Table of Contents

PART I. CLOUD COMPUTING BASICS

CHAPTER 1. AN INTRODUCTION TO ENTERPRISE CLOUD COMPUTING
§ 1:1 Cloud computing defined
§ 1:2 Enterprise cloud computing basics, benefits, and challenges
§ 1:3 Understanding the implications of “multi-tenancy”

CHAPTER 2. PERSONAL CLOUD COMPUTING
§ 2:1 In general
§ 2:2 Understanding the business models
§ 2:3 Getting into the personal cloud computing business
§ 2:4 Multiplatform development
§ 2:5 App distribution
§ 2:6 Hosting and back-end services
§ 2:7 Gaining consumer trust
§ 2:8 Adopting a privacy policy
§ 2:9 Maintaining security
§ 2:10 Terms of service

CHAPTER 3. NEGOTIATING CLOUD CONTRACTS
§ 3:1 In general
§ 3:2 Warranties
§ 3:3 “Click-through” agreements and the opportunity to negotiate
§ 3:4 Performance requirements
§ 3:5 Information to be protected
§ 3:6 Disaster planning and force majeure
§ 3:7 Interoperability
§ 3:8 Liability; indemnification; insurance
§ 3:9 Audit rights
§ 3:10 Termination and transition
CHAPTER 4. CLOUD CYBERSECURITY

I. INTRODUCTION

§ 4:1 In General
§ 4:2 Cybercrime
§ 4:3 Anatomy of a typical cyberattack
§ 4:4 Cyber threat trends

II. LEGAL REQUIREMENTS

§ 4:5 In general
§ 4:6 Federal requirements for cybersecurity
§ 4:7 Privacy statutes
§ 4:8 Other legal notice and reporting requirements and protections
§ 4:9 The Cybersecurity Act of 2015
§ 4:10 SAFETY Act
§ 4:11 State law, generally

III. PREPARING FOR A DATA BREACH

§ 4:12 In general
§ 4:13 Cybersecurity governance
§ 4:14 Information Security Incident Response Plan
§ 4:15 Assessing incident response readiness
§ 4:16 Cyber insurance

IV. RESPONDING TO A DATA BREACH

§ 4:17 Quick reference guide for the first 30 minutes

CHAPTER 5. U.S. EXPORT AND SANCTIONS REGULATIONS AND THE CLOUD

I. GENERAL CONSIDERATIONS

§ 5:1 In general
§ 5:2 Liability—The knowledge standard

II. ARMS EXPORT CONTROL ACT (AECA) AND INTERNATIONAL TRAFFIC IN ARMS REGULATIONS (ITAR)

§ 5:3 In general
TABLE OF CONTENTS

§ 5:4 Defense articles
§ 5:5 Exempt data
§ 5:6 Defense services
§ 5:7 Brokering provisions
§ 5:8 Enforcement and penalties

III. EXPORT ADMINISTRATION REGULATIONS (EAR)

§ 5:9 In general
§ 5:10 U.S.-origin goods
§ 5:11 “Deemed” exports
§ 5:12 Exempt software and services
§ 5:13 Agency guidance
§ 5:14 Enforcement and potential penalties

IV. ECONOMIC SANCTIONS REGULATIONS

§ 5:15 In general
§ 5:16 Exemptions
§ 5:17 Agency guidance
§ 5:18 Enforcement and potential penalties

V. E.U. AND OTHER FOREIGN EXPORT CONTROL LAWS

§ 5:19 Potential impact
§ 5:20 Economic sanctions

VI. COMPLIANCE ISSUES

§ 5:21 Compliance strategies
§ 5:22 Export control reform

PART II. CLOUD COMPUTING ISSUES FOR INDUSTRY

CHAPTER 6. INTELLECTUAL PROPERTY ISSUES

§ 6:1 In general
§ 6:2 Patent procurement considerations
§ 6:3 —Requirements of novelty and non-obviousness
§ 6:4 —Patentable subject matter
§ 6:5 Patent claim drafting strategies
§ 6:6 —Claims that read on direct infringers
§ 6:7 —Claims for which infringement is detectable
§ 6:8 —Claims that will be infringed in the patent territory
§ 6:9 —Claims that capture commercial value
§ 6:10 —Other patent filing considerations
§ 6:11 Litigation trends
§ 6:12 Trade secrets
§ 6:13 —Securing trade secrets in the cloud
§ 6:14 Trademark
§ 6:15 Copyright

