

# Table of Contents

## Volume 1

### CHAPTER 1. INTRODUCTION

- § 1:1 The rise of information security and privacy
- § 1:2 General privacy principles
- § 1:3 Fair Information Practices—Origins
- § 1:4 Organisation for Economic Co-operation and Development guidelines
  - § 1:5 —Scope of guidelines
  - § 1:6 —Basic principles of national application—Collection limitation principle
    - § 1:7 — —Data quality principle
    - § 1:8 — —Purpose specification principle
    - § 1:9 — —Use limitation principle
    - § 1:10 — —Security safeguards principle
    - § 1:11 — —Openness principle
    - § 1:12 — —Individual participation principle
    - § 1:13 — —Accountability principle
    - § 1:14 —Basic principles of international application—Free flow and legitimate restrictions
      - § 1:15 —National implementation
      - § 1:16 —International co-operation and interoperability
      - § 1:17 Principles adopted by the Asia-Pacific Economic Cooperation
      - § 1:18 APEC information privacy principles—Preventing harm
        - § 1:19 —Notice
        - § 1:20 —Collection limitation
        - § 1:21 —Uses of personal information
        - § 1:22 —Choice
        - § 1:23 —Integrity of personal information
        - § 1:24 —Security safeguards
        - § 1:25 —Access and correction
        - § 1:26 —Accountability
        - § 1:27 The FTC's formulation of FIPs
        - § 1:28 Privacy and security—The seven U.S. Safe Harbor privacy principles

## CHAPTER 2. INTERNET AND SOCIAL MEDIA PRIVACY

### I. OVERVIEW

- § 2:1 Introduction to Internet privacy
- § 2:2 Role of FTC in privacy and security enforcement
- § 2:3 Analyzing Internet service provider's obligations
- § 2:4 Reporting requirements of an ECS or RCS
- § 2:5 Forwarding of report
- § 2:6 Permitted disclosures by the National Center for Missing and Exploited Children
- § 2:7 Limited liability for electronic communication service providers, remote computing service providers, or domain name registrar
- § 2:8 Use to combat child pornography of technical elements relating to images reported to the CyberTipline
- § 2:9 Use by electronic communication service providers and remote computing service providers
- § 2:10 Posting of information on social networking sites operating as a waiver of privacy
- § 2:11 Logging of Internet Protocol addresses
- § 2:12 Internet gambling
- § 2:13 —Defining prohibited conduct
- § 2:14 —Preemption of other laws
- § 2:15 —Use of financial instruments for unlawful Internet gambling
- § 2:16 —Regulations on payment systems
- § 2:17 —Civil remedies
- § 2:18 —Limitations regarding interactive computer services
- § 2:19 —Criminal penalties
- § 2:20 —Circumventions
- § 2:21 Right to be forgotten—United States
- § 2:22 Digital Millennium Copyright Act and privacy
- § 2:23 Bankruptcy Reform Act of 2005—Privacy Issues
- § 2:24 —Complying with Bankruptcy Reform Act—Practice pointer
- § 2:25 Sharing of customer information with third parties—Opt-in versus opt-out issues
- § 2:26 Commercial emails—Double opt-ins
- § 2:27 Blogging
- § 2:28 Americans with Disabilities Act and websites
- § 2:29 Understanding ISP compliance
- § 2:30 Amendments to privacy policies
- § 2:31 Are IP addresses “personally identifiable information”?

## TABLE OF CONTENTS

§ 2:32	Subscriber information and privacy
§ 2:33	Online offers
§ 2:34	Restore Online Shopper Confidence Act
§ 2:35	—Requirements for certain Internet-based sales
§ 2:36	—Prohibition on data-pass used to facilitate certain deceptive Internet sales transactions
§ 2:37	—Application with other law
§ 2:38	—Negative option marketing on the Internet
§ 2:39	—Enforcement by Federal Trade Commission
§ 2:40	—Enforcement by State attorneys general
§ 2:41	—Notice to Commission required for Attorney General action
§ 2:42	—Construction
§ 2:43	—Preemption
§ 2:44	Social media privacy and Electronic Communications Privacy Act
§ 2:45	Social media and employers' requests for information
§ 2:46	Student online privacy statutes
§ 2:47	First Amendment and social media
§ 2:48	Privacy and Twitter posts
§ 2:49	National Labor Relations Board and social media— Costco Wholesale Corp., and Boch Imports
§ 2:50	Social media discovery

## II. SPECIFIC STATE PROVISIONS

### A. IN GENERAL

§ 2:51	In general
§ 2:52	Opt-out issues and public display of information

### B. ARKANSAS

§ 2:53	Arkansas
--------	----------

### C. CALIFORNIA

§ 2:54	The Online Privacy Protection Act—including DNT amendment
§ 2:55	Enforcement of Online Privacy Protection Act (Cal OPPA)
§ 2:56	Online Protection of Minors
§ 2:57	—Restrictions on advertising
§ 2:58	—Restrictions on use, disclosure, or compiling of information regarding minors
§ 2:59	—No requirement to collect or retain information
§ 2:60	—Advertising service compliance

## INFORMATION SECURITY AND PRIVACY

- § 2:61 —Exceptions
- § 2:62 —Deletion of information by minors
- § 2:63 —Deemed compliance
- § 2:64 —No requirement to collect age information
- § 2:65 —Effective date
- § 2:66 Internet and student marketing law—Section  
operative January 1, 2016
- § 2:67 —Exceptions
- § 2:68 Privacy of pupil records—Information obtained from  
social media
- § 2:69 Restrictions on direct marketing—Shine the Light
- § 2:70 —Disclosure
- § 2:71 — —Forms that do not trigger the statute
- § 2:72 — —Substantive requirements
- § 2:73 — —Other specialized requirements
- § 2:74 — —Other exceptions
- § 2:75 — —Enforcement
- § 2:76 — —Waiver
- § 2:77 —Shine the Light law interpreted
- § 2:78 Electronic Commerce Act of 1984
- § 2:79 California Internet of Things (IoT) Security Law—  
Introduction
- § 2:80 —Exemptions
- § 2:81 —Enforcement
- § 2:82 —Effective date

## D. COLORADO

- § 2:83 ISP data retention requirements
- § 2:84 Information regarding peace officers on the Internet

## E. DELAWARE

- § 2:85 Student Data Privacy Protection Act—Operator duties
- § 2:86 —Operator prohibited activities
- § 2:87 —Exclusions
- § 2:88 —Effective date
- § 2:89 —Enforcement
- § 2:90 Internet privacy—Online and Personal Privacy  
Protection Act
- § 2:91 — —Prohibitions on online marketing or advertising to  
a child
- § 2:92 — —Posting of privacy policy by operators of  
commercial online sites and services
- § 2:93 — —Privacy of information regarding book service  
users

## TABLE OF CONTENTS

- § 2:94 — — —Enforcement
- § 2:95 — — —Reporting requirements
- § 2:96 — — —Enforcement

### F. GEORGIA

- § 2:97 Disclosure requirements
- § 2:98 Data security requirements for telecommunications companies

### G. ILLINOIS

- § 2:99 Restrictions upon cancellation of Internet service
- § 2:100 Collection and storage of IP addresses
- § 2:101 Illinois supervised release

### H. MICHIGAN

- § 2:102 Michigan

### I. MINNESOTA

- § 2:103 ISP disclosure laws
- § 2:104 Wireless telecommunication
- § 2:105 Deceptive trade practice statute

### J. NEBRASKA

- § 2:106 Internet privacy policies

### K. NEVADA

- § 2:107 Restrictions upon ISPs

### L. NEW JERSEY

- § 2:108 Internet Dating Safety Act
- § 2:109 —Enforcement
- § 2:110 —Exceptions
- § 2:111 —Additional regulations

### M. OKLAHOMA

- § 2:112 State employee's personal information

### N. PENNSYLVANIA

- § 2:113 Internet privacy policies

O. TENNESSEE

- § 2:114 Restrictions upon certain Internet conduct

P. UTAH

- § 2:115 Notice of Intent to Sell Nonpublic Personal  
Information Act

**CHAPTER 3. THE CHILDREN'S ONLINE  
PRIVACY PROTECTION ACT**

- § 3:1 Children's Online Privacy Protection Act (COPPA)—A  
law in transition
- § 3:2 Age representations and click-wrap agreements
- § 3:3 Revised COPPA regulations
- § 3:4 Key concepts—What is personal information
- § 3:5 —Disclosure
- § 3:6 —Operators of websites and online services
- § 3:7 —Obtaining verifiable parental consent
- § 3:8 Regulation of unfair or deceptive acts or practices in  
connection with the collection, use, and/or disclosure  
of personal information from and about children on  
the Internet
- § 3:9 Notice
- § 3:10 Voluntary notice to parent of a child's online activities  
not involving the collection, use, or disclosure of  
personal information
- § 3:11 Notice to a parent of operator's intent to communicate  
with the child multiple times
- § 3:12 Notice to a parent in order to protect a child's safety
- § 3:13 Parental consent
- § 3:14 Right of parent to review personal information  
provided by a child
- § 3:15 Prohibition against conditioning a child's participation  
on collection of personal information
- § 3:16 Confidentiality, security, and integrity of personal  
information collected from children
- § 3:17 Enforcement
- § 3:18 Data retention and deletion requirements
- § 3:19 Safe harbor programs
- § 3:20 Voluntary commission approval processes
- § 3:21 Severability
- § 3:22 Practice tip—Complying with COPPA
- § 3:23 COPPA FAQ
- § 3:24 FTC enforcement actions—Pre-COPPA enforcement—  
In the Matter of Geocities

