- elements of, 167–70
- European Commission guidelines on, 166
- European Data Protection Supervisor guidelines on, 176
- Force Majeure clauses, 207–9
 - definition of, 208–9
- framework agreements, 171–77
 - definition of, 172
 - for Government Cloud system, 174
 - for outsourcing, of information technology, 169
 - public contract requirements, 174–75
- functions of, 165–66
- jurisdiction of, 220–22
 - in EU, 221–22
- liability in, 203–7
 - exclusions from, 204–7
 - indemnity clauses, 206–7
 - limitations of, 204–7
 - warranties against, 204–6
- limits of, 165–66
- location of, 220–22
- master services agreement, 170–71
 - for outsourcing of information technology, 169
- metrics and measurements in, 177–86
- organization of, 170–77
- for outsourcing, of information technology, 168–70
 - in framework agreements, 169
 - in master service agreements, 169
 - multi-sourcing model, 169–70
 - in service level agreements, 169
 - single-sourcing model, 168–69
 - in statements of work, 169
- overview of, 195, 246–47
- partners in, 186–95
- privacy harms, 210
- public procurement structure for, in EU, 172–73

- cloud computing contracts (cont.)
 - Restatement (Second) of Contracts, 193–94, 214
 - standard terms
 - unilateral amendment of, 217–20
 - variation of, 217–20
 - statements of work, 177–78
 - for outsourcing of information technology, 169
 - subcontractors and, 186–95
 - back-to-back contracts, 187–88
 - in EU, 188–89
 - privity of contract doctrine, 191–95
 - in UK, with Government Cloud system, 189–90
 - in US, with Environmental Protection Agency, 190–91
 - termination of services, 222–26
 - in UK
 - case studies for, 232–37
 - compliance mechanisms, 233–37
 - contract damages in, 211–13, 214–17
 - under Freedom of Information Act, 234–37
 - Government Cloud system and, 189–90, 214–20, 233–37
 - subcontractors and, with Government Cloud system, 189–90
 - in US
 - case studies for, 232–37
 - compliance mechanisms, 233–37
 - confidentiality in, 198
 - contract damages in, 213–17
 - data portability in, state-to-state variability in, 230–32
 - Federal Risk and Authorization Management Program and, 214–20, 233–37
 - under Freedom of Information Act, 234–37
 - subcontractors and, with Environmental Protection Agency, 190–91
 - warranties and, 217
 - against liability, 204–6
- cloud consumers. *See* cloud clients
- cloud first strategy, in US, 56–57
- Cloud Legal Project (CLP), 159–60
- cloud service providers (CSPs). *See also* data controllers; data processors; data transfers; government cloud computing; *specific topics*
 - Computer Science Corporation and, 22
 - contract terms for, 6–7
 - data location with, 60–61
 - in EU, 62
 - in United States, 62
 - definition of, 11
 - Government as a Service, 23
 - government cloud computing and, 4–5, 6–7, 16–17
 - Infrastructure as a Service, 22–23
 - infrastructure of, 4–5
 - jurisdiction of, 42
 - under CLOUD Act, 80–84, 90
 - law enforcement access and, 75
 - liability for, 42
 - location of, 60–64
 - models for, 22–23
 - types of, 22–23
 - parties in, 20–22
 - cloud auditors, 20–21
 - cloud brokers/integrators, 21–22
 - Platform as a Service, 22–23
 - for small and medium-sized enterprises, 6–7
 - Software as a Service, 22–23
 - virtual machines and, 18–19
 - warranties for, 42
- cloudification, 52
- CLP. *See* Cloud Legal Project
- Coco Cloud. *See* Confidential and Compliant Clouds project
- Communications as a Service (CaaS), 23
- community clouds, 24
- compliance
 - in cloud computing contracts, 233–37
 - Microsoft* warrant case and, 77–80
 - in standardization of cloud computing contracts, 241–42
 - in US data privacy mechanisms, 152
- Computer Science Corporation (CSC), 22
- Confidential and Compliant Clouds project (Coco Cloud), xii
- confidentiality
 - in cloud computing contracts, 196–203
 - discovery requirements and, 200–1
 - in Government Cloud system, 197–98
 - law enforcement access and, limitations on, 202–3
 - non-disclosure agreements, 196–98
 - in US, 198
 - in data protection, in EU, 109
 - in US data privacy approach, 154
- Confidentiality, Integrity, and Availability of data (CIA), 25–26
- conflict of laws, 60
- consent, subcontracts and, 121–22
- consequential damages, 210–11
- contracts. *See also* cloud computing contracts
 - back-to-back, 187–88
 - blockchain, 248
 - Business-to-Business agreements, 14–15, 205
 - Business-to-Consumer agreements, 14–15