CHAPTER 7. OPEN SOURCE ISSUES
§ 7:1 In general
§ 7:2 Legal issues with open source
§ 7:3 Tainting of proprietary software
§ 7:4 Patent grant provisions
§ 7:5 Patent non-assert provisions
§ 7:6 Assumption of legal obligations
§ 7:7 License incompatibility
§ 7:8 Compliance obligations
§ 7:9 Distribution
§ 7:10 Cloud-specific open source issues
§ 7:11 Developing corporate open source policies

CHAPTER 8. CONSTITUTIONAL PROTECTIONS OF PRIVACY IN THE CLOUD
§ 8:1 In general
§ 8:2 Stanley v. Georgia
§ 8:3 Limitations of Stanley v. Georgia
§ 8:4 Katz v. United States and the Fourth Amendment
§ 8:5 Limitations of Stanley v. Georgia and Katz v. United States
§ 8:6 Klayman v. Obama
§ 8:7 Recent “Playpen” cases, The Onion Router (TOR) Network, and privacy considerations for hidden IP addresses
§ 8:8 Jurisdictional considerations, extraterritoriality considerations, and recent cases

CHAPTER 9. EMPLOYMENT ISSUES IN THE CLOUD
§ 9:1 Employment from, in, and through the cloud
§ 9:2 Specific issues concerning the laws that apply to remote workers
§ 9:3 Protecting confidentiality and trade secrets

xx
CHAPTER 10. CRIMINAL LIABILITY
§ 10:1 In general
§ 10:2 Categories of activity garnering criminal liability
§ 10:3 —Unauthorized access and data protection
§ 10:4 —Tampering with or destruction of computer equipment
§ 10:5 —Computer fraud and theft
§ 10:6 —Other areas of criminal liability
§ 10:7 ——Unauthorized use of encryption
§ 10:8 ——Protection against spyware
§ 10:9 ——Protection of personal information and privacy
§ 10:10 State law penalties
§ 10:11 Federal penalties

CHAPTER 11. GENERAL GOVERNMENT CONTRACTING ISSUES IN THE CLOUD
§ 11:1 Federal Cloud Computing Strategy—Overview
§ 11:2 —Initial implementation
§ 11:3 Federal cloud computing strategy—First-generation challenges to government cloud migration efforts
§ 11:4 Federal Cloud Computing Strategy—Second-generation challenges to government cloud migration efforts
§ 11:5 Federal cloud acquisition strategies
§ 11:6 —Potential issues—Navigating the regulatory labyrinth
§ 11:7 ——Measured service
§ 11:8 ——Service level agreements (SLAs)
§ 11:9 ——Cloud terms of service (TOS) and end user license agreements (EULAs)
§ 11:10 Federal cloud computing strategy—Third-generation challenges being faced by the U.S. Department of Defense
§ 11:11 Federal cloud security
§ 11:12 —Regulations for contractors
§ 11:13 —Liability for data breach and data loss
§ 11:14 Cyber insurance for government contractors

CHAPTER 12. IP RISKS FOR GOVERNMENT USERS AND CONTRACTORS
§ 12:1 IP ownership and license rights in government contracts, generally
§ 12:2 Copyright liability
§ 12:3 Patent infringement
§ 12:4 Standard commercial license protections
§ 12:5 Patent and copyright authorization and consent
§ 12:6 Invasions of privacy
§ 12:7 Potential liability for invasions of privacy—Potential “government contractor defense”
§ 12:8 Risks—Changing government demands
§ 12:9 —Improper access and use of data
§ 12:10 —Minimizing the risk to intellectual property

CHAPTER 13. GSA PROCUREMENT AND FEDRAMP STANDARDIZATION
§ 13:1 “Cloud First” Policy and agency transition to the cloud
§ 13:2 Migrating to the cloud—NIST definitions and types of cloud services
§ 13:3 GSA purchasing vehicles
§ 13:4 GSA rules applicable to cloud contracts
§ 13:5 Data security and FedRAMP standardization
§ 13:6 FedRAMP—“Paths” available to CSPs
§ 13:7 —Security Assessment Framework
§ 13:8 —Third party assessment organizations
§ 13:9 —Beyond the FedRAMP moderate baseline
§ 13:10 —Agency purchasers
§ 13:11 State purchasers