## TABLE OF CONTENTS

- § 3:25 — —In the Matter of Liberty Financial Companies, Inc
- § 3:26 — —COPPA enforcement matters—In the Matter of  
Toysmart.com
- § 3:27 — —In the Matter of Bigmailbox.Com, Inc., Monarch  
Services, Inc., Et Al., and Looksmart, Ltd., Noan  
Quan
- § 3:28 — —In the Matter of Lisa Frank, Inc
- § 3:29 — —In the Matter of American Pop Corn Company  
(Jolly Time)
- § 3:30 — —In the Matter of The Ohio Art Company  
(Etch-A-Sketch)
- § 3:31 — —Mrs. Field's Famous Brands, Inc
- § 3:32 — —In the Matter of Hershey Foods Corporation
- § 3:33 — —Bonzi Software, Inc
- § 3:34 — —In the Matter of UMG
- § 3:35 — —In the Matter of Xanga.com, Inc
- § 3:36 — —In the Matter of Imbee.com and Industrious Kid,  
Inc.
- § 3:37 — —In the Matter of Sony BMG Entertainment
- § 3:38 — —In the Matter of Iconix Brand Group
- § 3:39 — —In the Matter of Playdom, Inc., and Howard  
Marks
- § 3:40 — —W3 Innovations, LLC
- § 3:41 — —USA v. Jones O. Godwin, doing business as  
skidekids.com (United States District Court for the  
Northern District of Georgia)
- § 3:42 — —RockYou, Inc.
- § 3:43 — —Artist Arena, LLC
- § 3:44 — —Path, Inc.
- § 3:45 — —In re the Matter of Yelp Inc.
- § 3:46 — —In the Matter of TinyCo.
- § 3:47 — —In re the Matter of LAI Systems
- § 3:48 — —In the Matter of Retro Dreamer

## CHAPTER 4. THE COMMUNICATIONS DECENCY ACT

- § 4:1 Communications Decency Act (CDA)
- § 4:2 CDA—Restrictions upon liability—Good Samaritan  
blocking and screening of offensive material
- § 4:3 — —Civil liability
- § 4:4 — —Effect on other laws
- § 4:5 CDA and defining who is an interactive service  
provider
- § 4:6 Immunity for the conduct of affiliates
- § 4:7 The CDA and gripe sites

- § 4:8 The CDA and social networking
- § 4:9 CDA—Immunity v. defense
- § 4:10 —Disclosures by interactive computer services
- § 4:11 Takeaways from the Ninth Circuit for the CDA
- § 4:12 Prior rulings regarding categories and the CDA
- § 4:13 The CDA and employers
- § 4:14 CDA—Criminal liability
- § 4:15 The CDA and injunctive relief
- § 4:16 Practice tip—CDA
- § 4:17 CDA and state securities laws
- § 4:18 Statements in Form U-5 and immunity for online defamation
- § 4:19 E-mails and the CDA
- § 4:20 The CDA held not to be a basis for a motion to dismiss

## **CHAPTER 5. UNAUTHORIZED ACCESS TO NETWORKS/COMPUTER CRIMES**

### **I. COMPUTER FRAUD AND ABUSE ACT**

- § 5:1 Introduction
- § 5:2 Defining a “computer” under the CFAA
- § 5:3 Defining a protected computer
- § 5:4 Preemption of state trespass law on unauthorized access
- § 5:5 Acts that constitute crimes under the CFAA
- § 5:6 Interstate commerce requirement
- § 5:7 Requirement of intent
- § 5:8 Intent for unauthorized access and fraud under the CFAA
- § 5:9 Definition of fraud
- § 5:10 Knowledge of value not required
- § 5:11 What constitutes damages under CFAA
- § 5:12 Must a plaintiff allege damage and loss?
- § 5:13 Inconsistent ruling regarding “loss”
- § 5:14 Are litigation expenses loss?
- § 5:15 Are data costs loss in the smartphone context?
- § 5:16 The CFAA and deletions
- § 5:17 Copying of data held to be insufficient
- § 5:18 Aggregation of damages under CFAA
- § 5:19 CFAA violations and circumstantial evidence
- § 5:20 Unsolicited emails creating damage
- § 5:21 Loss without damage
- § 5:22 The CFAA and employee breaches of loyalty and data destruction



## TABLE OF CONTENTS

§ 5:23	The CFAA and sovereign immunity
§ 5:24	Applying the CFAA
§ 5:25	CFAA and value of information—Criminal convictions and market value
§ 5:26	CFAA and nonprotectable information
§ 5:27	Employer’s vicarious liability under CFAA
§ 5:28	Examples of violations of CFAA—Unauthorized access, including technological barriers
§ 5:29	—Gathering of email addresses
§ 5:30	—Diversion of customers/harvesting of customer lists
§ 5:31	—Defective software/time bombs
§ 5:32	—Setting of cookies
§ 5:33	—Authorized users exceeding scope of authority
§ 5:34	—Illegal subpoenas
§ 5:35	—Sending emails to a personal account
§ 5:36	—Mere review of information
§ 5:37	—Download of source code
§ 5:38	—Internet advertising
§ 5:39	—Login pages and the CFAA
§ 5:40	—CFAA and misuse of passwords
§ 5:41	—ToS violation and social media
§ 5:42	—CFAA and “throttling”
§ 5:43	Lack of revocation of authority
§ 5:44	Mere violation of license under CFAA
§ 5:45	CFAA and terms of service
§ 5:46	Enforcement provisions
§ 5:47	Injunctive relief under CFAA
§ 5:48	Preemption by the CUTSA
§ 5:49	Obtaining customer information and loss under CFAA
§ 5:50	Misappropriation of trade secrets via email forwarding
§ 5:51	Conspiracy to violate the CFAA
§ 5:52	Does Rule 9(b)’s heightened pleading standard apply to § 1030(a)(4) claims?

## II. THE ECONOMIC ESPIONAGE ACT

§ 5:53	Theft of trade secrets
§ 5:54	Economic espionage involving foreign states
§ 5:55	Exceptions to liability
§ 5:56	Forfeiture
§ 5:57	Confidentiality issues
§ 5:58	Civil proceedings

## III. FRAUD AND ACCESS DEVICES

§ 5:59	Fraud and access devices—Generally
--------	------------------------------------

- § 5:60 Criminal enforcement
- § 5:61 Exceptions to liability
- § 5:62 Extraterritorial violations

## **CHAPTER 6. COMPUTER CRIMES— SPECIFIC STATE PROVISIONS**

### **A. ALABAMA**

- § 6:1 Alabama Digital Crime Act

### **B. ARIZONA**

- § 6:2 Computer tampering
- § 6:3 Unauthorized release of proprietary or confidential  
computer security information

### **C. ARKANSAS**

- § 6:4 Computer fraud
- § 6:5 Computer trespass
- § 6:6 Civil enforcement
- § 6:7 Unlawful computerized communications
- § 6:8 Unlawful acts regarding computers
- § 6:9 Unlawful interference with access to computers
- § 6:10 Unlawful use or access to computers
- § 6:11 Unlawful use of encryption
- § 6:12 Computer password disclosure

### **D. CALIFORNIA**

- § 6:13 Unauthorized access to computers and networks
- § 6:14 No acquisition of confidential information
- § 6:15 Access to software and data
- § 6:16 Restrictions upon academic institutions
- § 6:17 Civil remedies
- § 6:18 Criminal penalties
- § 6:19 Cyberstalking—Civil remedies
- § 6:20 —Criminal remedies

