

TABLE OF CONTENTS

CHAPTER 1

The Constitutional Right to Privacy, U.S. Federal Privacy Legislation, and Government and Private Access to Personal Information

§ 1.01	Introduction	1-4
§ 1.02	Constitutional Considerations	1-6
	[1] The Amendments	1-6
	[2] The Constitutional Right of Privacy	1-7
	[a] Searches and Seizures	1-8
	[i] Fourth Amendment Protection for Information	1-9
	[ii] State Constitutional Protection for Information	1-12
	[b] Zones of Privacy	1-12
	[3] Key Cases Federal Court Cases Addressing the Constitutional Right of Privacy	1-14
	[4] State Constitutions	1-16.3
	[a] State Constitutional Protection of Information	1-16.5
	[i] Cell Phone Location Data	1-16.7
§ 1.03	Privacy Laws That Impact Access to and Use of Personal Information by the Government	1-16.8
	[1] Federal Wiretap Statute	1-16.8
	[a] Prohibitions Against the Interception, Use or Disclosure of Oral, Wire and Electronic Communications	1-16.8
	[b] Exceptions	1-17
	[i] 18 U.S.C. Section 2518 Court Order or “Wiretap Order”	1-17

PRIVACY LAW

	[ii] Consent	1-21
	[iii] Inadvertently Obtained Criminal Evidence	1-21
	[iv] Subcontractor	1-22
	[v] Service Provider	1-22
	[vi] Computer Trespasser	1-23
	[vii] Extension Telephone	1-23
	[viii] Accessible to the Public	1-24
	[ix] FISA Electronic Surveillance	1-24
	[c] Remedies for Violations of the Wiretap Statute	1-25
	[d] State Wiretap Statutes	1-26
[2]	Electronic Communications Privacy Act and Stored Communications Act	1-26.1
	[a] Internet Service Providers and Other Online Providers	1-27
	[i] “Electronic Communication Service” and “Remote Computing Service”	1-27
	[ii] To the Public	1-28
	[iii] Exceptions	1-28
	[b] Warrants, Subpoenas, Orders: 18 U.S.C. Section 2703	1-29
	[i] Stored Contents	1-29
	[ii] Customer Records	1-30
	[iii] ECPA Section 2703(d) Court Order	1-31
	[iv] Delayed Notice to Customer	1-31
	[v] Customer Challenge	1-32
	[c] Preservation of Evidence	1-32
	[d] Release of Backup Copy	1-33
	[e] Civil Remedies	1-33
	[f] Limitation on Civil Actions	1-33
	[g] Defenses	1-33
	[h] Punishment for Unauthorized Access	1-34
	[i] Exceptions	1-35
[3]	Pen/Trap Statute	1-35
	[a] Exceptions	1-35
	[b] Orders	1-36
	[c] Cooperation and Secrecy	1-36
	[d] Roving Order	1-37
	[e] Emergency Situations	1-37

TABLE OF CONTENTS

	[f] Defenses	1-38
[4]	Right to Financial Privacy Act	1-38
	[a] Financial Institutions	1-40
	[b] Financial Record	1-40
	[c] Access for Intelligence and Protective Purposes	1-40
	[d] Delay in, Restrictions on, Notifying Customer	1-41
	[e] Customer Objections	1-42
	[f] Voluntary Disclosure	1-42
	[g] Defenses	1-42
[5]	Privacy Protection Act	1-42
[6]	Foreign Intelligence Surveillance Act	1-44
	[a] Scope of Intelligence Gathering	1-44
	[b] Business Records/Tangible Things	1-46
	[c] FISA Orders	1-46
	[d] Civil Remedies	1-48
§ 1.04	USA Patriot Act	1-49
	[1] Sunset Provision	1-49
	[2] Permanent Provisions	1-51
	[3] Challenges to the USA Patriot Act	1-56
	[4] The USA Freedom Act of 2015	1-57
§ 1.05	Other Federal Privacy Statutes	1-58
	[1] Fair Credit Reporting Act	1-58
	[2] Health Insurance Portability and Accountability Act	1-61
	[3] Gramm-Leach-Bliley Act	1-61
	[4] Computer Fraud and Abuse Act of 1986	1-62
	[5] Cable Communications Policy Act	1-62
	[6] Telecommunications Privacy Act	1-64
	[7] Family Educational Rights and Privacy Act	1-65
	[8] Video Privacy Protection Act of 1988	1-66.2
	[9] Employee Polygraph Protection Act of 1988	1-66.3
	[10] Telephone Consumer Protection Act of 1991	1-66.4
	[11] Children’s Online Privacy Protection Act of 1998	1-66.5
§ 1.06	Statutes Restricting Government’s <i>Disclosure</i> of Personal Information	1-67
	[1] Privacy Act of 1974	1-67
	[2] Freedom of Information Act	1-69

PRIVACY LAW

	[3] Driver’s Privacy Protection Act of 1994	1-71
§ 1.07	Social Security Numbers	1-74
	[1] Background	1-74
	[2] Federal Laws Restricting Use of SSNs	1-74
	[3] State Laws Restricting Use of SSNs	1-75
	[a] Treatment of SSNs in Texas Public Records	1-84

CHAPTER 2

Privacy and Security of Health Information

§ 2.01	Federal Regulation of Health Information	2-8
	[1] The Health Insurance Portability and Accountability Act of 1996 (HIPAA)	2-8
	[2] The HIPAA Administrative Simplification Regulations	2-8
	[3] The American Recovery and Reinvestment Act of 2009 (ARRA)	2-9
	[4] The Health Information Technology for Economic and Clinical Health (HITECH) Act	2-10
	[5] The Patient Protection and Affordable Care Act of 2010	2-11
	[6] The Genetic Information Nondiscrimination Act of 2008 (GINA)	2-11
	[a] Nondiscrimination Provisions	2-11
	[b] Privacy Protections for Generic Information	2-12
	[7] The HIPAA Omnibus Final Rule of 2013	2-13
	[8] Relationship to Other Federal Laws	2-14
	[a] Americans with Disabilities Act	2-14
	[b] Civil Rights of Institutionalized Persons Act	2-14
	[c] Clinical Laboratory Improvement Amendments (CLIA)	2-15
	[d] Controlled Substance Act (CSA)	2-15
	[e] Department of Transportation	2-15
	[f] Fair Credit Reporting Act (FCRA)	2-15
	[g] Family Medical Leave Act (FMLA)	2-16

TABLE OF CONTENTS

	[h]	Federal Educational Rights and Privacy Act (FERPA).....	2-16
	[i]	Freedom of Information Act (FOIA).....	2-16
	[j]	Gramm-Leach-Bliley (GLB) Act....	2-16
	[k]	National Labor Relations Act (NLRA).....	2-16
	[l]	Tribal Law.....	2-16.1
[9]		The Federal Trade Commission Act and Federal Trade Commission Authority...	2-16.1
	[a]	FTC involvement in Health Care...	2-16.1
	[b]	FTC Health Breach Notification Rule.....	2-16.2
	[c]	Application of FTC Health Breach Notification Rule to Intentional Disclosures.....	2-16.4
§ 2.02	State	Regulation of Health Information.....	2-17
	[1]	Health Information Laws.....	2-17
	[2]	Harmonizing State Privacy Laws.....	2-18
	[3]	Preemption of State Law.....	2-18
	[4]	U.S. State Genetic Privacy Laws.....	2-19
	[5]	Washington State “My Health My Data” Act.....	2-38.10
	[a]	Notice.....	2-38.11
	[b]	Consumer Rights.....	2-38.11
	[c]	Consent to Collect/Share and Authorization to Sell Consumer Health Data.....	2-38.12
	[i]	Consent Required to Collect or Share Consumer Health Data.....	2-38.12
	[ii]	Authorization Required to Sell or Offer to Sell Consumer Health Data....	2-38.13
	[d]	Security.....	2-38.14
	[e]	Mandatory Contract Between Regulated Entity and Processor.....	2-38.14
	[f]	Geofencing Prohibited.....	2-38.14
	[g]	Enforcement.....	2-38.14
[6]		Nevada Consumer Health Data Privacy Law.....	2-38.15
	[a]	Notice.....	2-38.15
	[b]	Consumer Rights.....	2-38.16