- Business-to-Government agreements, 14–15
- for data controllers, 113–17
 - designations for, 113–14
 - under Freedom of Information Act, 113–14
 - under General Data Protection Regulation, 114–17
 - obligations for, 114–17
 - subcontracts for, 120–22
- for government cloud computing, in US, 56
- legal frameworks for, 164–166
- principle of freedom for, 164
- privity of contract doctrine, 191–95
- smart, 248
- standard terms
 - for cloud service providers, 6–7
 - procurement requirements for, with outsourcing template, 48–49
 - transparency as element of, 43
- subcontracts, for data controllers and processors, 120–22
- in UK
 - under Freedom of Information Act, 163
 - Government Cloud system, 162
- US government, under Freedom of Information Act, 160–164, 162
- control, of data, 59. *See also* data sovereignty
- copyright laws, cloud computing and, 4
- Council of Europe's Convention, on data protection, 142–43
- Court of Justice of the European Union. *See also* *Schrems II*
 - cross-border data transfers and, 128–41
 - data controllers/processors and, in legal cases, 112–13
 - General Data Protection Regulation cases, 96, 97, 99
 - Schrems I*, 131–33
- COVID-19 pandemic, cloud computing during, xii
- cross-border data transfers. *See* data transfers
- CSC. *See* Computer Science Corporation
- CSPs. *See* cloud service providers
- DaaS. *See* Data as a Service
- damages, cloud computing contracts and, 209–11
 - consequential damages, 210–11
 - direct damages, 210, 213
 - limitations in sum, 217
 - liquidated damages, 214
- data access. *See* access
- Data as a Service (DaaS), 23
- data breaches, 3–4, 25–26, 42, 94, 117–19
 - determination of causation, 209
 - non-disclosure agreements and, 197
 - notification requirements, 148
- data controllers, data protection and, 110–27
 - contracts for, 113–17
 - designations for, 113–14
 - under Freedom of Information Act, 113–14
 - under General Data Protection Regulation, 114–17
 - obligations for, 114–17
 - controller-to-controller clauses, in standard contractual clauses, 133
 - in Court of Justice of the European Union cases, 112–13
- Data Protection by Design and by Default, 122–24
- qualifications for, 111–12
- subcontracting and, 120–22
 - consent in, 121–22
 - timing factors in, 122
- subprocessing and, 120–22
 - timing factors in, 122
- data hostage clauses, 227
- data location
 - with cloud service providers, 60–61
 - in EU, 62
 - in United Kingdom, 61
 - in United States, 62
 - of external data storage, 60–61
 - security of, 60–61
- data portability, 226–32
 - data hostage clauses, 227
 - under General Data Protection Regulation, 228–30
 - in US states, variability between, 230–32
- data privacy
 - data protection compared to, 12–13, 93
 - definition of, 12–13
 - in EU, 92–104
 - lack of control over, 3–4
 - theoretical approach to, 249–50
 - US approach to, 141–55
 - Carpenter v. US*, 146–48
 - compliance mechanisms in, 152
 - confidentiality aspects in, 154
 - constitutional privacy protections, 144–48
 - fair information principles in, 142–43
 - Federal Acquisition Regulation and, 153–54
 - in federal statutory law, 148–50
 - Federal Trade Commission and, 150–52
 - FedRAMP and, 152–54
 - in financial sector, 148
 - under Health Insurance Portability and Accountability Act of 1996, 148
 - under HITECH Act, 148
 - as individualistic, 142