### **E. COLORADO**

- § 6:21 Computer crimes
- § 6:22 Enforcement

### **F. CONNECTICUT**

- § 6:23 Unauthorized use of computer or computer network

## TABLE OF CONTENTS

- § 6:24 Unlawful sale of certain software
- § 6:25 —Exceptions to liability
- § 6:26 —Criminal enforcement
- § 6:27 —Civil enforcement
- § 6:28 Computer crime
- § 6:29 —Prohibited acts—Unauthorized access to a computer system
- § 6:30 — —Theft of computer services
- § 6:31 — —Interruption of computer services
- § 6:32 — —Misuse of computer system information
- § 6:33 — —Destruction of computer equipment
- § 6:34 —Criminal enforcement
- § 6:35 —Additional computer crimes related to terrorism
- § 6:36 —Civil remedies

## G. DELAWARE

- § 6:37 Computer crimes
- § 6:38 —Unauthorized access
- § 6:39 —Crimes involving emails
- § 6:40 —Enforcement

## H. FLORIDA

- § 6:41 Restrictions upon use of personal data
- § 6:42 Creation of identities
- § 6:43 Offenses against intellectual property
- § 6:44 Offenses against users of computers and electronic devices
- § 6:45 —Modification of equipment
- § 6:46 —Civil remedies
- § 6:47 —Forfeiture
- § 6:48 —Exemptions from civil remedies
- § 6:49 Offenses against public utilities
- § 6:50 Offenses against users of computers and electronic devices—Exceeding authorized access
- § 6:51 Trade secret exemption from public records act requests

## I. GEORGIA

- § 6:52 Computer systems protection
- § 6:53 —Computer trespass
- § 6:54 —Computer invasion of privacy
- § 6:55 —Computer forgery
- § 6:56 —Computer password disclosure

- § 6:57 —Civil relief
- § 6:58 —Criminal enforcement
- § 6:59 Transmission of trade names or trademarks

## **J. HAWAII**

- § 6:60 Computer fraud
- § 6:61 Computer damage
- § 6:62 Use of computer in commission of separate crime
- § 6:63 Unauthorized computer access
- § 6:64 Forfeiture of property

## **K. IDAHO**

- § 6:65 Computer crime

## **L. ILLINOIS**

- § 6:66 Computer tampering
- § 6:67 Aggravated computer tampering
- § 6:68 Computer fraud

## **M. IOWA**

- § 6:69 Electronic mail—Transmission of unsolicited bulk electronic mail
- § 6:70 —Sale or offer of direct sale of prescription drugs
- § 6:71 —Use of encryption
- § 6:72 —Civil relief and forfeiture

## **N. KANSAS**

- § 6:73 Computer crime
- § 6:74 Enforcement
- § 6:75 Defenses

## **O. LOUISIANA**

- § 6:76 Offenses against intellectual property
- § 6:77 Offenses against computer equipment or supplies
- § 6:78 Offenses against computer users
- § 6:79 Criminal use of internet virtual street-level map—Enhanced penalties
- § 6:80 Computer fraud
- § 6:81 Offenses against electronic mail service providers
- § 6:82 Computer tampering
- § 6:83 Criminal use of Internet, virtual, street map

TABLE OF CONTENTS

**P. MAINE**

§ 6:84 Criminal invasion of computer privacy

**Q. MARYLAND**

§ 6:85 Computer crimes

**R. MASSACHUSETTS**

§ 6:86 Computer crimes

**S. MICHIGAN**

§ 6:87 Accessing computers with the intent to defraud

§ 6:88 Accessing computers to acquire property or use  
computer services

§ 6:89 Use of computers to commit a crime

**T. MINNESOTA**

§ 6:90 Department of revenue

§ 6:91 Computer damage

§ 6:92 Computer theft

§ 6:93 Unauthorized computer access

§ 6:94 Facilitating access to computer security system

§ 6:95 Criminal use of encryption

**U. MISSISSIPPI**

§ 6:96 Computer fraud

§ 6:97 Offenses against computer users

§ 6:98 Tampering with computer equipment

§ 6:99 Offenses against intellectual property

§ 6:100 Cyberstalking

§ 6:101 Posting injurious messages

§ 6:102 Identity theft

§ 6:103 Expungement of criminal charges

§ 6:104 Additional penalties

§ 6:105 Improper use of a scanning device

**V. MISSOURI**

§ 6:106 Tampering with computer data

§ 6:107 Tampering with computer equipment

§ 6:108 Tampering with computer users

**W. NEBRASKA**

§ 6:109 Computer crimes

## INFORMATION SECURITY AND PRIVACY

- § 6:110 Depriving or obtaining property or services
- § 6:111 Harming or disrupting operations
- § 6:112 Obtaining confidential public information
- § 6:113 Access without authorization

## **X. NEVADA**

- § 6:114 Overview of Nevada criminal law
- § 6:115 Financial forgery laboratories
- § 6:116 Other identity theft crimes
- § 6:117 Public officials and databases
- § 6:118 Possession or sale of information to establish false status
- § 6:119 Computer crimes
- § 6:120 Interference with access or use of computers
- § 6:121 Forgery by creation, alteration, or deletion of data or other information
- § 6:122 Email restrictions
- § 6:123 Damages and enforcement
- § 6:124 Unlawful use of encryption
- § 6:125 Unlawful acts regarding information services
- § 6:126 Presumption of employee authority
- § 6:127 Civil enforcement

## **Y. NEW HAMPSHIRE**

- § 6:128 Computer crimes
- § 6:129 Misuse of computer network information
- § 6:130 Destruction of computer equipment
- § 6:131 Criminal enforcement

## **Z. NEW JERSEY**

- § 6:132 Computer related theft
- § 6:133 Disclosure of data from wrongful access
- § 6:134 Copy or alteration of program or software with reduced value
- § 6:135 Calculation of the value of property or services

## **AA. NEW MEXICO**

- § 6:136 Computer Crimes Act
- § 6:137 Computer access with intent to defraud or embezzle
- § 6:138 Computer abuse
- § 6:139 Unauthorized computer use
- § 6:140 Remedies

## TABLE OF CONTENTS

### **BB. NEW YORK**

- § 6:141 Unauthorized use of computer
- § 6:142 Computer trespass
- § 6:143 Computer tampering
- § 6:144 Unlawful duplication of computer related material
- § 6:145 Criminal possession of computer related material
- § 6:146 Defenses
- § 6:147 Theft of computer service

### **CC. NORTH CAROLINA**

- § 6:148 Accessing computers
- § 6:149 Accessing government computers
- § 6:150 Damaging computers
- § 6:151 Denial of computer services
- § 6:152 Denial of governmental computer services
- § 6:153 Computer trespass
- § 6:154 Exceptions to liability
- § 6:155 Conversion of computer information under North Carolina law

### **DD. NORTH DAKOTA**

- § 6:156 Computer crimes
- § 6:157 Fraudulent or misleading communications
- § 6:158 Unauthorized scanning of a network under North Dakota's computer crime law

### **EE. OHIO**

- § 6:159 Computer crimes

### **FF. OKLAHOMA**

- § 6:160 Computer Crimes Act
- § 6:161 Presumption of violation
- § 6:162 Criminal enforcement
- § 6:163 Access to computers
- § 6:164 Pre-action subpoenas

### **GG. OREGON**

- § 6:165 Computer crimes

### **HH. PENNSYLVANIA**

- § 6:166 Unlawful use of computer

## INFORMATION SECURITY AND PRIVACY

- § 6:167 Disruption of service
- § 6:168 Restitution and defenses
- § 6:169 Computer theft
- § 6:170 Unlawful duplication
- § 6:171 Computer trespass
- § 6:172 Distribution of computer viruses
- § 6:173 Computer-assisted remote harvesting of animals
- § 6:174 Email crimes
- § 6:175 False or misleading statements in Internet privacy policies

## II. RHODE ISLAND

- § 6:176 Access to computer for fraudulent purposes
- § 6:177 Unauthorized access
- § 6:178 Computer scanned documents
- § 6:179 Computer trespass
- § 6:180 Cyberstalking and cyberharassment
- § 6:181 Transmission of false data
- § 6:182 Tampering with computer source documents
- § 6:183 Criminal penalties for felony violations
- § 6:184 Civil remedies

## JJ. SOUTH CAROLINA

- § 6:185 Computer crimes in the first degree
- § 6:186 Computer crimes in the second degree
- § 6:187 Computer crimes in the third degree
- § 6:188 Civil remedies

## KK. TENNESSEE

- § 6:189 Computer crime law
- § 6:190 Restrictions on electronic mail
- § 6:191 Criminal enforcement
- § 6:192 Civil remedies
- § 6:193 Protection of secrecy and security
- § 6:194 Implied consent under the Tennessee Personal and Commercial Computer Act of 2003
- § 6:195 Litigation under Tennessee's computer crime law
- § 6:196 Scanning devices and reencoder