PRIVACY LAW

	[c]	Consent to Collect/Share and Authorization to Sell Consumer Health Data	2-38.17
	[i]	Consent Required to Collect or Share Consumer Health Data	2-38.17
	[ii]	Authorization Required to Sell or Offer to Sell Consumer Health Data	2-38.17
	[d]	Security	2-38.18
	[e]	Mandatory Contract Between Regulated Entity and Processor	2-38.19
	[f]	Geofencing Prohibited.	2-38.19
	[g]	Enforcement.	2-38.19
§ 2.03		Who Must Comply with HIPAA?	2-38.20
	[1]	Introduction	2-38.20
	[2]	Covered Entities.	2-38.20
	[a]	Health Plans.	2-38.20
	[b]	Health Care Clearinghouses	2-38.21
	[c]	Health Care Providers.	2-38.21
	[d]	Organizational Requirements for Certain Covered Entities	2-38.22
	[i]	Hybrid Entities	2-38.22
	[ii]	Affiliated Covered Entities.	2-38.22
	[iii]	Covered Entities with Multiple Covered Functions.	2-38.23
	[iv]	Organized Health Care Arrangements.	2-38.23
	[3]	Business Associates	2-38.24
	[a]	Introduction	2-38.24
	[b]	Definition of Business Associate Expanded by Final Rule.	2-38.24
	[c]	Direct Liability of Business Associates	2-38.24
	[4]	Who Are Not Business Associates	2-38.25
	[a]	Workforce Members	2-38.25
	[b]	Health Care Providers and Disclosures for Treatment	2-38.25
	[c]	Group Health Plan Sponsors.	2-38.25
	[d]	Government Agencies.	2-38.26
	[e]	Covered Entities Participating in an Organized Health Care Arrangement (OHCA)	2-38.26
	[f]	Conduits of PHI	2-38.26

TABLE OF CONTENTS

	[g] Financial Institutions Processing Consumer-Conducted Transactions	2-38.26
	[h] Personal Health Record Services . . .	2-38.26
§ 2.04	The Business Associate Agreement	2-38.27
	[1] Regulatory Background	2-38.27
	[2] Required Terms of a Business Associate Agreement	2-38.27
	[a] Compliance with Applicable Regulations	2-38.27
	[b] Report Breaches of Unsecured PHI	2-38.28
	[c] Use and Disclosure of PHI	2-38.28
	[d] Safeguards	2-38.28
	[e] Individual’s Right of Access to PHI	2-38.29
	[f] Material Breach	2-38.29
	[g] Termination	2-38.29
	[3] Compliance Dates	2-38.30
	[4] Penalties	2-38.30
§ 2.04A	Information Protected	2-38.31
	[1] Protected Health Information	2-38.31
	[2] Psychotherapy Notes	2-38.31
	[3] De-identified Information	2-38.32
	[4] Information Further Protected by Other Laws	2-38.33
	[a] State Laws	2-38.33
	[b] Other Federal Laws	2-38.34
	[5] Wellness Programs	2-38.35
§ 2.05	Disclosures of Limited Data Sets	2-38.37
	[1] General Rule	2-38.37
	[2] Definition of Limited Data Set	2-38.37
	[3] Data-Use Agreement	2-38.37
§ 2.06	Personal Representatives	2-40
	[1] General Rule	2-40
	[2] Exceptions	2-40
§ 2.07	Individual Rights	2-42
	[1] Restriction of Otherwise Permitted Uses and Disclosures of PHI	2-42
	[2] Notice of Privacy Provisions	2-42
	[a] Generally	2-42
	[b] Content Requirements	2-42
	[c] Joint Notice of Privacy Practices for Organized Health Care Arrangements	2-43

PRIVACY LAW

	[d] Provision of the Notice	2-43
	[i] Requirements for Health Plans	2-44
	[ii] Requirements for Websites and E-Mail	2-44
	[e] Revision of the Notice	2-45
	[f] Documentation	2-45
[3]	Access to the Designated Record Set	2-45
	[a] Generally	2-45
	[b] Electronic Copies of PHI Contained in an Electronic Health Record	2-46
	[c] Exceptions	2-46
	[d] Denial of Access	2-46
	[e] Request for Access and Timely Response	2-47
	[f] Provision of Access	2-48
	[g] Documentation	2-48
[4]	Amendment of the Designated Record Set	2-48
	[a] Generally	2-48
	[b] Exceptions	2-49
	[c] Request for Amendment and Timely Response	2-49
	[d] Documentation	2-50
[5]	Accounting for Disclosures of PHI	2-50
	[a] Generally	2-50
	[b] Exceptions	2-50.1
	[c] Required Information	2-50.2
	[d] Request for Accounting and Timely Response	2-50.3
	[e] Provision of the Accounting	2-50.3
	[f] Documentation	2-50.3
[6]	Complaints	2-50.3
§ 2.08	Minimum Necessary Standard	2-50.5
	[1] Minimum Necessary Data Uses	2-50.5
	[2] Minimum Necessary Disclosures	2-50.5
	[3] Reasonable Reliance Permitted in Certain Circumstances	2-50.5
	[4] Minimum Necessary Requests	2-50.6
	[5] Expectations	2-50.6
	[6] HHS Guidance	2-50.6
§ 2.09	Required Disclosures of PHI	2-50.7
§ 2.10	Permitted Uses and Disclosures of PHI	2-50.8
	[1] Disclosures of PHI to the Individual	2-50.8
	[2] Uses and Disclosures of PHI for Treatment, Payment and Health Care Operations	2-50.8

TABLE OF CONTENTS

xvii

	[a] Treatment	2-50.9
	[b] Payment	2-50.9
	[c] Health Care Operations	2-50.9
	[d] Consent	2-50.10
[3]	Incidental Uses and Disclosures	2-51
[4]	Uses and Disclosures Required by Law	2-51
	[a] Disclosures to Report Victims of Abuse, Neglect or Domestic Violence	2-51
	[b] Disclosures for Judicial and Administrative Proceedings	2-52
	[c] Disclosures for Law Enforcement Purposes	2-53
	[i] Disclosures Pursuant to Process or Required by Law	2-53
	[ii] Disclosure of Limited PHI for Identification and Location	2-54
	[iii] Disclosures About a Victim of a Crime	2-54
	[iv] Disclosure About a Decedent	2-54
	[v] Disclosure About a Crime on Premises	2-54
	[vi] Disclosure to Report a Crime in an Emergency	2-55
[5]	Disclosures for Public Health Activities	2-55
	[a] Disclosures to Public Health Authorities	2-55
	[b] Disclosures Related to Child Abuse or Neglect	2-55
	[c] Disclosures Related to FDA-Regulated Products	2-55
	[d] Disclosures for Exposure to a Communicable Disease	2-56
	[e] Disclosures to an Employer About a Member of Its Workforce	2-56
[6]	Use and Disclosures to Avert a Serious Threat to Health or Safety	2-56
[7]	Uses and Disclosures for Certain Government Functions	2-57
[8]	Uses and Disclosures for Health Oversight Activities	2-57

PRIVACY LAW

	[a] Generally	2-57
	[b] Disclosures by Whistleblowers	2-58
[9]	Uses and Disclosures for Research	
	Purposes	2-58
	[a] General Rule	2-58
	[b] Waiver or Alteration of the Authorization	2-58
	[c] Other Exceptions	2-59
[10]	Uses and Disclosures for Marketing	2-59
[11]	Uses and Disclosures for Fundraising	2-60
[12]	Disclosures by a Group Health Plan to a Plan Sponsor	2-60
	[a] Summary Health Information	2-61
	[b] Enrollment and Disenrollment Information	2-61
	[c] Plan Administration Functions	2-61
[13]	Disclosures for Workers' Compensation	2-62
[14]	Disclosures About Decedents and for Organ and Tissue Procurement	2-62
[15]	Uses and Disclosures for Underwriting	2-62
[16]	Uses and Disclosures for Facility Directories	2-62
[17]	Uses and Disclosure Related to Persons Involved in the Individual's Care	2-63
[18]	Uses and Disclosures for Notification	2-63
§ 2.11	Authorization to Use or Disclose PHI	2-65
	[1] Content Requirements	2-65
	[2] Defective Authorization	2-65
	[3] Conditioning Authorizations	2-66
	[4] Compound Authorizations	2-66
	[5] Revocation of an Authorization	2-66
	[6] Administrative Requirements	2-67
§ 2.12	Breach Notification Requirements	2-68
	[1] Requirements for Covered Entities and Business Associates	2-68
	[2] Requirements for PHR Vendors and Other Non-HIPAA-Covered Entities	2-69
§ 2.13	Administrative and Managerial Requirements	2-70
	[1] Privacy Official	2-70
	[2] Policies and Procedures	2-70
	[3] Duty to Mitigate	2-70
	[4] Training	2-70
	[5] Sanctions	2-71
	[6] Safeguards	2-71