- data privacy (cont.)
 - overview of, 154–55
 - under Privacy Act of 1974, 148–49
 - providing principles in, 148
 - Riley v. California*, 146
 - security aspects in, 154
 - state regulations in, variability in, 143
 - in Supreme Court cases, 146–48
 - under Videotape Privacy Protection Act, 149–50
- data processors, data protection and, 110–27
 - contracts and
 - under General Data Protection Regulation, 114–17
 - requirements for, 127
 - in Court of Justice of the European Union cases, 112–13
 - Data Protection by Design and by Default, 122–24
 - liability for, 117–19
 - under General Data Protection Regulation, 118–19
 - requirements for, 127
 - obligations for, 117–19, 126–27
 - for audits, 119–20
 - in EU, 120
 - in UK, 119–20
 - qualifications for, 111–12
 - subcontracting and, 120–22
 - consent in, 121–22
 - timing factors in, 122
 - subprocessing and, 120–22
 - timing factors in, 122
- data protection, in EU, 92–104. *See also* data controllers; data processors; General Data Protection Regulation
 - accountability principle and, 110
 - accuracy in, 108
 - authorities for, 10
 - under Charter of Fundamental Rights of the European Union, 92
 - confidentiality in, 109
 - Council of Europe's Convention on, 142–43
 - data minimization and, 108
 - data privacy compared to, 12–13, 93
 - data quality and, 105–10
 - processing requirements, 106
 - purpose limitation principle and, 106–8
 - EU Data Protection Board, 9–10, 83–84, 94, 103–4
 - under EU Data Protection Directive, 9–10
 - European Commission guidelines on, 91
 - under European Convention on Human Rights, 92
 - under European Data Protection Board, 9–10
 - fairness in, 106
 - under General Data Protection Regulation, 155–56
 - of personal data, 104–5
 - pseudonymization and, 109
 - storage limitations, 108–9
 - in territories outside EU, 102–4
 - theoretical approach to, 249–50
 - transparency in, 106
- Data Protection as a Service (DPaaS), 23
- data protection authorities (DPAs), 10
- Data Protection by Design and by Default (DPbD), 122–24, 176
- Data Protection v Facebook*. *See* *Schrems II*
- data residency, 35
- data security, 12. *See also* data protection
 - data privacy law and, 124–26
 - General Data Protection Regulation and, 124–26
- data sovereignty
 - data residency compared to, 35
 - definition of, 12, 36
 - in government cloud computing, 42, 58
 - barriers to cloud and, 35–36
 - state sovereignty and, 63–64
- data storage
 - data protection and, storage limitations, 108–9
 - data shard in, 78
 - external, 60–61
 - in US government cloud computing, 55
- data transfers, cross-border, 127–41
 - adequacy determinations for, 129–32, 136–37
 - binding corporate rules for, 134
 - in Court of Justice of the European Union cases, 128–41
 - definition of, 128–29
 - derogations, 140–41
 - encryption in, 139
 - EU Data Protection Board guidance on, 139–40
 - European Commission and, 129–32, 133–34
 - European Data Protection Supervisor and, 128–29
 - means of, 129–32
 - Privacy Shield Framework, 132–33, 136–37
 - Safe Harbour Framework for, 131
 - Privacy Shield Framework and, 132–33
 - Schrems II* and, 140
 - Schrems I*, 131–33
 - Schrems II*, 134–40
 - legal legacy of, 141
 - Safe Harbour Framework and, 140
 - standard contractual clauses after, 135–40
 - standard contractual clauses and, 133–34
 - controller-to-controller clauses, 133