## LL. TEXAS

- § 6:197 Breach of computer security
- § 6:198 Online solicitation of minor



## TABLE OF CONTENTS

- § 6:199 Tampering with direct recording electronic voting machines

### **MM. VERMONT**

- § 6:200 Unauthorized access
- § 6:201 Access to computers for fraudulent purposes
- § 6:202 Alteration, damage, or interference
- § 6:203 Theft or destruction
- § 6:204 Civil remedies

### **NN. VIRGINIA**

- § 6:205 Computer fraud
- § 6:206 Unsolicited email
- § 6:207 Computer trespass
- § 6:208 Computer invasion of privacy
- § 6:209 Use of computer to gather identifying information
- § 6:210 Theft of computer services
- § 6:211 Personal trespass by computer
- § 6:212 Computer as instrument of offense
- § 6:213 Cyberstalking
- § 6:214 Unlawful use of encryption
- § 6:215 Embezzlement
- § 6:216 Damages and enforcement
- § 6:217 Civil enforcement
- § 6:218 Preemption

### **OO. WASHINGTON**

- § 6:219 Computer trespass
- § 6:220 Fraud in obtaining telecommunications service

### **PP. WEST VIRGINIA**

- § 6:221 Computer fraud
- § 6:222 Access to certain government computers
- § 6:223 Unauthorized access to computer services
- § 6:224 Unauthorized possession of computer data or programs
- § 6:225 Alteration or destruction of computer equipment
- § 6:226 Disruption of computer services
- § 6:227 Unauthorized possession of computer information
- § 6:228 Disclosure of computer security information
- § 6:229 Obtaining confidential public information
- § 6:230 Computer invasion of privacy
- § 6:231 Fraud regarding access devices

- § 6:232 Endangering public safety
- § 6:233 Harassment by computer
- § 6:234 Soliciting minor via computer
- § 6:235 Using a computer as an instrument of forgery
- § 6:236 Defenses to criminal actions
- § 6:237 Civil remedies

## **QQ. WISCONSIN**

- § 6:238 Offenses against computer data and programs
- § 6:239 Offenses against computers, computer equipment, or supplies
- § 6:240 Computer crime statute and deletions

## **RR. WYOMING**

- § 6:241 Computer crime—Crimes against intellectual property
- § 6:242 — —Penalties
- § 6:243 Crimes against computer equipment or supplies
- § 6:244 Interruption or impairment of governmental operations or public services
- § 6:245 Crimes against computer users
- § 6:246 —Enforcement

# **CHAPTER 7. PRIVACY IN ELECTRONIC AND WIRE COMMUNICATIONS**

## **I. OVERVIEW**

- § 7:1 In general
- § 7:2 History of wiretapping
- § 7:3 Fourth Amendment and wiretapping
- § 7:4 Overview of ECPA
- § 7:5 Temporal distinctions—An introduction
- § 7:6 Temporal distinctions, interceptions, and inferences
- § 7:7 Lack of rerouting or other interception fatal to ECPA claim
- § 7:8 Understanding the temporal nature
- § 7:9 Temporal distinctions—Forwarding email
- § 7:10 Public v. private service providers
- § 7:11 What is “ECS”?
- § 7:12 Electronic storage and computers
- § 7:13 What is an “RCS” and why does it matter?
- § 7:14 ECS v. RCS
- § 7:15 A summary of disclosure restrictions

## TABLE OF CONTENTS

- § 7:16 The ECPA and its lack of clarity
- § 7:17 Constitutionality of ECPA
- § 7:18 ECPA and preemption—A conflict in holdings
- § 7:19 Purpose of ECPA
- § 7:20 Standing under the Stored Communications Act
- § 7:21 ECPA and extraterritoriality

## II. TITLE I: THE WIRETAP ACT

### A. RESTRICTIONS ON INTERCEPTIONS AND DISCLOSURES

- § 7:22 Prohibited interceptions and disclosures of communications
- § 7:23 Collection of referrer header is not an interception of content
- § 7:24 Oral communications and reasonable expectation of privacy
- § 7:25 Review of emails on a laptop may not violate the ECPA
- § 7:26 Definition of intent for ECPA
- § 7:27 Practice tip—Consent under the ECPA
- § 7:28 Who is a party?
- § 7:29 Exceptions to consent
- § 7:30 Mandated disclosure of email—Court ordered consent
- § 7:31 When is a communication aurally acquired under the ECPA
- § 7:32 Requirement that communication be intercepted in transit for Title I violation
- § 7:33 Exceptions to liability
- § 7:34 —Disclosure to government entities
- § 7:35 —Acting under color of authority and participants in communications
- § 7:36 —Systems that transmit public communications
- § 7:37 —Public systems—Practice tip
- § 7:38 —Interception due to interference
- § 7:39 —Fraudulent, unlawful, or abusive acts
- § 7:40 Interception of communications by computer trespassers
- § 7:41 Restrictions upon interception of transmissions service providers that provide service to the public
- § 7:42 Recipient issues and consent to interception
- § 7:43 Interceptions by party to communication
- § 7:44 ECPA and access to servers
- § 7:45 Accessing coworker's email accounts
- § 7:46 Listening to a wrongfully acquired tape of a phone call is not an acquisition

## INFORMATION SECURITY AND PRIVACY

- § 7:47 Use of another's login information
- § 7:48 Enforcement
- § 7:49 Gmail litigation
- § 7:50 Availability of civil liability for aiding and abetting violation of Wiretap Act
- § 7:51 Requirement of commercial gain for certain violations
- § 7:52 Civil damages
- § 7:53 Lack of civil remedy for violation of section 2512
- § 7:54 Defense for good-faith reliance upon a warrant
- § 7:55 Governmental liability under the ECPA
- § 7:56 ECPA liability and municipalities
- § 7:57 Requirement of actual damages under ECPA
- § 7:58 Number of SCA violations
- § 7:59 Governmental civil liability
- § 7:60 Exclusion of evidence due to violation of ECPA and emails
- § 7:61 Authorization of interception of communications
- § 7:62 Enforcement of the communications assistance for Law Enforcement Act
- § 7:63 Videotaping of employees under the ECPA
- § 7:64 Private right of action under the ECPA for interception of encrypted signals
- § 7:65 Good faith warrant exception
- § 7:66 Good faith reliance on invalid warrant as ECPA defense
- § 7:67 Aiding and abetting liability for ECPA violations
- § 7:68 Procurement liability under ECPA
- § 7:69 Consent under the ECPA
- § 7:70 Participation in email investigations
- § 7:71 Purchasers of assets or businesses can monitor prior email addresses
- § 7:72 Is mere access to an email account sufficient to establish an ECPA violation?
- § 7:73 Request for subscriber information and anonymous subpoenas

## B. RESTRICTIONS ON DEVICES

- § 7:74 Manufacture, distribution, possession, and advertising of wire, oral, or electronic communication interception devices
- § 7:75 Exceptions to liability
- § 7:76 Enforcement

TABLE OF CONTENTS

**III. TITLE II: STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORDS ACCESS ACT**

§ 7:77	Intent of Act
§ 7:78	Distribution of stored communications
§ 7:79	Restrictions
§ 7:80	Exceptions permitting disclosure
§ 7:81	Remote computing services and Warshak—No clear answers for now
§ 7:82	Disclosures of customer records
§ 7:83	Disclosure of information regarding a subscriber
§ 7:84	Requirements of a court order
§ 7:85	Recent rulings regarding subscriber privacy
§ 7:86	Intent under ECPA for disclosures by ISPs
§ 7:87	Access to stored communications when sought by an intended recipient
§ 7:88	Restrictions upon disclosures by public service providers
§ 7:89	Out of district subpoenas under the ECPA
§ 7:90	Civil subpoenas for stored communications and the ECPA
§ 7:91	Violation of terms not actionable under the SCA for “public websites”
§ 7:92	Public display and discovery
§ 7:93	Procedural requirements of a court order
§ 7:94	Requirement to preserve evidence
§ 7:95	Backup preservation
§ 7:96	Delays in notice
§ 7:97	Cost reimbursement
§ 7:98	Disclosures of stored communications by nonservice providers
§ 7:99	Enforcement
§ 7:100	Disclosure of intercepted communications in response to a subpoena
§ 7:101	Civil actions and remedies
§ 7:102	Limits on statutory damages
§ 7:103	Actions against the United States
§ 7:104	Preclusion of civil action

**IV. PEN REGISTERS**

§ 7:105	In general
§ 7:106	Government acquisition of real-time cellular phone data

- § 7:107 Fourth Amendment and pen registers/real-time tracking through historical cell site data
- § 7:108 The Patriot Act