TABLE OF CONTENTS

xix

	[7] Complaints	2-71
	[8] Partial Exemption for Fully Insured Group Health Plans	2-71
§ 2.14	Security Rule Risk Analysis Requirements	2-72
	[1] Introduction	2-72
	[2] Office for Civil Rights (OCR) Guidance	2-72
	[3] NIST Standards and Guidance	2-72
	[4] Required Elements of a Risk Analysis	2-73
	[a] Scope of the Analysis	2-73
	[b] Data Collection	2-73
	[c] Identify and Document Potential Threats and Vulnerabilities	2-74
	[d] Assess Current Security Measures	2-74
	[e] Determine the Likelihood of Threat Occurrence	2-74
	[f] Determine the Potential Impact of Threat Occurrence	2-74
	[g] Determine the Level of Risk	2-75
	[h] Finalize Documentation	2-75
	[i] Periodic Review and Updates of the Risk Assessment	2-75
§ 2.15	[Reserved]	2-76
§ 2.16	Compliance and Enforcement	2-77
	[1] Assistance with Compliance	2-77
	[2] Compliance Reviews and Complaint Investigations	2-77
	[3] Criminal Penalties	2-81
	[4] Civil Penalties	2-82
	[a] In General	2-82
	[b] Violations by More Than One Covered Entity	2-83
	[c] Violations Attributed to a Covered Entity	2-83
	[d] Notice of Proposed Determination	2-84
	[e] Hearings	2-85
	[i] Request for Hearing	2-85
	[ii] Burden of Proof	2-85
	[iii] Statistical Sampling	2-85
	[f] Decision	2-86
	[g] Appeals	2-86
	[h] Judicial Review	2-86
	[i] Enforcement by State Attorneys General	2-87

PRIVACY LAW

	[5] Private Right of Action	2-88
	[6] Distribution of Civil Penalties Collected	2-88
§ 2.17	<i>Form: Key ARRA/HITECH Act Amendments</i>	2-89
§ 2.18	<i>Form: Sample Notice of Privacy Practices</i>	2-92
§ 2.19	<i>Form: Sample Acknowledgment of Receipt of Notice of Privacy Practices.</i>	2-97
§ 2.20	<i>Form: Sample Authorization to Release Protected Health Information and Protected Financial Information (Health Insurance Plan)</i>	2-99
§ 2.21	<i>Form: Sample Agreement to Amend Existing Business Associate Agreement to Include Breach Notification Requirements.</i>	2-101
§ 2.22	<i>Form: Sample Patient Consent for Electronic Communication.</i>	2-105
§ 2.23	<i>Form: Sample Policy—Safeguarding Protected Health Information (PHI).</i>	2-107

CHAPTER 3

Financial Institutions and the Collection of Financial Data: The Gramm-Leach-Bliley Act and Related Laws and Rules

§ 3.01	The Gramm-Leach-Bliley Act: The Statutory Scheme.	3-8
	[1] Privacy Rules: Regulatory Agency Rulemaking	3-18
	[a] Banks	3-18
	[b] Brokers, Dealers and Funds	3-19
	[c] Credit Unions	3-20
	[d] Non-Federally Insured Credit Unions and Non-SEC Registered Broker-Dealers	3-21
	[e] Insurance Companies.	3-21
	[f] Other “Financial Institutions”.	3-22
	[2] Federal Trade Commission Regulatory Authority	3-23
	[a] FTC’s Jurisdiction	3-24
	[b] “Significantly Engaged” in, or “Incidental” to such, Financial Activities.	3-25

TABLE OF CONTENTS

	[3] Security Guidelines and Rules:		
	Regulatory Agency Rulemaking		3-28
	[a] Banking Agencies		3-29
	[b] Securities and Exchange Commission.		3-30
	[c] Federal Trade Commission.		3-30
	[d] National Credit Union Administration.		3-32.1
	[e] OCC, FRB and FDIC Joint Rule on Computer Security		3-32.2
	[4] Overlapping Privacy Rules; Hybrid Entities		3-32.3
	[5] No Private Cause of Action		3-32.4
§ 3.01A	The Dodd-Frank Wall Street Reform And Consumer Financial Protection Act		3-32.6
	[1] Bureau of Consumer Financial Protection		3-32.6
	[a] Rulemaking Authority: GLB’s Privacy Provisions		3-32.6
	[i] The CFPB		3-33
	[ii] Banking Agencies and NCUA.		3-34
	[iii] SEC		3-34
	[iv] CFTC.		3-34
	[v] State Insurance Authorities		3-35
	[vi] FTC		3-35
	[b] Rulemaking Authority: GLB’s Security Provisions		3-36
	[c] Supervision and Enforcement Authority		3-36
	[i] The CFPB		3-36
	[ii] SEC, FTC, State Insurance Authorities		3-38
	[iii] FRB, FDIC, OCC, NCUA		3-39
	[iv] CFTC.		3-39
	[2] FCRA		3-40
	[a] Rulemaking Authority.		3-40
	[i] Red Flag Rules		3-40
	[ii] Data Disposal Rules		3-40
	[iii] Other Rules		3-40
	[b] Enforcement.		3-41
§ 3.02	Relation to State Law		3-42
	[1] Greater Protection		3-42
	[2] State Law		3-42

§ 3.03	Who Must Comply with GLB?: “Financial Institutions”	3-47
	[1] Definition of “Financial Institution”	3-47
	[a] Financial Activities	3-47
	[b] Attorneys	3-51
	[2] E-commerce	3-52
	[3] Exemptions	3-53
	[a] Specific Exemptions	3-53
	[b] FTC Limitation: “Significantly Engaged” in Financial Activities	3-53
§ 3.04	What Information Is Covered?: “Nonpublic Personal Information”	3-54
	[1] Publicly Available Information	3-54
	[2] Personally Identifiable Financial Information	3-57
§ 3.05	Restrictions on Disclosures to a “Nonaffiliated Third Party”	3-62
	[1] Affiliate	3-62
	[2] Nonaffiliated Third Party	3-63
	[3] Exceptions	3-63
	[a] Section 6802(b)(2) Exceptions to Opt-Out Rule: Service Providers and Joint Marketers	3-63
	[b] Section 6802(e) Exceptions to Opt-Out Rule	3-65
	[i] Section 6802(e)(1): Processing and Servicing Transactions	3-66
	[ii] Overlapping Exceptions: Section 6802(b)(2) Versus Section 6802(e)(1)	3-67
	[iii] Section 6802(e)(2): Consent	3-68
	[iv] Section 6802(e)(3): Protection of Interests	3-70
	[v] Section 6802(e)(4): Compliance Purposes	3-70
	[vi] Section 6802(e)(5): Law Enforcement	3-70
	[vii] Section 6802(e)(6): FCRA	3-71
	[viii] Section 6802(e)(7): Business Transactions	3-71
	[ix] Section 6802(e)(8): Compliance with Law, Legal Process	3-71
§ 3.06	Disclosures to Affiliates	3-73
	[1] FCRA Affiliate Sharing	3-73

TABLE OF CONTENTS

xxiii

§ 3.07	Consumer Versus Customer	3-75
	[1] Consumer	3-75
	[a] Financial Product or Service.	3-77
	[b] Transfer of Account	3-78
	[2] Customer.	3-78
	[a] Insurance Policies	3-83
	[b] Loans	3-83
	[c] Former Customers.	3-84
	[3] Representatives of Individuals.	3-85
	[4] Trusts	3-85
§ 3.08	Privacy Notices: Initial Privacy Notice	3-87
	[1] To Consumers	3-87
	[a] In General	3-87
	[b] Short-Form Notice.	3-88
	[2] To Customers.	3-89
	[a] Exceptions	3-89
	[b] New Financial Products or Services.	3-91
	[c] Joint Accountholders.	3-91
	[d] Mergers and Acquisitions	3-92
	[3] Revised Privacy Notices	3-92
	[4] Model Privacy Notice	3-93
§ 3.09	Opt-Out Notice	3-95
	[1] When Required; Timing of	3-95
	[2] Content of Opt-Out Notice	3-96
	[3] Reasonable Means of Opting Out.	3-97
	[4] Reasonable Opportunity to Opt Out.	3-98
	[5] Partial Opt Out.	3-99
	[6] Duration of Opt Out	3-99
	[7] New Opt-Out Notices	3-99
	[8] Transfer of Accounts	3-100
	[9] Joint Accounts	3-102
	[10] When Information Is Disclosed Only Pursuant to the Opt-Out Exceptions (Section 6802(b)(2) or Section 6802(e)).	3-102
§ 3.10	Annual Privacy Notice	3-103
	[1] Continuation of Customer Relationship.	3-103
	[2] Termination of Customer Relationship.	3-103
§ 3.11	Content of Privacy Notice	3-105
	[1] Clear and Conspicuous/Format of Notice	3-106
	[2] Websites	3-107
	[3] Collection Versus Pass-Through of Information.	3-108