PART III. CONCERNS AND CONSIDERATIONS UNIQUE TO CLOUD COMPUTING

CHAPTER 14. FEDERAL CLOUD PROCUREMENT DISPUTES, OR “BID PROTESTS”
§ 14:1 In general
§ 14:2 Types of challenges
§ 14:3 Tribunals
§ 14:4 When to file
§ 14:5 Pre-award issues
§ 14:6 Post-award issues
§ 14:7 Standard GAO timeline
§ 14:8 Decisions in cloud computing cases
CHAPTER 15. VIRTUAL JURISDICTION: CLOUD COMPUTING AND PERSONAL JURISDICTION
§ 15:1 Personal jurisdiction, generally
§ 15:2 General jurisdiction
§ 15:3 Specific jurisdiction
§ 15:4 Statutory exceptions
§ 15:5 Jurisdiction over electronic communications
§ 15:6 Jurisdiction over websites
§ 15:7 Jurisdiction over entities operating social networking sites
§ 15:8 Jurisdiction and business considerations

CHAPTER 16. LITIGATION CONSIDERATIONS: E-DISCOVERY
§ 16:1 Scope of discovery
§ 16:2 Electronically stored information (ESI)
§ 16:3 Duty to preserve information
§ 16:4 Duty to produce information
§ 16:5 “Control, not location” determines discovery obligation
§ 16:6 Safeguards for privileged or confidential information
§ 16:7 Cloud computing as a discovery tool

CHAPTER 17. ATTORNEY-CLIENT PRIVILEGE AND RELATED DUTIES
§ 17:1 In general
§ 17:2 Waiver and breach of the attorney-client privilege
§ 17:3 Reasonable precautions required
§ 17:4 Best practice tip: Review security protections

CHAPTER 18. CLOUD PAYMENT/BANKING CONSIDERATIONS
§ 18:1 In general
§ 18:2 Cloud-based financial technology
§ 18:3 Regulation and consumer finance laws
§ 18:4 Regulators and regulations
§ 18:5 Regulator—Federal Financial Institutions Examination Council (FFIEC)
§ 18:6 —Federal Trade Commission (FTC)
§ 18:7 —Consumer Financial Protection Bureau
§ 18:8 —Federal Deposit Insurance Corporation (FDIC) and National Credit Union Association (NCUA) Insurance
§ 18:9 —Financial Industry Regulatory Authority (FINRA)
§ 18:10 Regulation—Electronic Funds Transfer Act (EFTA)
§ 18:11 —Truth in Lending Act (TILA) and Truth in Savings Act (TISA)
§ 18:12 —Gramm-Leach-Bliley Act (GLBA)
§ 18:13 Data privacy and security compliance

CHAPTER 19. MERGERS AND ACQUISITIONS IN CLOUD COMPUTING
§ 19:1 Merger and acquisition drivers
§ 19:2 Provisions in merger and acquisition agreements
§ 19:3 IP representations and warranties
§ 19:4 Due diligence, selected topics

CHAPTER 20. LOSS OF DATA ISSUES AND REMEDIES FOR DATA LOSS

I. TYPES OF DATA LOSS
§ 20:1 In general
§ 20:2 Inaccessibility that prevents a user from retrieving data
§ 20:3 Loss or theft that results in unauthorized use
§ 20:4 Inadvertent disclosure of private data
§ 20:5 Unauthorized access to private data

II. THEORIES OF RELIEF
§ 20:6 Federal law, generally
§ 20:7 Stored Communications Act
§ 20:8 FTC enforcement actions
§ 20:9 State law, generally
§ 20:10 Deceptive business practices
§ 20:11 Security breach notification laws
§ 20:12 Common-law breach of contract
§ 20:13 Common-law negligence
§ 20:14 Shareholder derivative actions
§ 20:15 Class action issues
§ 20:16 Standing

III. REMEDIES FOR DATA LOSS
§ 20:17 Monetary relief
§ 20:18 —Damages
§ 20:19 —Restitution
Table of Contents

§ 20:20 Injunctive relief
§ 20:21 Evolving legal landscape
§ 20:22 Best practices to avoid and/or mitigate harm caused by data breach events

Appendix

Appendix A. State Statutes Applicable to Information Security and Privacy

Table of Laws and Rules
Table of Cases
Index