## **V. APPLICATION OF MONITORING LAWS**

- § 7:109 Viewing of computer screen or other devices as an interception
- § 7:110 Screenshots and the ECPA
- § 7:111 Disclosure of information in excess of a privacy policy—No violation of the ECPA
- § 7:112 Seizure of devices as an interception
- § 7:113 Unauthorized access to information constitutes a violation of the ECPA
- § 7:114 Disclosures of information to third parties
- § 7:115 ISP's liability for gathering a subscriber's email
- § 7:116 Use of illegally intercepted communications
- § 7:117 Review and recording of voicemail
- § 7:118 Recording by spouses
- § 7:119 Interspousal immunity
- § 7:120 SCA still applies to "post transmission" emails
- § 7:121 Impact of governmental regulations
- § 7:122 Specificity of wiretap
- § 7:123 Sealing of call data content information
- § 7:124 ECPA and trial subpoenas
- § 7:125 Sealing of Section 2703(d) orders
- § 7:126 Keystroke loggers and common law liability
- § 7:127 Pocket dials and the ECPA
- § 7:128 A conflict in holdings in social media
- § 7:129 Impersonation of person is not a violation of the SCA
- § 7:130 Wi-Fi sniffing
- § 7:131 ECPA and third-party data pass

## **CHAPTER 8. STATE ELECTRONIC AND WIRE COMMUNICATION LAWS**

### **I. GENERAL CONSIDERATIONS**

- § 8:1 Introduction
- § 8:2 One party consent issues, generally
- § 8:3 The First Amendment and positions of special importance
- § 8:4 Constitutionality of wiretap laws that do not require confidentiality
- § 8:5 Wiretap law and anti-SLAPP statutes

## TABLE OF CONTENTS

§ 8:6 Common law vicarious consent issues

## II. STATE LAWS

### A. ALABAMA

- § 8:7 Wiretapping—Criminal eavesdropping
- § 8:8 Criminal surveillance
- § 8:9 Installing an eavesdropping device
- § 8:10 Criminal possession of an eavesdropping device
- § 8:11 Divulging illegally obtained information
- § 8:12 Defenses
- § 8:13 Forfeiture of eavesdropping devices

### B. ALASKA

- § 8:14 Wiretapping—Improper use or disclosure of communications
- § 8:15 Eavesdropping
- § 8:16 Exceptions
- § 8:17 Duty to report
- § 8:18 Enforcement

### C. ARIZONA

- § 8:19 False or forged messages
- § 8:20 Opening, reading, or publishing sealed letter of another without authority
- § 8:21 Sending threatening or anonymous letter
- § 8:22 Interception of wire, electronic, and oral communications and pen registers
- § 8:23 Divulging communication service information
- § 8:24 Possession of interception devices
- § 8:25 Duty to report
- § 8:26 Court applications by law enforcement
- § 8:27 Exceptions
- § 8:28 Defenses
- § 8:29 Right to compensation
- § 8:30 Surreptitious photographing, filming, or recording

### D. CALIFORNIA

- § 8:31 California's Invasion of Privacy Act—An introduction
- § 8:32 Defining a confidential communication under the Invasion of Privacy Act
- § 8:33 Existence of a service-observing exception—CIPA
- § 8:34 Gmail and email litigation

## INFORMATION SECURITY AND PRIVACY

- § 8:35 Class certification and 632
- § 8:36 Statute of limitations on Invasion of Privacy Act claims
- § 8:37 Nature of allegation to survive demurrer or motion to dismiss
- § 8:38 Restrictions on eavesdropping
- § 8:39 Restrictions on recording confidential communications
- § 8:40 Exclusion from evidence
- § 8:41 Criminal enforcement of the restrictions on eavesdropping and recording confidential communications
- § 8:42 Restrictions on interception of cellular and cordless telephone communications
- § 8:43 Criminal enforcement
- § 8:44 Recordation of cordless or cellular radio telephones without consent
- § 8:45 Manufacture, sale, and possession of eavesdropping devices
- § 8:46 Police radio communications
- § 8:47 Disclosure of telegraphic or telephonic messages
- § 8:48 Procurement of telegraphic or telephone messages
- § 8:49 General exemptions
- § 8:50 Mailing list brokers
- § 8:51 Electronic tracking devices
- § 8:52 Restrictions upon lists for carpooling
- § 8:53 Application of California's Wiretap Law to calls originating in other states
- § 8:54 Choice of law without of state plaintiffs and CIPA
- § 8:55 Videotaping of employees—Immunity for certain government officials
- § 8:56 Immunity for violations of section 1708.8
- § 8:57 Immunity for violations of California's constitutional right of privacy
- § 8:58 Damages for violation of California's constitutional right of privacy
- § 8:59 Electronic Communications Privacy Act

## E. COLORADO

- § 8:60 Wiretapping devices
- § 8:61 Wiretapping
- § 8:62 Eavesdropping
- § 8:63 Exemptions
- § 8:64 Restrictions on telephones
- § 8:65 Abuse or obstruction of telephone and telegraph service
- § 8:66 Refusal to yield party line



## TABLE OF CONTENTS

- § 8:67 Directory requirements
- § 8:68 Cloning equipment
- § 8:69 Civil enforcement

### F. CONNECTICUT

- § 8:70 Civil action for wiretapping
- § 8:71 Restrictions on wiretapping
- § 8:72 Exemptions
- § 8:73 Tampering with private communications
- § 8:74 Eavesdropping
- § 8:75 Voyeurism
- § 8:76 Disseminating voyeuristic material

### G. DELAWARE

- § 8:77 Interception of communications
- § 8:78 Single party consent and other exceptions
- § 8:79 Divulging contents of communications
- § 8:80 Enforcement
- § 8:81 Civil enforcement
- § 8:82 Interception devices
- § 8:83 Law enforcement issues
- § 8:84 Admissibility of evidence
- § 8:85 Applicable privileges
- § 8:86 Civil liability
- § 8:87 Defense to enforcement
- § 8:88 Breaking and entering to place or remove equipment
- § 8:89 Obstruction, impediment, or prevention of interception
- § 8:90 Stored wire and electronic communications and transactional records access
- § 8:91 Divulging contents of communications, generally
- § 8:92 Disclosure of information
- § 8:93 Limitation on actions
- § 8:94 Order requirements and motions to quash
- § 8:95 Civil actions
- § 8:96 Pen registers and trap and trace devices

### H. FLORIDA

- § 8:97 Introduction
- § 8:98 Interception and disclosure of communications
- § 8:99 Key stroke loggers
- § 8:100 Restrictions on public providers of electronic communication service
- § 8:101 Enforcement

## INFORMATION SECURITY AND PRIVACY

- § 8:102 Manufacture, distribution, or possession of certain interception devices
- § 8:103 Confiscation of interception devices
- § 8:104 Prohibition on use of improperly intercepted wire or oral communications
- § 8:105 Civil remedies
- § 8:106 Good faith reliance
- § 8:107 Cutting, rerouting, and diverting of phone lines
- § 8:108 Unlawful access to stored communications
- § 8:109 Voluntary disclosure of customer communications or records
- § 8:110 Unlawful use of a two-way communications device
- § 8:111 Civil enforcement
- § 8:112 Good faith reliance as a defense to a sections 934.21 to 934.28 claim
- § 8:113 Restrictions on trap and trace and pen registers
- § 8:114 Defenses and cost reimbursement
- § 8:115 Criminal disclosure of a subpoena

### I. GEORGIA

- § 8:116 Restrictions on improper viewing through windows or doors
- § 8:117 Unlawful eavesdropping or surveillance
- § 8:118 Possession, sale, and distribution of eavesdropping devices
- § 8:119 Law enforcement
- § 8:120 Public Service Commission licenses to intercept telecommunications
- § 8:121 Consent
- § 8:122 Stored communications—Access to stored communications
- § 8:123 Inadmissibility of evidence
- § 8:124 Criminal enforcement

### J. ILLINOIS

- § 8:125 Eavesdropping
- § 8:126 Exempted acts
- § 8:127 Interception of communications by prison officials
- § 8:128 Additional exemptions
- § 8:129 Recording of interceptions
- § 8:130 Notice of interception
- § 8:131 Criminal enforcement
- § 8:132 Restrictions on the admission of evidence
- § 8:133 Civil remedies

## TABLE OF CONTENTS

- § 8:134 Assistance by common carriers
- § 8:135 Discovery of an eavesdropping device

### K. MAINE

- § 8:136 Interception of oral communications
- § 8:137 Disclosure or use of wire or oral communications
- § 8:138 Duty to report
- § 8:139 Possession of interception devices
- § 8:140 Sale of interception devices
- § 8:141 Civil enforcement
- § 8:142 Exceptions
- § 8:143 Disclosure to another state agency
- § 8:144 Exclusion from evidence

### L. MARYLAND

- § 8:145 Wiretapping
- § 8:146 Other interceptions
- § 8:147 Two party consent
- § 8:148 Additional exceptions
- § 8:149 Additional restrictions
- § 8:150 Police accessing text messages
- § 8:151 Enforcement
- § 8:152 Additional restrictions