PRIVACY LAW

	[4]	Level of Detail	3-108
	[5]	Affiliate-Sharing Disclosure in Initial and Annual Privacy Notices: FCRA Considerations	3-109
	[6]	FCRA Credit Header Information	3-111
	[7]	Simplified Notices	3-112
	[8]	Security and Confidentiality	3-112
§ 3.12		Delivery of Notices	3-113
	[1]	Notices Displayed on a Website	3-113
	[a]	Initial Privacy and Opt-Out Notices	3-113
	[b]	Annual Privacy Notices When Customer Agrees to Receive Notice Electronically	3-114
	[c]	Alternative Method for Providing Annual Notices When Customer Has Not Agreed to Receive Notice Electronically	3-114.1
	[2]	Isolated Transactions; Oral Notice	3-114.4
	[3]	New Versions of Privacy Notice	3-114.4
	[4]	Joint Notices by More than One Financial Institution	3-114.4
	[5]	Joint Accounts	3-114.5
	[a]	Financial Institutions, Except Credit Unions and Financial Institutions Under the FTC's Enforcement Jurisdiction	3-114.5
	[b]	Financial Institutions Under the FTC's Enforcement Jurisdiction	3-114.5
	[c]	Credit Unions	3-114.5
	[d]	Opt Outs	3-114.6
	[6]	Customer Requests Not to Send Information	3-114.6
	[7]	Recordkeeping	3-114.6
§ 3.12A		Fair Credit Reporting Act	3-114.8
	[1]	Consumer Report Information	3-114.8
	[2]	Disclosure to Affiliates and to Nonaffiliates	3-114.9
	[3]	Consumer Opt-Out Rights	3-114.10
	[a]	Affiliate Sharing Opt Out: 15 U.S.C. Section 1681a(d)(2)(A)(iii)	3-114.10
	[b]	Affiliate Marketing Opt Out: 15 U.S.C. Section 1681s-3	3-114.11
	[i]	Eligibility Information	3-114.11

TABLE OF CONTENTS

xxv

	[ii]	Delivery of Opt-Out Notice	3-114.12
	[iii]	Contents of Opt-Out Notice	3-114.12
	[iv]	Scope and Duration of Opt Out	3-114.13
	[v]	Opportunity to Opt Out	3-114.13
	[vi]	Exceptions	3-114.14
	[vii]	Safe Harbor: Model Opt-Out Notices	3-114.14
[4]		Damages	3-114.15
[5]		FACTA	3-114.15
	[a]	Covered Accounts	3-114.16
	[b]	Identity Theft	3-114.17
	[c]	Red Flags	3-114.18
	[d]	Elements of Identity Theft Prevention Program	3-114.18
	[e]	Updating	3-114.19
	[f]	Red Flag Rules Not Applicable to Attorneys	3-114.19
	[g]	Accuracy and Integrity of Information Submitted to Consumer Reporting Agencies	3-114.19
	[h]	Disputes by Consumers Made Directly to Furnishers	3-114.21
	[i]	Contents of Dispute Notice (16 C.F.R. § 660.4(d) Information)	3-114.22
	[ii]	Disputes That a Furnisher Must Investigate	3-114.22
	[iii]	Disputes That a Furnisher Is <i>Not</i> Required to Investigate (16 C.F.R. § 660.4(b) Exceptions)	3-114.23
	[i]	Disposal of Records	3-114.24
	[i]	FTC Disposal Rule	3-114.25
	[ii]	Overlap with GLB Security Requirements	3-114.26
	[iii]	Relation to Other Laws	3-114.26
§ 3.13		Reuse and Redisclosure of Nonpublic Personal Information	3-114.27
	[1]	Use of Agent by Financial Institution: To Which Entity Does the Customer Relationship Attach?	3-114.27

PRIVACY LAW

	[2]	Nonaffiliated Third Parties (Including Service Providers)	3-114.27
	[3]	Information Disclosed Pursuant to Section 6802(b)(2) and Section 6802(e) Exceptions.	3-114.29
	[4]	Vendor Contract Requirements for Disclosures Made Pursuant to Section 6802(b)(2) Exception	3-114.33
	[5]	Account Number Information for Marketing Purposes	3-114.34
	[6]	FCRA Considerations: Redisclosure of GLB Information by Consumer Reporting Agencies	3-114.35
	[7]	USA Patriot Act Compliance	3-114.38
§ 3.14		Security	3-114.40
	[1]	SEC.	3-114.41
		[a] Security Rule	3-114.41
		[b] Incident Disclosure Guidelines	3-114.41
	[2]	Joint Banking Security Guidelines	3-114.42
		[a] Security Program, Customer Information, and Customer Information Systems	3-114.42
		[b] Assess Risks	3-114.44
		[c] Manage and Control Risks	3-114.44
		[d] Systems Testing.	3-114.46
		[e] Adjustments to Security Program	3-115
		[f] Unauthorized Access.	3-116
		[g] Service Providers and Subservicers	3-116
		[i] Due Diligence	3-117
		[ii] Service Provider Contracts	3-117
		[iii] Oversight.	3-118
		[iv] Service Provider Audits	3-119
		[h] Board of Directors.	3-119
		[i] Liability, Enforcement Actions.	3-120
		[j] Bank Holding Companies.	3-121
	[3]	FTC Security Rule.	3-122
		[a] Purpose and Scope	3-122
		[b] Overlapping Security Requirements.	3-122
		[c] Recipients of Customer Information	3-123
		[d] Affiliates and Service Providers	3-124
		[e] Customer Information and Consumer Information	3-125

TABLE OF CONTENTS

- [f] Standards for Safeguarding Customer Information 3-126
- [g] Designated Employee Responsible for Security Program 3-126
- [h] Assess Risks 3-126
- [i] Adjustments to Security Program 3-127
- § 3.15 State Financial Law 3-128
 - [1] California Financial Information Privacy Act 3-128
 - [a] Sharing Information with Affiliates 3-128
 - [b] Sharing Information with Nonaffiliated Third Parties 3-129
 - [i] Service Provider 3-130
 - [ii] Joint Marketing 3-130
 - [c] Exceptions 3-131
 - [d] Partial Preemption by FCRA 3-132
 - [e] Challenges to SB1 3-132
 - [2] California Insurance Law 3-134
 - [3] New York Department of Financial Services Cybersecurity Requirements 3-134.2
 - [a] Accountability 3-134.2
 - [b] Class A Company 3-134.3
 - [c] Risk Assessment 3-134.3
 - [d] Data Governance and Classification 3-134.4
 - [e] Access Control and Identity Management 3-134.5
 - [f] Systems and Network Security 3-134.5
 - [g] Data Retention 3-134.6
 - [h] Incident Response Plan 3-134.6
 - [i] Regulatory Reporting 3-134.7
 - [j] Exemptions 3-134.7
 - [k] Chronology of Enforcement and Amendments 3-134.8
- § 3.16 *Form: Model Privacy Notices* 3-135

CHAPTER 4

Privacy and Surveillance in the Workplace

- § 4.01 Overview 4-4
- § 4.02 The Fair Credit Reporting Act (FCRA) 4-7
 - [1] Who Is Affected? 4-7

PRIVACY LAW

	[2]	The Privacy Implications of the FCRA	4-7
		[a] Qualifying to Receive Reports from a Consumer Reporting Agency	4-8
		[b] Written Notice and Authorization	4-9
		[c] Adverse Action Procedures	4-9
		[d] The Fair and Accurate Credit Transactions Act of 2003 (FACTA)	4-9
		[i] Workplace Investigations	4-9
		[ii] Disposal of Consumer Credit Information	4-11
	[3]	Penalties for Noncompliance	4-11
	[4]	Additional Information About the FCRA	4-12
§ 4.03		The Americans with Disabilities Act (ADA)	4-13
	[1]	Who Must Comply with the ADA?	4-13
	[2]	Restrictions on Medical Inquires and Medical Examinations	4-13
		[a] Job Applicants	4-13
		[b] Individuals Who Have Received a Conditional Offer of Employment	4-15
		[c] Current Employees	4-15
	[3]	Confidentiality of Medical Information	4-16
	[4]	Administrative Enforcement and Litigation	4-17
	[5]	Additional Resources	4-18
§ 4.04		The Family and Medical Leave Act (FMLA)	4-19
	[1]	Covered	4-19
	[2]	Eligible Employees	4-19
	[3]	Health Information and Determining FMLA Eligibility	4-20
		[a] Medical Certification	4-20
		[b] The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule	4-21
		[c] Additional Information	4-21
		[d] Authentication and Clarification	4-22
		[e] Second and Third Opinions	4-22
		[f] Recertification	4-22
	[4]	Confidentiality and Storage of FMLA Records	4-23
		[a] FMLA Regulations	4-23