- after *Schrems II*, 135–40
 - standard processes for, 127–28
 - in US, 130–31
- derogations, cross-border data transfers and, 140–41
- direct damages, 210, 213
- disclosure, in cloud computing contracts, 196–203
 - discovery requirements and, 200–1
 - under Freedom of Information Acts, 198–200
 - LEA access and, limitations on, 202–3
 - non-disclosure agreements, 196–98
- DPaaS. *See* Data Protection as a Service
- DPAs. *See* data protection authorities
- DPbD. *See* Data Protection by Design and by Default
- EBA. *See* European Banking Authority
- EC. *See* European Commission
- EDPB. *See* EU Data Protection Board
- EDPS. *See* European Data Protection Supervisor
- effects principle, 104
- EIOPA. *See* European Insurance and Occupational Pensions Authority
- encryption, in cross-border data transfers, 139
- enforcement jurisdiction, 70
- environmental issues. *See also* green computing
 - carbon footprints, of cloud computing, xi–xii
 - cloud computing's impact on, xi–xii
- Environmental Protection Agency (EPA), 181–82, 190–91
- Equinor, in Norway, 39–40
- EU. *See* European Union
- EU Data Protection Board (EDPB), 9–10, 83–84, 94, 103–4, 116–17
 - on cross-border data transfers, 139–40
- EU Data Protection Directive, Article 29 (WP29), 9–10
- European Banking Authority (EBA), 120
- European Commission (EC)
 - on cross-border data transfers, 129–32, 133–34
 - data protection guidelines, 91
- European Convention on Human Rights, 92
- European Data Protection Supervisor (EDPS), 83–84, 128–29
- European Insurance and Occupational Pensions Authority (EIOPA), 120
- European Union (EU). *See also* data protection; European Commission; General Data Protection Regulation; United Kingdom Charter of Fundamental Rights of the European Union, 92
 - cloud computing contracts in, jurisdiction of, 221–22
 - Confidential and Compliant Clouds project, xii
 - data location in, for cloud service providers, 62
 - data privacy in, 92–104
 - data processor obligations in, 120
 - EU Data Protection Board, 9–10, 83–84, 94, 103–4, 116–17
 - on cross-border data transfers, 139–40
 - EU Data Protection Directive, Article 29, 9–10
 - European Data Protection Supervisor, 83–84, 128–29
 - Free Software Foundation Europe, 16
 - government cloud computing in, 50–53
 - adoption strategies for, 51
 - marketplace and procurement model, 51–52
 - procurement requirements, 47–48
 - resource pooling model, 52–53
 - standalone applications for, 53
 - Human Brain Project, xii
 - service level agreements in, regulation mechanisms for, 185–186
 - Treaty on the Functioning of the European Union, 33
- Everything as a Service (XaaS), 23
- Executive Order 12333, data access under, 85–86
- extraterritorial application, of jurisdiction, 71–73
- FAA. *See* Federal Aviation Administration
- fair information principles (FIPs), 142–43
- FAR. *See* Federal Acquisition Regulation
- FCA. *See* Financial Conduct Authority
- FDA. *See* Food and Drug Administration
- Federal Acquisition Regulation (FAR), US, 153–54
- Federal Aviation Administration (FAA), 183–185, 184
- Federal Risk and Authorization Management Program (FedRAMP), 7–8, 34–35, 56–57, 152–54, 190–91
 - cloud computing contracts and, 214–20, 233–37
 - standardization of, 238–39
- Federal Trade Commission (FTC), 150–52
- FedRAMP. *See* Federal Risk and Authorization Management Program
- Financial Conduct Authority (FCA), 119–20
- FIPs. *See* fair information principles
- FISA. *See* Foreign Intelligence Surveillance Act
- flexibility, in standardization of cloud computing contracts, 243
- FOI. *See* Freedom of Information
- FOIA. *See* Freedom of Information Act; UK Freedom of Information Act
- Food and Drug Administration (FDA), 182
- Force Majeure clauses, 207–9
 - definition of, 208–9
- Foreign Intelligence Surveillance Act, US (1978) (FISA), 85–86