### M. MASSACHUSETTS

- § 8:153 Interception of oral communications prohibited
- § 8:154 Application to electronic communications
- § 8:155 Editing of tape recordings in judicial proceeding prohibited
- § 8:156 Disclosure or use of wire or oral communications prohibited
- § 8:157 Disclosure of contents of applications, warrants, renewals, and returns prohibited
- § 8:158 Possession of interception devices prohibited
- § 8:159 Vicarious liability
- § 8:160 Exemptions to restrictions on interceptions
- § 8:161 Permitted disclosures and use of intercepted wire or oral communications
- § 8:162 Privileged communications
- § 8:163 Suppression of evidence
- § 8:164 Civil remedies
- § 8:165 Defenses to civil causes of action
- § 8:166 Other provisions

## INFORMATION SECURITY AND PRIVACY

- § 8:167 Massachusetts wiretap statute and application to cellular technology

### N. MICHIGAN

- § 8:168 Divulging contents of message
- § 8:169 Trespassing for purpose of eavesdropping
- § 8:170 Eavesdropping upon a private conversation
- § 8:171 One party or two party consent
- § 8:172 Installation of devices
- § 8:173 Use or divergence of information in violation of other laws
- § 8:174 Unlawful manufacture, possession, or transfer of eavesdropping devices
- § 8:175 Exceptions
- § 8:176 Civil remedies
- § 8:177 Civil cause of action under Michigan's Wiretap Law
- § 8:178 Inapplicability of Michigan's eavesdropping law to electronic communications
- § 8:179 Lack of civil remedy for violation of Michigan's electronic communication law
- § 8:180 Prima facie evidence of certain violations
- § 8:181 Surveillance of an individual in certain forms of undress
- § 8:182 Exceptions
- § 8:183 Interruption of messages
- § 8:184 Refusal to yield use of party line
- § 8:185 Offenses related to publication in a telephone directory
- § 8:186 Telecommunications access devices
- § 8:187 Seizure of devices
- § 8:188 Malicious use of service
- § 8:189 Publication of a telecommunications access device
- § 8:190 Unauthorized use or diversion of telecommunications services

### O. MINNESOTA

- § 8:191 Restrictions on wiretapping

### P. MONTANA

- § 8:192 Privacy in communications
- § 8:193 —Two party consent
- § 8:194 Enforcement
- § 8:195 Montana's restrictions on recording private conversations

## TABLE OF CONTENTS

- § 8:196 Montana’s warrantless recording of telephone conversations

### Q. NEVADA

- § 8:197 Wiretap
- § 8:198 Disclosure of existence, content, or substance of wire or radio communications
- § 8:199 Unauthorized connections
- § 8:200 Intrusion of privacy by listening device
- § 8:201 Enforcement
- § 8:202 Defenses
- § 8:203 Recording or telephone calls regarding emergency or service outages
- § 8:204 Interception of cellular calls and text messages under Nevada law

### R. NEW HAMPSHIRE

- § 8:205 Interception and disclosure of telecommunication or oral communications—Two party consent
- § 8:206 —Exceptions

### S. NEW JERSEY

- § 8:207 Wiretapping law
- § 8:208 Exceptions to liability
- § 8:209 Interception of radio communications
- § 8:210 Enforcement
- § 8:211 Interception devices
- § 8:212 Authorization to intercept communications
- § 8:213 Application for an order
- § 8:214 Grounds for entry of order
- § 8:215 Additional requirements for public facilities
- § 8:216 Requirements of an order
- § 8:217 Emergency authorization without an order
- § 8:218 Recording of intercepted communications
- § 8:219 Sealing of applications
- § 8:220 Inventories and inspection of intercepted communications
- § 8:221 Disclosure and use of intercepted communications
- § 8:222 Interception of communications relating to other offenses
- § 8:223 Improper disclosure of order or information regarding interceptions
- § 8:224 Service of copy of order and application before disclosure

## INFORMATION SECURITY AND PRIVACY

- § 8:225 Motion to suppress
- § 8:226 Reports by judges regarding orders
- § 8:227 Civil enforcement
- § 8:228 Good faith reliance on an order as a defense
- § 8:229 Severability
- § 8:230 Stored Communications Act—Unlawful access to stored communications
- § 8:231 Disclosures by public service providers and remote computer service companies
- § 8:232 Prerequisites to access
- § 8:233 Backup preservation
- § 8:234 Cost reimbursement
- § 8:235 Civil action
- § 8:236 Good faith defenses to civil or criminal actions

## T. NEW YORK

- § 8:237 Restrictions on evidence obtained via wiretapping
- § 8:238 New York's criminal restrictions on wiretapping—Eavesdropping
- § 8:239 Failure to report wiretapping
- § 8:240 Possession of eavesdropping devices
- § 8:241 Divulging an eavesdropping warrant
- § 8:242 Tampering with private communications
- § 8:243 Unlawfully obtaining communications information
- § 8:244 Failing to report criminal communications
- § 8:245 Unlawful surveillance
- § 8:246 Dissemination of an unlawful surveillance image in the second degree
- § 8:247 Dissemination of an unlawful surveillance image in the first degree
- § 8:248 Exceptions and application of certain provisions
- § 8:249 Eavesdropping and video surveillance warrants—Timing
- § 8:250 When eavesdropping and video surveillance warrants can be issued
- § 8:251 Applications for eavesdropping or video surveillance warrant
- § 8:252 Temporary authorization for eavesdropping or video surveillance
- § 8:253 Determination of applications for eavesdropping warrants
- § 8:254 Form and content of eavesdropping and video surveillance warrants
- § 8:255 Manner and time of execution of eavesdropping and video surveillance warrants

## TABLE OF CONTENTS

- § 8:256 Extension of eavesdropping and video surveillance warrants
- § 8:257 Progress reports and notice regarding eavesdropping and video surveillance warrants
- § 8:258 Custody of warrants, applications, and recordings
- § 8:259 Reports to the administrative office of the United States courts
- § 8:260 Disclosure and use of information obtained
- § 8:261 Notice before use of evidence
- § 8:262 Good faith defense

## U. NORTH CAROLINA

- § 8:263 Wiretap law
- § 8:264 Additional violations—Disclosure of interceptions
- § 8:265 Manufacture, distribution, possession, and advertising of certain devices
- § 8:266 Civil enforcement
- § 8:267 Good faith reliance defense
- § 8:268 Authorization for wiretaps

## V. PENNSYLVANIA

- § 8:269 Improper interception, disclosure, or use of communications
- § 8:270 Interceptions based upon consent
- § 8:271 Other permitted interceptions
- § 8:272 Exemptions for telemarketing or customer service, requirements, and data destruction
- § 8:273 Restrictions upon electronic, mechanical, or other devices
- § 8:274 Exceptions to restrictions on devices
- § 8:275 Seizure and forfeiture of devices
- § 8:276 Privileged communications
- § 8:277 Civil enforcement
- § 8:278 Defense
- § 8:279 Action for removal from office or employment
- § 8:280 Right to injunctive relief

## W. TEXAS

- § 8:281 Wiretap Act—Civil relief
- § 8:282 Defenses
- § 8:283 Criminal wiretapping—Unlawful use of criminal instrument
- § 8:284 Unlawful interception, use, or disclosure of communications

## INFORMATION SECURITY AND PRIVACY

- § 8:285 Public systems
- § 8:286 Effect of consent
- § 8:287 Creation or advertisement of interception devices
- § 8:288 Obstruction of monitoring
- § 8:289 Pen registers and trap and trace devices
- § 8:290 Unlawful access to stored communications
- § 8:291 Knowing disclosure of a communication
- § 8:292 Warrant requirements
- § 8:293 Texas law-enforcement warrants for installation of tracking equipment —Installation and use of pen register, esn reader, or similar equipment
- § 8:294 Texas law-enforcement warrants for installation of tracking equipment—Order authorizing installation and use of trap and trace device or similar equipment
- § 8:295 —Emergency installation and use of pen register or trap and trace device
- § 8:296 Texas law-enforcement warrants for mobile tracking devices
- § 8:297 Texas law-enforcement access to stored communications and other stored customer data—Grounds for a warrant
- § 8:298 —Requirements for government access to stored communications
- § 8:299 —Warrant issued in Texas for stored customer data or communications
- § 8:300 —Warrant issued in another state for stored customer data or communications
- § 8:301 —Backup preservation
- § 8:302 —Preclusion of notification
- § 8:303 —No cause of action

## X. VERMONT

- § 8:304 Wiretap prohibitions

## Y. WASHINGTON

- § 8:305 Wrongfully obtaining a telegraphic message
- § 8:306 Opening a sealed letter
- § 8:307 Interception or recording—Two party consent and other restrictions
- § 8:308 Civil enforcement
- § 8:309 Criminal enforcement
- § 8:310 Exemptions
- § 8:311 Other provisions