TABLE OF CONTENTS

	[b]	Confidentiality Requirements of the Generic Information Nondiscrimination Act of 2008 (GINA)	4-23
	[5]	Enforcement and Penalties for Noncompliance	4-23
§ 4.05		Verification of Employment Eligibility	4-24
	[1]	Who Is Affected?	4-24
	[2]	The Privacy Implications of the Employment Eligibility Verification Laws	4-24
	[3]	Penalties for Noncompliance	4-24.1
	[4]	Additional Resources	4-24.1
§ 4.06		The Employee Polygraph Protection Act of 1988 (EPPA)	4-24.2
	[1]	Who Is Covered?	4-24.2
	[2]	The Privacy Implications of the EPPA	4-24.2
	[3]	Penalties for Noncompliance	4-24.4
	[4]	Additional Resources	4-24.5
§ 4.07		Monitoring Employee Communications	4-25
	[1]	Telephone Conversations	4-25
		[a] Who Is Covered?	4-26
		[b] Exceptions	4-27
		[i] Ordinary Course of Business	4-27
		[ii] Prior Consent	4-28
	[2]	Online Communications (E-Mail and Internet Use)	4-29
		[a] The Wiretap Act	4-29
		[i] Ordinary Course of Business Exception	4-31
		[ii] Prior Consent	4-31
		[iii] Interception of Transactional Information	4-31
		[b] The Stored Communications Act	4-32
		[i] Service Provider Exception	4-32
		[ii] User Consent	4-33
		[c] Social Networking Media	4-34
	[3]	Radio Frequency Identification (RFID) Devices	4-35
	[4]	Penalties for Noncompliance	4-36
§ 4.08		The Health Insurance Portability and Accountability Act (HIPAA)	4-37
	[1]	Who Is Covered?	4-37

PRIVACY LAW

	[2]	The Privacy Implications of HIPAA	4-37
	[3]	Penalties for Noncompliance	4-38
	[4]	Employee Privacy and Personnel Information	4-39
	[5]	Additional Resources	4-40
§ 4.09		Searches at the Workplace	4-41
	[1]	Constitutional Limitations	4-41
	[2]	Employee Liability to Employers	4-42.1
	[3]	Employer Liability for Employee Actions	4-42.1
§ 4.10		Drug and Alcohol Testing	4-44
§ 4.11		Bring Your Own Device Programs	4-47
	[1]	What Is Bring Your Own Device (BYOD)?	4-47
	[2]	Employee Personal Data?	4-47
	[a]	Expectation of Privacy	4-47
	[b]	Remotely Deleting Data from Employee Devices	4-47
	[c]	Accessing Employee Private and Cloud-Based Accounts	4-48
	[3]	Regulatory Compliance	4-48
	[a]	The Health Insurance Portability and Accountability Act (HIPAA) Security Rule	4-48
	[b]	State Information Security Laws	4-49
	[c]	State Security Breach Notification Laws	4-49
	[d]	Federal Security Breach Notification Laws	4-50
	[4]	Litigation and Discover Procedures	4-50
	[5]	Information Security Risks	4-51
	[6]	Cloud Storage Applications	4-51
	[7]	Contractual Obligations	4-51
	[8]	Protection of Trade Secrets	4-51
	[9]	Employment Law Issues	4-53
	[10]	International Data Protection Laws	4-53
	[11]	Terms of BYOD Policies	4-53
§ 4.12		Post-Employment Inquiries	4-56
	[1]	EEOC Prohibited Practices	4-56
	[2]	State Qualified Privilege Statutes	4-56
	[3]	Recommended Practices	4-58
§ 4.13		Other Workplace Privacy Considerations	4-59
	[1]	Recordkeeping Obligations of Employers	4-59

TABLE OF CONTENTS xxxi

[a] Personnel and Employment
Records 4-59

[b] Other Employment Records 4-59

[c] Records Relating to a Charge
of Discrimination 4-60

[2] Questioning Employees About Other
Political Activity 4-60

CHAPTER 5

Global Data Protection Laws

§ 5.01 International Models of Privacy Protection 5-6.1

[1] Introduction 5-6.1

[2] Privacy Principles 5-7

[a] The OECD Guidelines 5-7

[i] Data Protection Principles 5-7

[ii] Transborder Data Flows 5-8

[iii] Cross-Border Enforcement
of Privacy Laws 5-9

[iv] The Evolving Privacy
Landscape 5-10

[b] The APEC Privacy Framework 5-10

[i] Introduction 5-10

[ii] APEC Privacy Principles 5-10

[iii] Cross-Border Privacy
Rules 5-13

[iv] Cross-Border Privacy
Enforcement Arrangement 5-14

[c] The United Nations Guidelines
for the Regulation of
Computerized Personal
Data Files 5-14.1

[d] The Madrid Privacy
Declaration 5-17

[e] Statement of Privacy Principles
by the United States and
Canada 5-19

[3] Approaches to Privacy 5-22

[a] The Right to Privacy 5-22

[b] Comprehensive Laws 5-23

[i] European Union 5-24

PRIVACY LAW

	[c]	Sectoral Laws	5-24
	[i]	Introduction	5-24
	[ii]	The United States	5-25
	[d]	Self-Regulation	5-25
§ 5.02		Data Protection Law in Europe	5-27
	[1]	Introduction	5-27
	[a]	Regulations	5-27
	[b]	Directives	5-27
	[c]	Decisions	5-28
	[2]	The Council of Europe	5-28
	[a]	Protection of the Privacy of Individuals vis-à-vis Electronic Data Banks: 1973 and 1974 Resolutions.	5-28
	[b]	Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data	5-30
	[c]	Amendments to the Convention	5-31
	[d]	Additional Protocol to the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data Regarding Supervisory Authorities and Transborder Data Flows.	5-32
	[3]	The European Economic Area	5-33
	[a]	Overview	5-33
	[b]	The Right to Privacy	5-33
	[c]	The EU Directives	5-34
	[i]	Introduction	5-34
	[ii]	Directive 95/46/EC of October 24, 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data	5-35
	[iii]	Directive 97/66/EC of December 15, 1997 Concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector	5-38

TABLE OF CONTENTS

xxxiii

	[iv]	Directive 2002/58/EC of July 12, 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications or ePrivacy Directive)	5-38
	[v]	Directive 2006/24/EC of March 15, 2006 on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC	5-47
	[d]	The General Data Protection Regulation	5-50
		[i] Background	5-50
		[ii] Controller versus Processor	5-51
		[iii] Penalties	5-52.2
§ 5.03		Member State Privacy Legislation	5-52.4
	[1]	Austria	5-52.4
	[2]	Belgium	5-53
	[3]	France	5-55
	[4]	Germany	5-58
		[a] Federal Data Protection Act	5-58
		[b] Federal and State Data Protection Authorities	5-62
		[c] Safe Harbor	5-63
	[5]	Italy	5-64
	[6]	The Netherlands	5-66
	[7]	Spain	5-68
	[8]	Sweden	5-70
	[9]	The United Kingdom	5-72
		[a] Brexit	5-75
		[b] UK Cross-Border Data Transfers	5-76
		[i] Adequacy Regulations	5-76
		[ii] Data Transfer Contract Clauses	5-76.1
	[10]	Other EU Member States	5-76.1

§ 5.04	Transfers of Personal Data from Europe	5-76.1
	[1] Introduction	5-76.1
	[a] Appropriate Safeguards	5-77
	[b] Derogations	5-77
	[c] Transfers to the U.S.	5-78
	[2] Standard Contractual Clauses	5-79
	[a] Standard Contractual Clauses Adopted Pursuant to the Data Protection Directive	5-80
	[b] Standard Contractual Clauses Adopted Pursuant to the GDPR	5-81
	[3] Data Transfers Between the U.S. and the EU	5-83
	[3A] The History of Data Transfers Programs Between the EU and the U.S.—The Rise and Fall of the EU-U.S. Safe Harbor and the EU-U.S. Privacy Shield	5-84
	[a] <i>Maximillian Schrems v. Data Protection Commissioner— “Schrems I”</i>	5-84
	[i] Post-Schrems Safe Harbor Negotiations	5-86
	[ii] Judicial Redress Act of 2015.	5-86
	[b] EU-U.S. Privacy Shield	5-87
	[i] Organizations That Could Participate in the EU-U.S. Privacy Shield	5-88
	[ii] Enforcement	5-88
	[iii] EU-U.S. Privacy Shield Principles	5-89
	[iv] Claims Handling	5-92
	[v] Benefits of Participation in the EU-U.S. Privacy Shield Framework	5-92
	[vi] U.S. Government Access to Personal Data of EU Citizens	5-92.1
	[vii] EU Individuals’ Rights	5-92.1
	[c] Invalidation of the Privacy Shield—“ <i>Schrems II</i> ”	5-92.2
	[4] The United States-Swiss Safe Harbor	5-92.3
	[5] Binding Corporate Rules	5-92.4
	[6] Exceptions	5-92.5