- framework agreements, 171–77
 - in cloud computing contracts, 169
 - definition of, 172
 - for Government Cloud system, 174
 - for outsourcing, of information technology, 169
 - Privacy Shield Framework, 132–33, 136–37
 - public contract requirements, 174–75
 - Safe Harbour Framework, 131
 - Privacy Shield Framework and, 132–33
 - Schrems II* and, 140
- Free Software Foundation Europe, 16
- Freedom of Information (FOI)
 - under Government Cloud system, 162
 - in UK, 163
- Freedom of Information Act, US (FOIA)
 - agreements under, xii, 7–8
 - data controller contracts under, 113–14
 - disclosure requirements under, 198–200
 - disclosure under, 198–200
 - service level agreements under, 182–83
- FTC. *See* Federal Trade Commission
- GaaS. *See* Government as a Service
- G-Cloud system. *See* Government Cloud system
- General Data Protection Regulation (GDPR), EU,
 - 9–10, 83, 91–92, 93–94
 - application of, 95–104
 - in Court of Justice of the European Union cases, 96, 97, 99
 - data controller contracts and, 114–17
 - data portability under, 228–30
 - data processor liability under, 118–19
 - data protection under, 155–56
 - effects principle, 104
 - jurisdiction of, 100
 - material scope of, 95–104
 - principle of territoriality, 102–4
 - pseudonymization, 99
- GovCloud, 24
- Government as a Service (GaaS), 23
- government cloud computing, 4–7. *See also*
 - United Kingdom; United States
- adoption of, 16–17, 33–34
- assumptions about, 16–17
- budget requests for, 4
- cloud barriers to, 47–50
- as cloud client, 42–46
 - accessibility and, 45–46
 - accountability in, 44–45, 57–58
 - availability and, 45–46
 - legitimacy and, 45, 57–58
 - loss of competence and, 46
 - transparency for, 43–44, 57–58
- cloud service providers and, 4–5, 6–7, 16–17
- cloudification, 52
- community clouds, 24
 - Government Cloud system, 24
- data sovereignty in, 42, 58
 - barriers to cloud and, 35–36
- in EU, 50–53
 - adoption strategies for, 51
 - marketplace and procurement model, 51–52
 - procurement requirements, 47–48
 - resource pooling model, 52–53
 - standalone applications for, 53
- Free Software Foundation Europe campaign
 - for, 16
- Freedom of Information Act requirements in,
 - 33–34
 - under Treaty on the Functioning of the European Union, 33
- information and communications technology
 - outsourcing, 4
- Intelligence Community Information
 - Enterprise, 31–32
- long-term issues with, 16–17
- markets for, government influences on, 9
- outsourcing for, 33, 37–42
 - information and communications technology and, 4
 - in Norway, 37–40
 - State of Indiana v. IBM*, 40–42
 - in Sweden, 38
- in private markets, 42–46
- procurement requirements, 47–50
 - data location barriers, 49–50
 - in EU, 47–48
 - price comparisons, 47–48
 - standard contracts, with outsourcing template, 48–49
- risk factors for, 5–6
- state clouds, 37–42
- theoretical approach to, 31–35
- in UK, 53–55
 - for public sector organizations, 54
- in US, 55–57
 - cloud first strategy, 56–57
 - contract terms for, negotiation of, 56
 - data storage systems and, 55
 - legacy systems for, 55–56
- Government Cloud system (G-Cloud system), in
 - UK, 7–8, 34–35, 54–55
- access to data for, limitations on, 24
- in cloud computing contracts, 189–90, 214–20, 233–37
- cloud computing contracts and, confidentiality
 - in, 197–98
- community clouds, 24

framework agreements and, 174
 Freedom of Information under, 162
 governments. *See also* Norway; Sweden; United Kingdom; United States
 definition of, 13
 sovereignty of, data sovereignty and, 63–64
 green computing, xi

Hammond, Philip, 72–73
 HBP. *See* Human Brain Project
 Health Insurance Portability and Accountability Act of 1996 (HIPAA), US, 148
 Health South-East, in Norway, 37–38
 HIPAA. *See* Health Insurance Portability and Accountability Act of 1996
 HITECH Act, US, 148
 Human Brain Project (HBP), xii
 hybrid clouds, 25

IaaS. *See* Infrastructure as a Service
 ICITE. *See* Intelligence Community Information Enterprise
 indemnity clauses, 206–7
 India, government cloud computing outsourced to, 39–40
 information and communications technology (ITC)
 government uses of
 budget requests for, 4
 outsourcing and, 3
 outsourcing for, 3
 by governments, 4
 information security, 12
 Infrastructure as a Service (IaaS), 22–23, 193
 Intelligence Community Information Enterprise (ICITE), 31–32
 international law. *See* private international law; public international law
 Internet, jurisdiction on, 64–71
 investigative jurisdiction, 70–71
 ITC. *See* information and communications technology