## TABLE OF CONTENTS

§ 8:312 Washington privacy act and implied consent

### Z. DISTRICT OF COLUMBIA

§ 8:313 Interception, disclosure, and use of communications  
§ 8:314 Enforcement  
§ 8:315 Exceptions  
§ 8:316 Possession, sale, distribution, manufacture, assembly,  
and advertising of interception devices  
§ 8:317 Confiscation of interception devices  
§ 8:318 Civil enforcement  
§ 8:319 Defenses  
§ 8:320 Restrictions and authorizations for government  
wiretapping

## CHAPTER 9. EMPLOYEE PRIVACY

### I. OVERVIEW

§ 9:1 Introduction  
§ 9:2 Employee privacy in the workplace  
§ 9:3 Searches of government employees  
§ 9:4 Internal investigations and invasion of privacy claims  
§ 9:5 Employee emails and the attorney-client privilege  
§ 9:6 Right to purchase creating an expectation of privacy  
§ 9:7 No general duty to monitor employee computer use  
§ 9:8 Employee emails and the spousal privilege  
§ 9:9 National Labor Relation Board's assessment of  
computer use policies  
§ 9:10 Other employee email issues  
§ 9:11 Employee privacy  
§ 9:12 Personal use of systems  
§ 9:13 Use of GPS for employee monitoring  
§ 9:14 Videotaping in workplace—Generally  
§ 9:15 Registered representatives and customer lists  
§ 9:16 New York City restrictions on use of credit history in  
employment

### II. FEDERAL AUTHORITIES

#### A. STATUTES

§ 9:17 Employee polygraphs  
§ 9:18 Notice of protections  
§ 9:19 Additional rulemaking and investigations  
§ 9:20 Enforcement

- § 9:21 No waiver of rights
- § 9:22 Rights of examinee
- § 9:23 Exemptions
- § 9:24 Restrictions on number and duration of tests
- § 9:25 Qualifications and requirements of examiners
- § 9:26 Disclosure of information
- § 9:27 Preemption

## B. REGULATIONS

- § 9:28 Employee Polygraph Protection Act—Scope of the  
Employee Polygraph Protection Act
- § 9:29 —Restrictions on conduct
- § 9:30 —Exemptions
- § 9:31 —Preemption
- § 9:32 —Notice requirements
- § 9:33 —Actions by the Secretary
- § 9:34 —Who is an “employer”?
- § 9:35 —Exclusions and exceptions—Public sector employers
- § 9:36 — —National defense and security
- § 9:37 — —Certain investigations
- § 9:38 — —Drug testing
- § 9:39 — —Access to property
- § 9:40 — —Exemptions for employers authorized to  
manufacture, distribute, or dispense controlled  
substances
- § 9:41 — —Employers providing security services
- § 9:42 — —Limitation on ongoing investigation exception
- § 9:43 — —Additional limitations on exceptions for security  
and controlled substances
- § 9:44 — —Rights of examinees
- § 9:45 —Pretest phase
- § 9:46 —Actual testing phase
- § 9:47 —Posttest phase
- § 9:48 —Qualifications and requirements of examiners
- § 9:49 —Three year record retention requirement
- § 9:50 —Disclosure of test information
- § 9:51 —Enforcement
- § 9:52 —Request for hearing

## III. STATE AUTHORITIES

### A. CALIFORNIA

- § 9:53 Restrictions on the use of polygraphs in certain  
contexts

## TABLE OF CONTENTS

- § 9:54 Restrictions on certain employment application questions
- § 9:55 Civil enforcement
- § 9:56 Exceptions
- § 9:57 Consideration of certain information related to applications to cities and other governmental agencies
- § 9:58 Additional restrictions
- § 9:59 Application to other crimes
- § 9:60 Cases interpreting section 432.7
- § 9:61 Disclosures to unions

### B. DELAWARE

- § 9:62 New Delaware law on employment and criminal records

### C. PENNSYLVANIA

- § 9:63 Use of records for employment
- § 9:64 City of Philadelphia—Fair Criminal Records Screening Standards
  - § 9:65 — —Prior arrest for a criminal offense
  - § 9:66 — —Previous conviction for a criminal offense
  - § 9:67 — —Enforcement
  - § 9:68 — —Advisory Committee
  - § 9:69 — —Constitutionality

### D. VIRGINIA

- § 9:70 Release of employee’s personal identifying information

## **CHAPTER 10. FOREIGN INTELLIGENCE SURVEILLANCE ACT, NATIONAL SECURITY LETTERS AND THE BANK SECRECY ACT**

### **I. OVERVIEW**

- § 10:1 Overview
- § 10:2 FISA and sovereign immunity
- § 10:3 Private sector immunity under FISA
- § 10:4 Clapper and Article III
- § 10:5 Metadata cases

### **II. FISA**

#### **A. ELECTRONIC SURVEILLANCE**

- § 10:6 Key definitions

INFORMATION SECURITY AND PRIVACY

- § 10:7 Electronic surveillance authorization without court order
- § 10:8 Designation of judges
- § 10:9 Court of review; record, transmittal to Supreme Court
- § 10:10 Expeditious conduct of proceedings; security measures for maintenance of records
- § 10:11 Tenure of judges
- § 10:12 Jurisdiction and procedures for review of petitions
- § 10:13 Stay of order
- § 10:14 Establishment and transmittal of rules and procedures
- § 10:15 Compliance with orders, rules, and procedures
- § 10:16 Amicus curiae—Designation
- § 10:17 —Qualifications
- § 10:18 —Duties
- § 10:19 —Assistance
- § 10:20 —Access to information
- § 10:21 —Notification
- § 10:22 —Assistance of executive branch
- § 10:23 —Administration
- § 10:24 —Receipt of information
- § 10:25 —Compensation
- § 10:26 Review of FISA court decisions
- § 10:27 Review of FISA court of review decisions
- § 10:28 Applications for court orders—Submission by Federal officer; approval of Attorney General; contents
- § 10:29 —Additional affidavits or certifications
- § 10:30 —Additional information
- § 10:31 —Personal review by Attorney General
- § 10:32 Issuance of order—Necessary findings
- § 10:33 —Determination of probable cause
- § 10:34 —Specifications and directions of orders
- § 10:35 —Special directions for certain orders
- § 10:36 —Duration of order; extensions; review of circumstances under which information was acquired, retained or disseminated
- § 10:37 —Emergency orders
- § 10:38 —Emergencies involving non-United States persons
- § 10:39 —Testing of electronic equipment; discovering unauthorized electronic surveillance; training of intelligence personnel
- § 10:40 —Retention of certifications, applications and orders
- § 10:41 —Bar to legal action
- § 10:42 —Pen registers and trap and trace devices

## TABLE OF CONTENTS

- § 10:43 Use of information—Compliance with minimization procedures; privileged communications; lawful purposes
- § 10:44 —Statement for disclosure
- § 10:45 —Notification by United States
- § 10:46 —Notification by States or political subdivisions
- § 10:47 —Motion to suppress
- § 10:48 —In camera and ex parte review by district court
- § 10:49 —Suppression of evidence; denial of motion
- § 10:50 —Finality of orders
- § 10:51 —Destruction of unintentionally acquired information
- § 10:52 —Notification of emergency employment of electronic surveillance; contents; postponement, suspension or elimination
- § 10:53 —Coordination with law enforcement on national security matters
- § 10:54 Report of electronic surveillance—Report to Administrative Office of the United States Court and to Congress
- § 10:55 Report of Attorney General to Congressional committees; limitation on authority or responsibility of information gathering activities of Congressional committees; report of Congressional committees to Congress
- § 10:56 Criminal sanctions
- § 10:57 Civil liability
- § 10:58 Authorization during time of war
- § 10:59 Statement of exclusive means by which electronic surveillance and interception of certain communications may be conducted
- § 10:60 Procedures for the retention of incidentally acquired communications—Requirement to adopt procedures
- § 10:61 —Coordination and approval
- § 10:62 —Application Procedures
- § 10:63 —Limitation on retention

## B. PHYSICAL SEARCHES

- § 10:64 Authorization of physical searches for foreign intelligence purposes
- § 10:65 Application for order; authorization
- § 10:66 Jurisdiction of Foreign Intelligence Surveillance Court
- § 10:67 Court of review; record; transmittal to Supreme Court
- § 10:68 Expeditious conduct of proceedings; security measures for maintenance of records