TABLE OF CONTENTS

xxxv

	[7] Consent by the Data Subject.	5-92.6
	[8] Compliance Checklist for Data Transfers	5-92.6
	[9] Transfer of Passenger Name Records (PNR) to the United States	5-92.8
	[10] The United States-European Union High Level Contact Group for Law Enforcement and Security	5-92.9
§ 5.05	Global Privacy Laws.	5-92.10
	[1] Canada	5-92.10
	[a] Alberta	5-96
	[b] British Columbia	5-98
	[c] Quebec	5-99
	[i] 2001 Private Sector Act	5-99
	[ii] 2021 Act	5-100
	[2] Latin America.	5-102.5
	[a] Argentina	5-102.6
	[b] Brazil	5-102.8
	[c] Chile.	5-107
	[d] Mexico	5-107
	[i] Principles of the Personal Data Protection Law	5-108
	[ii] Rights of Access, Rectification, Cancellation and Objection	5-110
	[iii] Data Transfers.	5-111
	[iv] Other Data Privacy Laws.	5-111
	[e] Peru	5-113
	[3] Asia-Pacific	5-114
	[a] Australia.	5-114
	[b] China	5-118.1
	[i] China’s Personal Information Protection Law	5-118.1
	[ii] Laws in China Impacting Personal Information Before the PIPL.	5-129
	[c] Hong Kong	5-133
	[d] Indonesia	5-134.1
	[e] Japan	5-134.2
	[i] History	5-134.2
	[ii] 2015 Amendment	5-134.2
	[iii] 2020 Amendment	5-134.3
	[iv] Background	5-134.4
	[v] Principles	5-134.6
	[f] Malaysia.	5-134.7

PRIVACY LAW

	[g] New Zealand	5-134.8
	[h] Philippines	5-134.9
	[i] Qatar	5-134.11
	[j] Russia	5-134.11
	[k] Singapore	5-134.12
	[l] South Korea	5-134.15
	[m] Taiwan	5-134.16
	[n] Thailand	5-134.18
	[o] Vietnam	5-134.19
	[p] Sri Lanka	5-134.20
	[i] General Provisions	5-134.20
	[ii] Cross Border Transfers.	5-134.21
[4]	India	5-134.22
	[a] The Digital Personal Data Protection Act, 2023.	5-134.22
	[b] Data Protection Before the Digital Personal Data Protection Act, 2023.	5-134.25
[5]	Middle East	5-134.26
	[a] Bahrain.	5-134.26
	[b] Israel.	5-134.27
	[c] United Arab Emirates: Dubai	5-134.29
§ 5.06	Multinational Data Protection Audit	5-134.30
	[1] Purpose of the Audit	5-134.30
	[2] Conducting the Audit.	5-134.30
§ 5.07	<i>Form: Sample Data Protection Audit Questionnaire for the European Union</i>	5-136
§ 5.08	<i>Form: Sample Multinational Privacy Audit Checklist</i>	5-139
§ 5.09	<i>Form: Sample Privacy Policy That Complies with Safe Harbor</i>	5-146

CHAPTER 6

Internet, Online and Mobile Privacy

§ 6.01	Introduction	6-5
§ 6.02	Federal Laws and Regulations	6-7
	[1] Laws and Regulations	6-7
	[a] Overview	6-7
	[b] The Children’s Online Privacy Protection Act (COPPA)	6-7
	[c] The Computer Fraud and Abuse Act	6-7

TABLE OF CONTENTS

xxxvii

	[2]	Federal Policy and Initiatives	6-8
		[a] Consumer Privacy Bill of Rights . . .	6-8
		[b] Fair Information Practice Principles	6-8
§ 6.03		The Federal Trade Commission and the Regulation of Internet, Online and Mobile Privacy	6-9
	[1]	Overview of the FTC’s Investigative and Law Enforcement Authority	6-9
		[a] The FTC Act	6-9
		[b] Privacy Laws and Rules the FTC Enforces	6-9
		[c] Online Privacy	6-10
		[d] Foreign Law Enforcement	6-11
		[i] The U.S. SAFE WEB Act of 2006	6-11
	[2]	The FTC’s Authority to Regulate Data Security	6-12
	[3]	The FTC’s Self-Regulatory Principles	6-14
		[a] Fair Information Practice Principles for Online Data Collection	6-14
		[b] Principles for Online Behavioral Advertising	6-14
	[4]	The FTC’s Enforcement Actions	6-15
		[a] Overview of Enforcement Activities	6-15
		[b] Online Privacy	6-15
		[c] Data Security	6-18
		[d] Children’s Privacy	6-21
		[e] Health Privacy	6-22
		[f] Location-Based Tracking and Cross-Device Tracking	6-23
		[g] Financial Privacy	6-24
	[5]	Legal Resources	6-24
§ 6.04		State Laws and Enforcement of Internet and Online Privacy	6-28.2
	[1]	The Role of the State Attorneys General	6-28.2
	[2]	Privacy Enforcement Actions	6-29
	[3]	The National Association of Attorneys General (NAAG)	6-30
	[4]	State Laws	6-31
		[a] Online Privacy	6-31

PRIVACY LAW

	[b]	Data Security and Encryption	6-31
	[c]	Do Not Track Disclosures	6-33
	[d]	Mandatory Privacy Policies for Websites or Online Services	6-33
	[e]	Privacy of Personal Information Held by Internet Service Providers	6-35
	[f]	False and Misleading Statements in Website Privacy Policies	6-35
	[g]	Notice of Monitoring Employee E-Mail Communications and Internet Access	6-36
	[5]	Consumer Fraud and Deceptive Trade Practices Legislation	6-37
	[a]	State UDAP Statutory Law	6-37
	[b]	State UDAP Caselaw	6-38
	[6]	Spyware Legislation	6-39
	[7]	Data Security Breach Legislation	6-40
	[8]	Tort of Invasion of Privacy	6-40.3
§ 6.05		Children's Privacy	6-40.5
	[1]	The Children's Online Privacy Protection Act	6-40.5
	[a]	Legislative History	6-40.5
	[i]	The Children's Online Privacy Protection Act (COPPA)	6-40.5
	[ii]	The Children's Online Privacy Protection Act Rule (the Rule)	6-40.5
	[iii]	Rulemaking and Rule Reviews	6-40.5
	[iv]	2013 COPPA Rule Amendments	6-40.6
	[b]	Who Must Comply?	6-41
	[c]	Who Is an "Operator"?	6-42
	[d]	Collection of Personal Information	6-42
	[e]	"Website or Online Service"	6-44
	[f]	"Directed to Children"	6-44
	[g]	General Audience Websites	6-45
	[h]	"Internal Operations"	6-46
	[i]	Privacy Notice	6-46
	[j]	Direct Notice to Parents Before Collecting Information	6-47

TABLE OF CONTENTS

xxxix

	[k]	Exceptions to Prior Consent	6-50
	[l]	Verifiable Parental Consent	6-50
	[m]	Confidentiality and Security Requirements.	6-51
	[n]	Data Retention.	6-52
	[o]	The Ban on Conditioning Participation on Information Collection	6-52
	[p]	Access to Information Collected.	6-52
	[q]	Revoking Consent and Deleting Information	6-53
	[r]	Safe Harbor Program	6-53
		[i] Compliance with Self- Regulatory Guidelines.	6-53
		[ii] Criteria for Approval of Self-Regulatory Guidelines	6-53
		[iii] CARU’s Safe Harbor Program	6-54
	[s]	COPPA and Voice Recordings.	6-55
	[t]	Compliance and Enforcement.	6-55
		[i] FTC Authority	6-55
		[ii] State Authority	6-56
		[iii] Enforcement	6-56
	[u]	FTC Educational and Compliance Resources	6-60
	[2]	State Legislation Protecting Children’s Privacy	6-66
		[a] Social Media Privacy: Postsecondary Education	6-66
		[b] The Right to Erase Social Media Posts.	6-66
		[c] Marketing and Advertising Activities	6-66
§ 6.06		Industry Self-Regulation.	6-68
	[1]	Introduction	6-68
	[2]	General Online Privacy Programs.	6-68
		[a] The Network Advertising Initiative (NAI).	6-68
		[i] NAI Self-Regulatory Principles	6-68
		[ii] Web Beacons	6-68.2
		[b] The Online Privacy Alliance	6-68.3
		[c] The DMA’s Online Information Guidelines	6-68.4

PRIVACY LAW

	[3]	Online Behavioral Advertising	6-69
		[a] Self-Regulatory Program.	6-69
		[b] The Principles	6-69
		[i] Education.	6-69
		[ii] Transparency.	6-70
		[iii] Consumer Control.	6-70
		[iv] Data Security	6-70
		[v] Material Changes	6-70
		[vi] Sensitive Data.	6-70
		[vii] Accountability.	6-71
	[c]	The Digital Advertising Alliance	6-71
		[i] The DAA’s Self-Regulatory Principles	6-72
		[ii] Application of the Principles to the Mobile Environment	6-73
		[iii] DAA Enforcement	6-73
	[4]	Mobile Marketing Guidelines	6-74
	[5]	Self-Regulatory Programs for Children’s Information	6-75
		[a] The CARU Guidelines for Interactive Electronic Media.	6-75
		[b] The DMA Children’s Guidelines.	6-76
	[6]	Privacy Seal Programs.	6-76
§ 6.07		Consumer Privacy.	6-76.2
	[1]	Big Data Privacy Concerns	6-76.2
	[2]	Online Behavioral Advertising	6-79
	[3]	Do Not Track.	6-80.1
		[a] California Online Privacy Protection Act Do Not Track Amendments	6-80.1
		[b] The “Do Not Track” Disclosure Requirement	6-80.1
		[c] The Meaning of “Do Not Track”	6-81
		[d] Industry Program Safe Harbor	6-81
		[e] Alternative Methods to Satisfy “Do Not Track” Disclosure	6-82
		[f] Sanctions	6-82
	[4]	The Internet of Things.	6-83
	[5]	Social Media Sites	6-84
	[6]	Mobile Privacy.	6-85
	[7]	Mobile Location Analytics	6-86