Joint Enterprise Defense Infrastructure contract (JEDI contract), 252
 judicial jurisdiction, 69–70
 jurisdiction. *See also* Microsoft warrant case
 assertion of, on Internet, 64–71
 under CLOUD Act
 for cloud service providers, 80–84, 90
 in Microsoft warrant case, 76–77
 mutual legal assistance treaties and, 81, 83
 of cloud computing contracts, 220–22
 of cloud service providers, 42

 under CLOUD Act, 80–84, 90
 conflict of laws and, 60
 definition of, 60, 64–65
 enforcement, 70
 extraterritorial application of, 71–73
 of General Data Protection Regulation, 100
 investigative, 70–71
 judicial, 69–70
 law enforcement access and, 74–75
 cloud service providers and, 75
 mutual legal assistance treaties, 74–75
 mutual legal assistance treaties
 under CLOUD Act, 81, 83
 law enforcement access and, 74–75
 in Microsoft warrant case, 76
 personal, 60
 personality principle and, 67
 prescriptive, 60, 68–69
 in private international law, 67–68
 protective principle and, 67
 in public international law, 67–68
 state sovereignty and, 64–65
 territoriality principle and, 66, 71–73

law enforcement, data access and, 3–4
 law enforcement access (LEA), 74–75
 under cloud computing contracts, limitations on, 202–3
 cloud service providers and, 75
 mutual legal assistance treaties, 74–75
 legitimacy, of government cloud computing, 45, 57–58

liability
 in cloud computing contracts, 203–7
 exclusions from, 204–7
 indemnity clauses, 206–7
 limitations of, 204–7
 warranties against, 204–6
 for cloud service providers, 42
 liquidated damages, 214
 location. *See also* data location; jurisdiction
 cloud computing contracts and, 220–22
 of cloud service providers, 60–64
 Lynch, Gerard E., 79

MaaS. *See* Monitoring as a Service
 marketplace and procurement model, for government cloud computing, 51–52
 master services agreement (MSA), 41, 169, 170–71
 McNealy, Scott, 250
 Microsoft warrant case, 75–80
 appeals for, 76–77
 under CLOUD Act, 76–77
 compliance issues in, 77–80

- Microsoft warrant case (cont.)
 Microsoft services in, 77–80
 mutual legal assistance treaties and, 76
 under Stored Communications Act, 76–77
 minimization of data, 108
 MLATs. *See* mutual legal assistance treaties
 Monitoring as a Service (MaaS), 23
 MSA. *See* master services agreement
 mutual legal assistance treaties (MLATs)
 under CLOUD Act, 81, 83
 law enforcement access and, 74–75
 in *Microsoft* warrant case, 76
- NaaS. *See* Network as a Service
 NDAs. *See* non-disclosure agreement; non-disclosure agreements
 Network as a Service (NaaS), 23
 non-disclosure agreements (NDAs), 196–98
 data breaches and, 197
 Norway, government cloud computing in, outsourcing for, 37–40
 for critical infrastructure, 39–40
 Equinor, 39–40
 Health South-East, 37–38
 to India, 39–40
- offshoring, definition of, 13–14
 outsourcing
 in cloud computing contracts, 168–70
 in framework agreements, 169
 in master services agreement, 169
 multi-sourcing model, 169–70
 in service level agreements, 169
 single-sourcing model, 168–69
 in statements of work, 169
 definition of, 13–14
 for government cloud computing, 33, 37–42
 information and communications technology and, 4
 in Norway, 37–40
State of Indiana v. IBM, 40–42
 in Sweden, 38
 for information and communications technology, 3
 by governments, 4
- PaaS. *See* Platform as a Service
 personal jurisdiction, 60
 personality principle, 67
 Platform as a Service (PaaS), 22–23
 prescriptive jurisdiction, 60, 68–69
 principle of freedom, in contracts, 164
 PRISM program, 86–88
 privacy. *See also* data privacy
 in cloud computing contracts, 210
 in Data Protection by Design and by Default, 122–24
 Privacy Act of 1974, US, 148–49
 Privacy Shield Framework, 132–33, 136–37
 private clouds, 24
 private international law, jurisdiction of, 67–68
 private sector
 government cloud computing in, 42–46
 public embrace of, 18
 privacy of contract doctrine, 191–95
 procurement
 in cloud computing contracts, structure for, in EU, 172–73
 marketplace and procurement model, 51–52
 in standard contract terms, 48–49
 theoretical approach to, 251
 protection. *See* data protection
 protective principle, 67
 providing principles, in data privacy, 148
 pseudonymization, 99, 109
 public clouds, 24–25
 in UK, 54
 public international law, jurisdiction of, 67–68
 public sector
 public embrace of, 18
 in United Kingdom, government cloud computing in, 54
 purpose limitation principle, 106–8
- Re Warrant to Search a Certain Email Account Controlled & Maintained by Microsoft Corporation*, 59–60
 resource pooling model, for government cloud computing, 52–53
 Restatement (Second) of Contracts, 193–94, 214
Riley v. California, 146
- SaaS. *See* Software as a Service
 Safe Harbour Framework, 131
 Privacy Shield Framework and, 132–33
Schrems II and, 140
 SCCs. *See* standard contractual clauses
 Schrems, Maximilian, 131–33, 134–40
Schrems I, 131–33
Schrems II (Data Protection v Facebook), 134–40
 legal legacy of, 141
 Safe Harbour Framework and, 140
 standard contractual clauses after, 135–40
 SECaaS. *See* Security as a Service
 security. *See also* data security; information security
 for cloud computing, 25–28