TABLE OF CONTENTS

xli

§ 6.08	Cybersecurity and Government Surveillance	6-87
	[1] Introduction	6-87
	[1A] Data Breach Notification Laws	6-87
	[2] The Federal Cybersecurity Framework	6-88
	[3] Federal Laws Governing Surveillance	6-90
	[a] Overview	6-90
	[b] The Foreign Intelligence Surveillance Act of 1978	6-91
	[i] The FISA Amendments Act of 2008	6-92
	[ii] Fourth Amendment Challenge	6-93
	[iii] FISA Amendments Act Reauthorization Act of 2012	6-94
	[iv] USA Freedom Act Provisions	6-94
	[c] The Electronic Communications Privacy Act	6-95
	[d] Reform of the Electronic Communications Privacy Act	6-96
	[e] Criminal and Civil Penalties	6-96
	[f] Government Access to Online Service Provider Information	6-97
	[g] The USA Freedom Act of 2015	6-97
	[h] Clarifying Lawful Overseas Use of Data (CLOUD) Act	6-98

CHAPTER 7

Privacy Concerns in Business Transactions: Mergers, Acquisitions, Corporate Restructuring, Bankruptcies, Liquidations

§ 7.01	Background: The Law Before the Year 2000	7-4
§ 7.02	The Case for Customer Lists as Business Assets	7-5
	[1] General Intangibles	7-5
	[2] Value	7-6
	[3] Trade Secrets	7-7
	[4] Intellectual Property	7-9
	[5] Alienable Property	7-10

§ 7.03	The Intersection with Privacy	7-12
	[1] The Influence of Technology	7-12
	[2] Customer Lists Sold for Marketing Purposes	7-12
	[3] Competing Legal Theories	7-13
§ 7.04	Consumer Protection Laws	7-14
	[1] The Federal Trade Commission Act	7-14
	[a] Misrepresentations Regarding Personal Information	7-14
	[i] Social Media and Social Networking	7-16
	[b] Enforcement	7-17
	[1A] The Federal Communications Act and FCC Authority to Regulate ISPs	7-19
	[2] State Consumer Protection Laws	7-20
	[a] Examples of State Enforcement Activity	7-20.1
§ 7.04A	Causes of Actions for Unauthorized Disclosures of Personal Information	7-20.7
	[1] Theories of Liability	7-20.8
§ 7.04B	Standing: U.S. Federal Court Subject Matter Jurisdiction	7-20.14
	[1] Standing in Identity Theft Cases	7-20.14
	[2] Standing in Cases Involving Internet Browsing History	7-20.22
	[3] Standing in Cases Involving Inaccurate Data	7-20.23
§ 7.05	Breach of Contract	7-20.24
	[1] Prerequisites for a Binding Contract	7-20.24
	[2] Offline Contracts	7-21
	[3] Online Contracts	7-21
	[a] Assent Is Required	7-22
	[b] Contracts of Adhesion	7-23
	[4] Damages	7-24
	[5] Equitable Relief	7-24
	[6] Privacy Seal Programs	7-25
	[7] Commercial Contracts	7-25
	[8] Breach of Contract Claims	7-26
§ 7.06	Privacy Rights	7-27
	[1] Constitutional Right Versus Tort	7-27
	[a] State Constitutions	7-27
	[2] Origins of Right Against Invasion of Privacy	7-28
	[3] Elements of Invasion of Privacy Claim	7-28

TABLE OF CONTENTS

xliii

	[4] Invasion of Privacy Claims Involving Personal Information	7-28.1
	[5] The Law Is Evolving	7-28.2
	[6] Negligence	7-28.2
	[a] Duty of Care	7-28.2
	[b] Proximate Cause	7-28.3
	[c] Injury	7-28.3
	[7] Conversion	7-28.5
§ 7.07	Special Concerns in Bankruptcy	7-29
	[1] The Clash Between Privacy and Bankruptcy Law	7-29
	[2] Goals of Bankruptcy	7-29
	[a] Assets of the Bankruptcy Estate	7-29
	[b] Customer List as an Asset of the Estate	7-30
	[c] The Trustee Must Maximize the Value of the Estate	7-30
	[d] Chapter 7: Liquidation	7-30
	[e] Chapter 11: Reorganization	7-31
	[f] The Bankruptcy Court Has Broad Powers	7-32
	[3] The <i>Toysmart</i> Bankruptcy	7-32
	[a] Background	7-32
	[b] Objections to Sale	7-33
	[c] Issues Raised	7-34
	[4] Transfer of Assets Under Bankruptcy Law	7-35
	[a] Restrictions on Transfer Outside Bankruptcy	7-35
	[b] Contractual Restrictions on Transfer	7-36
	[c] Restrictions Arising Under Consumer Protection Laws	7-36
	[d] The Code Ignores Restraints on Alienation	7-36
	[e] The Aggrieved Party Has a Claim Against the Estate	7-37
	[f] The Debtor May Reject an Executory Contract	7-37
	[g] May a Customer List Be Sold “Free and Clear”?	7-39
	[h] The Code Permits a “Free and Clear” Sale Under Certain Circumstances	7-39

PRIVACY LAW

		[i] Whether a Third Party May Have an “Interest” in a Customer List Is Unresolved	7-40
		[j] Whether a Customer List Could be Sold “Free and Clear” Is Questionable	7-41
	[5]	Automatic Stay	7-41
		[a] Pre-Petition Claims Are Stayed Automatically	7-41
		[b] Post-Petition Claims Are Not Stayed	7-42
		[c] The Automatic Stay Prevents Enforcement of an Order	7-43
		[d] An Enforcement Action Is Excepted from the Automatic Stay Under Section 362(b)(4)	7-44
		[e] Judicial Code Section 959(b)	7-46
		[f] The Law Is Unsettled	7-47
		[g] The Bankruptcy Court Has Discretion over Stays	7-47
	[6]	Bankruptcy Abuse Prevention and Consumer Protection Act of 2005	7-48
§ 7.08		Additional Concerns in Mergers, Acquisitions and Divestitures	7-51
	[1]	Ownership of Personal Information	7-51
	[2]	Fair Information Practice Principles	7-51
		[a] Notice/Awareness	7-52
		[b] Choice/Consent	7-52
		[c] Access/Participation	7-53
		[d] Integrity/Security	7-53
		[e] Enforcement/Redress	7-54
	[3]	Considerations for Business Transactions	7-54
		[a] Consumer Notice and Choice	7-54
		[b] Due Diligence	7-55
		[c] Transfer Issues	7-55
		[d] Post-Transfer Issues	7-56
		[e] Privacy Representations	7-57
	[4]	U.S. “Consumer Privacy Bill of Rights”	7-58
		[a] U.S. Sectoral Approach to Data Privacy	7-58
		[b] Seven Principles	7-59

CHAPTER 8

U.S. State Data Protection Laws

§ 8.01	State Privacy Statutes	8-6.1
§ 8.02	Data Security Breach Notification Laws	8-6.2
§ 8.03	Laws Governing Social Security Numbers	8-8
§ 8.04	Laws Regarding Merchant Liability	8-9
§ 8.05	Laws Addressing Information Security	8-10
	[1] Statutes Requiring Compliance with Technical Standards	8-30
	[2] Statutes Requiring Encryption	8-32
	[3] Statutes Requiring Businesses to Identify Personal Information They Disclose for Direct Marketing Purposes	8-32
	[4] Statutes Regulating Internet Service Providers	8-35
	[5] Statutes Requiring Identity Theft Protection	8-36
§ 8.06	Financial Industry Regulation	8-37
§ 8.07	Statutes Affecting Employment and Social Media	8-39
§ 8.08	Statutes Concerning Website and Mobile App Privacy Policies	8-53
	[1] Generally	8-53
	[2] Government Websites	8-54
	[3] False and Misleading Statements in Website Privacy Policies	8-63
§ 8.09	Statutes Regarding Internet Tracking	8-64
§ 8.10	Statutes Addressing Monitoring of Employee E-mail Communications and Internet Access	8-65
§ 8.11	Statutes Addressing Library Records, Books and e-Readers	8-66
§ 8.12	Statutes Addressing Online and Social Media Information About Students	8-67
§ 8.13	Statutes Regulating Use of Automated License Plate Readers	8-69
§ 8.14	Statutes on Collection and Use of Biometric Information	8-74
	[1] State Law	8-74
	[2] Local Laws	8-80.2
§ 8.15	Statutes Regulating the Sale of Personal Information (Data Brokers)	8-80.4