- Confidentiality, Integrity, and Availability of
 - data, 25–26
 - logical protections, 27
 - transparency in, 27
- data location and, 60–61
- transparency and, 43
- Security as a Service (SECaaS), 23
- security services, data access and, 3–4
- service level agreements (SLAs), 178–86
 - in cloud computing contracts, 169
 - components of, 178–79
 - definition of, 178
 - in EU, regulation mechanisms for, 185–186
 - exception from uptime guarantees, 180–81
 - exclusions in, 179
 - functions of, 179–80
 - importance of, in cloud computing, 179–185
 - for outsourcing of information technology, 169
 - transparency of, 43
 - in UK, 186
 - in US government contracts, 181–185
 - with Environmental Protection Agency, 181–82
 - for Federal Aviation Administration, 183–185, 184
 - for Food and Drug Administration, 182
 - under Freedom of Information Act, 182–83
- SGSA. *See* Supply of Goods and Services Act
- SLA. *See* service level agreement
- small and medium-sized enterprises (SMEs),
 - cloud service providers for, 6–7
- smart contracts, 248
- SMEs. *See* small and medium-sized enterprises
- Snowden, Edward, 72
- Software as a Service (SaaS), 22–23, 48, 178, 193
- sovereignty. *See also* data sovereignty
 - jurisdiction and, 64–65
- SOWs. *See* statements of work
- standard contract terms
 - in cloud computing contracts
 - unilateral amendment of, 217–20
 - variation of, 217–20
 - for cloud service providers, 6–7
 - for government cloud computing, with outsourcing template, 48–49
 - for legal requirements, incorporation of, 239–40
 - transparency as element of, 43
- standard contractual clauses (SCCs), 133–34
 - controller-to-controller clauses, 133
 - after *Schrems II*, 135–40
- standardization, of cloud computing contracts,
 - 237–45
 - audits, 243–44
 - compliance requirements for, 241–42
 - core requirements for, 240–41
 - flexibility in, 243
 - inventories, 243–44
 - of legal requirements, 237–39
 - incorporation of, through standard terms, 239–40
 - monitoring mechanisms, 243–44
 - policy objectives as contract element in, 244–45
- state clouds, 37–42
- State of Indiana v. IBM*, 40–42, 207–8
- statements of work (SOWs), 169, 177–78
- states, definition of, 13. *See also* governments
- Stored Communications Act, US, 76–77
- subcontractors, in cloud computing contracts,
 - 186–95
 - back-to-back contracts, 187–88
 - in EU, 188–89
 - privity of contract doctrine, 191–95
 - in UK, with Government Cloud system, 189–90
 - in US, with Environmental Protection Agency, 190–91
- subcontracts, for data controllers and processors,
 - 120–22
 - consent in, 121–22
 - timing factors in, 122
- subprocessing, for data controllers and processors,
 - 120–22
 - timing factors in, 122
- Supply of Goods and Services Act (SGSA),
 - UK, 186
- Sweden, government cloud computing in, 38
- termination of services, in cloud computing contracts, 222–26
- territoriality principle
 - in General Data Protection Regulation, 102–4
 - jurisdiction and, 66, 71–73
- transparency
 - in audits, 43
 - in cloud computing security, 27
 - in data protection, 106
 - in government cloud computing, 43–44, 57–58
 - security and, 43
 - of service level agreements, 43
 - in standard contracts, 43
- Treaty on the Functioning of the European Union, 33
- UK. *See* United Kingdom
- UK Freedom of Information Act (UK FOIA),
 - 7–8
 - disclosure requirements under, 198–200
 - government cloud computing requirements under, 33–34

- UK Freedom of Information Act (cont.)
 - under Treaty on the Functioning of the European Union, 33
- United Kingdom (UK). *See also* cloud computing contracts; Government Cloud system
 - Business-to-Business agreements in, 14–15, 205
 - data location in, 61
 - data processor obligations in, 119–20
 - Financial Conduct Authority, 119–20
 - Freedom of Information Act, 7–8
 - disclosure requirements under, 198–200
 - disclosure under, 198–200
 - government cloud computing requirements under, 33–34
 - under Treaty on the Functioning of the European Union, 33
 - government cloud computing in, 7–8, 53–55
 - for public sector organizations, 54
 - service level agreements in, 186
 - Supply of Goods and Services Act, 186
- United States (US). *See also* cloud computing contracts; data privacy
 - CLOUD Act
 - for cloud service providers, 80–84, 90
 - in *Microsoft* warrant case, 76–77
 - mutual legal assistance treaties and, 81, 83
 - cross-border data transfers in, 130–31
 - data location in, with cloud service providers, 62
 - data protection in, data protection authorities, 10
 - Environmental Protection Agency, 181–82, 190–91
 - Executive Order 123333, data access under, 85–86
 - Federal Acquisition Regulation in, 153–54
 - Federal Risk and Authorization Management Program, 7–8, 34–35, 56–57, 152–54, 190–91
 - cloud computing contracts and, 214–20, 233–37
 - Federal Trade Commission, 150–52
 - Foreign Intelligence Surveillance Act, 85–86
 - Freedom of Information Act, xii, 7–8
 - data controller contracts under, 113–14
 - disclosure requirements under, 198–200
 - service level agreements under, 182–83
 - GovCloud access limitations, 24
 - government cloud computing in, 7–8, 55–57
 - cloud first strategy, 56–57
 - contract terms for, negotiation of, 56
 - data storage systems and, 55
 - legacy systems for, 55–56
 - Health Insurance Portability and Accountability Act of 1996, 148
 - HITECH Act, 148
 - Privacy Act of 1974, 148–49
 - Re Warrant to Search a Certain Email Account Controlled & Maintained by Microsoft Corporation*, 59–60
 - service level agreements, in government contracts, 181–185
 - with Environmental Protection Agency, 181–82
 - for Federal Aviation Administration, 183–185, 184
 - for Food and Drug Administration, 182
 - under Freedom of Information Act, 182–83
 - Stored Communications Act, 76–77
 - Videotape Privacy Protection Act, 149–50
 - UPSTREAM program, 87–88
 - US. *See* United States
- Videotape Privacy Protection Act (VPPA), US (1988), 149–50
- virtual machines (VMs), cloud service providers and, 18–19
- VPPA. *See* Videotape Privacy Protection Act
- warranties
 - in cloud computing contracts, against liability, 204–6
 - for cloud service providers, 42
- warrants. *See* *Microsoft* warrant case
- WP29. *See* EU Data Protection Directive
- XaaS. *See* Everything as a Service