PRIVACY LAW

	[1]	Vermont	8-80.4
	[2]	Nevada	8-81
		[a] Application of Law	8-81
		[b] Notice of Information Collection Practices to be Given by Operator.	8-82.1
		[c] Requests Not to Sell Information	8-82.2
		[d] Enforcement and Penalties	8-82.2
	[3]	California	8-82.3
§ 8.16		Statutes Addressing the Internet of Things (IoT)	8-82.4
§ 8.17		“Comprehensive” Data Protection Laws: Statutes Addressing Consumer Privacy and Personal Information Generally.	8-83
	[1]	Introduction	8-83
	[2]	California Consumer Privacy Act of 2018.	8-83
		[a] Businesses Affected	8-84
		[b] Definition of Personal Information	8-84
		[c] Rights Granted to California Consumers.	8-85
		[i] The Right to Know.	8-86
		[ii] The Right to Access.	8-87
		[iii] The Right to Deletion.	8-87
		[iv] The Right to Opt-Out of the Sale of PI (Opt-In for Children Under Sixteen).	8-88
		[v] The Right to Equal Service.	8-88
		[d] Implementation of Rights	8-88
		[e] Enforcement.	8-89
	[3]	California Privacy Rights and Enforcement Act of 2020	8-89
		[a] Businesses Affected	8-89
		[b] Definition of Personal Information	8-90
		[c] Rights Granted to California Consumers.	8-92
		[i] The Right to Know.	8-92
		[ii] The Right to Access.	8-97
		[iii] The Right to Correct Inaccurate PI	8-98
		[iv] The Right to Deletion.	8-98
		[v] The Right to Opt-Out of the Sale or Sharing of PI (Opt-In for Children Under Sixteen).	8-99

TABLE OF CONTENTS

- [vi] The Right to Limit the Use of Sensitive Personal Information 8-100
- [vii] The Right to Equal Service and Against Discriminatory Practices; Financial Incentives for Providing PI. 8-101
- [d] Implementation of Rights 8-101
 - [i] Limitations on Retention and Processing of PI. 8-101
 - [ii] Required Contract with Third Parties 8-102
 - [iii] Security Requirements 8-102
 - [iv] Exercising Consumers’ Rights 8-102
- [e] Enforcement. 8-103
- [f] California Privacy Protection Agency 8-104
- [4] Virginia Consumer Data Protection Act of 2021 8-106.1
 - [a] Businesses Affected 8-106.1
 - [b] Information Impacted 8-107
 - [c] Rights Granted to Virginia Consumers. 8-108
 - [i] Right to Notice of Personal Data Practices 8-108
 - [ii] Rights Regarding Personal Data 8-108
 - [iii] Obligations of the Controller in Responding to a Consumer Request. 8-109
 - [d] Responsibilities of a Controller 8-110
 - [i] General Duties 8-110
 - [ii] Controller—Processor Contract 8-111
 - [iii] Data Protection Assessments. 8-111
 - [iv] De-identified Data 8-112
 - [e] Responsibilities of a Processor. 8-113
 - [f] Enforcement and Penalties 8-113
- [5] Colorado Data Protection Act of 2021. 8-114
 - [a] Businesses Affected 8-114
 - [b] Information Implicated 8-115

PRIVACY LAW

	[c]	Rights Granted to Colorado Consumers	8-116
		[i] Right to Notice of Personal Data Practices	8-116
		[ii] Rights Regarding Personal Data	8-118
		[iii] Obligations of the Controller in Responding to a Consumer Request	8-119
	[d]	Responsibilities of a Controller	8-120
		[i] General Duties	8-120
		[ii] Controller—Processor Contract	8-121
		[iii] Data Protection Assessments	8-122
		[iv] De-identified Data	8-123
	[e]	Responsibilities of a Processor	8-123
	[f]	Enforcement and Penalties	8-124
[6]	Utah	Consumer Privacy Act of 2022	8-124.1
		[a] Businesses Affected	8-124.1
		[b] Information Impacted	8-124.2
		[c] Rights Granted to Utah Consumers	8-124.4
		[i] Right to Notice of Personal Data Practices	8-124.4
		[ii] Rights Regarding Personal Data	8-124.5
		[iii] Obligations of the Controller in Responding to a Consumer Request	8-124.5
	[d]	Responsibilities of a Controller	8-124.7
		[i] General Duties	8-124.7
		[ii] Controller—Processor Contract	8-124.8
		[iii] Pseudonymous and Deidentified Data	8-124.8
	[e]	Responsibilities of a Processor	8-124.8
	[f]	Enforcement and Penalties	8-124.9
[7]	Connecticut	Personal Data Privacy Act of 2022	8-124.9
		[a] Businesses Affected	8-124.9
		[b] Information Impacted	8-124.10
		[c] Rights Granted to Connecticut Consumers	8-124.12
		[i] Right to Notice of Personal Data Practices	8-124.12

TABLE OF CONTENTS

	[ii] Rights Regarding Personal Data	8-124.13
	[iii] Obligations of the Controller in Responding to a Consumer Request	8-124.14
	[d] Responsibilities of a Controller	8-124.16
	[i] General Duties	8-124.16
	[ii] Controller—Processor Contract	8-124.17
	[iii] Data Protection Assessments	8-124.18
	[iv] Pseudonymous and Deidentified Data	8-124.19
	[e] Responsibilities of a Processor	8-124.19
	[f] Enforcement and Penalties	8-124.20
[8]	Iowa: An Act Relating to Consumer Data Protection	8-124.20
[9]	Indiana Consumer Data Privacy Act	8-124.20
[10]	Tennessee Information Protection Act	8-124.21
[11]	Montana Consumer Data Privacy Act	8-124.21
[12]	Florida Digital Bill of Rights	8-124.21
[13]	Texas Data Privacy and Security Act	8-124.21
[14]	Oregon Consumer Privacy Act	8-124.22
[15]	Delaware Personal Data Privacy Act	8-124.22
[16]	New Jersey Data Privacy Act	8-124.22
[17]	New Hampshire Expectation of Privacy Act	8-124.22
[18]	Kentucky Consumer Data Protection Act	8-124.23
[19]	Nebraska Data Privacy Act	8-124.23
[20]	Maryland Online Data Privacy Act	8-124.23
[21]	Minnesota Consumer Data Privacy Act	8-124.23
[22]	Rhode Island Data Transparency and Privacy Protection Act	8-124.24
§ 8.18	Comparison of the EU GDPR with U.S. State Data Protection Laws	8-125
§ 8.19	Laws Governing Information of Children	8-306
	[1] Age Verification Laws	8-306
	[a] Table of Age Verification Laws	8-306
	[b] Specific Examples of Age Verification Laws	8-308

PRIVACY LAW

	[i]	Louisiana Liability for Harmful Material, Age Verification Law	8-309
	[ii]	Texas Age Verification Law	8-309
	[iii]	Florida Age Verification Law	8-310
	[iv]	Tennessee Age Verification Law	8-311
[2]		Laws Restricting Social Media for Minors	8-312
	[a]	Utah Social Media Law	8-312
		[i] Requirements of the Minor Protection in Social Media Act	8-312
		[ii] Enforcement and Violations for the Minor Protection in Social Media Act.	8-313
		[iii] Utah Act Regarding Harm to Minors by Algorithmically Curated Social Media Service	8-314
	[b]	Florida Social Media Law	8-314
		[i] Requirements of the Law	8-314
		[ii] Enforcement and Violations	8-315
	[c]	Tennessee Protecting Children from Social Media Act.	8-316
		[i] Requirements of the Tennessee Protecting Children from Social Media Act.	8-316
[3]		California Right to be Forgotten Law for Minors	8-316
[4]		California Age-Appropriate Design Code Act	8-318
	[a]	Data Protection Impact Assessment	8-319
	[b]	Requirements for the Service	8-320
	[c]	Restrictions	8-321
	[d]	Enforcement and Violations	8-322
[5]		Florida Protection of Children in Online Spaces Act	8-322
	[a]	Prohibitions	8-323
	[b]	Enforcement and Violations	8-324

TABLE OF CONTENTS

li

[6]	Maryland Age-Appropriate Design Code Act (Maryland Kids Code).....	8-325
[a]	Data Protection Impact Assessment	8-325
[b]	Requirements for the Online Product	8-326
[c]	Restrictions	8-327
[d]	Enforcement and Violations	8-328
APPENDIX A: Summary of State Data Breach Notification Laws		A-1
INDEX.....		I-1