## INFORMATION SECURITY AND PRIVACY

- § 10:69 Application for order—Submission by Federal officer; approval of Attorney General; contents
- § 10:70 —Additional affidavits or certifications
- § 10:71 —Additional information
- § 10:72 —Personal review by Attorney General
- § 10:73 Issuance of order—Necessary findings
- § 10:74 —Determination of probable cause
- § 10:75 —Specifications and directions of orders
- § 10:76 —Duration of order; extensions; assessment of compliance
- § 10:77 —Emergency orders
- § 10:78 —Retention of applications and orders
- § 10:79 Use of information—Compliance with minimization procedures; lawful purposes
- § 10:80 —Notice of search and identification of property seized, altered, or reproduced
- § 10:81 —Statement for disclosure
- § 10:82 —Notification by United States
- § 10:83 —Notification by States or political subdivisions
- § 10:84 —Motion to suppress
- § 10:85 —In camera and ex parte review by district court
- § 10:86 —Suppression of evidence; denial of motion
- § 10:87 —Finality of orders
- § 10:88 —Notification of emergency execution of physical search; contents; postponement, suspension, or elimination
- § 10:89 —Coordination with law enforcement on national security matters
- § 10:90 Congressional oversight
- § 10:91 Prohibited activities
- § 10:92 Civil liability
- § 10:93 Authorization during time of war

### C. PEN REGISTERS AND TRAP AND TRACE DEVICES FOR FOREIGN INTELLIGENCE PURPOSES

- § 10:94 Application for authorization or approval of pen registers and trap and trace devices
- § 10:95 Form of application; recipient
- § 10:96 Executive approval; contents of application
- § 10:97 Ex parte judicial order of approval
- § 10:98 Time limitation
- § 10:99 Cause of action barred
- § 10:100 Furnishing of results

## TABLE OF CONTENTS

- § 10:101 Privacy procedures
- § 10:102 Authorization during emergencies—Requirements for authorization
- § 10:103 —Determination of emergency and factual basis
- § 10:104 —Effect of absence of order
- § 10:105 —Privacy procedures
- § 10:106 Authorization during time of war
- § 10:107 Use of information
- § 10:108 Notification of intended disclosure by United States
- § 10:109 Notification of intended disclosure by State or political subdivision
- § 10:110 Motion to suppress
- § 10:111 In camera and ex parte review
- § 10:112 Effect of determination of lawfulness
- § 10:113 Binding final orders
- § 10:114 Congressional oversight

### D. ACCESS TO CERTAIN BUSINESS RECORDS FOR FOREIGN INTELLIGENCE AND INTERNATIONAL TERRORISM INVESTIGATIONS

- § 10:115 Application for order; conduct of investigation generally
- § 10:116 Recipient and contents of application
- § 10:117 Ex parte judicial order of approval
- § 10:118 Nondisclosure
- § 10:119 Liability for good faith disclosure; waiver
- § 10:120 Judicial review of FISA orders
- § 10:121 Minimization procedures
- § 10:122 Use of information
- § 10:123 Emergency authority for production of tangible things
- § 10:124 Compensation
- § 10:125 Congressional oversight
- § 10:126 Notification of changes to retention of call detail record policies

### E. OVERSIGHT

- § 10:127 Semiannual report of the Attorney General
- § 10:128 —Submissions to Congress
- § 10:129 —Protection of national security
- § 10:130 Declassification of significant decisions, orders, and opinions

INFORMATION SECURITY AND PRIVACY

- § 10:131 Annual reports—Report by Director of the  
Administrative Office of the United States Courts
- § 10:132 —Mandatory reporting by Director of National  
Intelligence
- § 10:133 —Timing
- § 10:134 —Exceptions
- § 10:135 — —Certification
- § 10:136 Public reporting by persons subject to orders

F. ADDITIONAL PROCEDURES REGARDING  
CERTAIN PERSONS OUTSIDE THE UNITED  
STATES

1. Procedures for targeting certain persons  
outside the United States other than United  
States persons

- § 10:137 Authorization and limitations
- § 10:138 Reporting of material breach
- § 10:139 Congressional Review and Oversight of Abouls  
Collection
- § 10:140 —Exception for emergency acquisitions
- § 10:141 Amicus amendments in 2017
- § 10:142 Conduct of acquisition
- § 10:143 Timing of determination
- § 10:144 Construction
- § 10:145 Targeting procedures
- § 10:146 Minimization procedures
- § 10:147 Queries—Procedures required
- § 10:148 —Access to results of certain queries conducted by  
the FBI
- § 10:149 Guidelines for compliance with limitations
- § 10:150 Certification
- § 10:151 Directives and compensation
- § 10:152 Release from liability
- § 10:153 Challenging directives
- § 10:154 Enforcement of directives
- § 10:155 Appeals
- § 10:156 Judicial review of certifications and procedures—  
Review by the FISC
- § 10:157 —Orders
- § 10:158 —Appeal to the Court of Review
- § 10:159 —Certiorari to the Supreme Court
- § 10:160 —Reauthorization of authorizations in effect
- § 10:161 —Reauthorization of orders, authorizations, and  
directives



## TABLE OF CONTENTS

§ 10:162	Judicial proceedings
§ 10:163	Maintenance and security of records and proceedings
§ 10:164	Assessments, reviews, and reporting—Semiannual assessment
§ 10:165	—Agency assessment
§ 10:166	—Annual review
2. Certain acquisitions inside the United States targeting United States persons outside the United States	
§ 10:167	Jurisdiction of FISA court
§ 10:168	Application and order
§ 10:169	Review and limitations on review
§ 10:170	Directives
§ 10:171	Duration
§ 10:172	Emergency authorization
§ 10:173	Release from liability
§ 10:174	Appeal
§ 10:175	Construction
3. Other acquisitions targeting United States persons outside the United States	
§ 10:176	Jurisdiction and scope
§ 10:177	Orders by the FISC
§ 10:178	Emergency authorization
§ 10:179	Appeals
4. Joint applications and concurrent applications	
§ 10:180	Joint applications and orders
§ 10:181	Emergency authorization
5. Use of information under this subchapter	
§ 10:182	Use of information acquired under section 1881a
§ 10:183	Use of information acquired under section 1881b
6. Congressional oversight	
§ 10:184	Semiannual report
7. Savings provisions	
§ 10:185	Savings provision
G. PROTECTION FOR PERSONS ASSISTING THE GOVERNMENT	
§ 10:186	Procedures for implementing statutory defenses

## INFORMATION SECURITY AND PRIVACY

- § 10:187 Preemption
- § 10:188 Reporting
- § 10:189 FISA rules of procedure
- § 10:190 —Scope of rules
- § 10:191 —Amendment
- § 10:192 —National security information
- § 10:193 —Structure
- § 10:194 —Authority of the judges
- § 10:195 —Means of requesting relief from the court
- § 10:196 — —Filing applications, certifications, petitions,  
motions, or other papers
- § 10:197 — —Service
- § 10:198 — —Time and manner of submission of applications
- § 10:199 — —Computation of time
- § 10:200 —Notice and briefing of novel issues
- § 10:201 —Submission of targeting and minimization  
procedures
- § 10:202 —Correction of misstatement or omission; disclosure  
of noncompliance
- § 10:203 —Motion to amend court orders
- § 10:204 —Sequestration
- § 10:205 —Returns
- § 10:206 —Hearings
- § 10:207 —Court orders
- § 10:208 —Enforcement of order
- § 10:209 —Supplemental procedures for proceedings under 50  
U.S.C. § 1881a(h)—Scope
- § 10:210 — —Petition to modify or set aside a directive
- § 10:211 — —Petition to compel compliance with a directive
- § 10:212 — —Contents of petition
- § 10:213 — —Response
- § 10:214 — —Length of petition and response; other papers
- § 10:215 — —Notification of presiding judge
- § 10:216 — —Assignment
- § 10:217 — —Review of petition to modify or set aside a  
directive
- § 10:218 — —Review of petition to compel compliance  
pursuant to 50 U.S.C.A. § 1881a(h)(5)(C)
- § 10:219 — —*In camera* review
- § 10:220 — —Appeal
- § 10:221 —Supplemental procedures for proceedings under 50  
U.S.C. § 1861(f)—Scope
- § 10:222 — —Petition challenging production or  
nondisclosure order
- § 10:223 — —Contents of petition

## TABLE OF CONTENTS

§ 10:224	— —Length of petition
§ 10:225	— —Request to stay production
§ 10:226	— —Notification of presiding judge
§ 10:227	— —Assignment
§ 10:228	— —Initial review
§ 10:229	— —Response to petition; other papers
§ 10:230	— —Rulings on nonfrivolous petitions
§ 10:231	— —Failure to comply
§ 10:232	— — <i>In camera</i> review
§ 10:233	— —Appeal
§ 10:234	— En banc proceedings—Standard for hearing or rehearing en banc
§ 10:235	— —Initial hearing en banc on request of a party
§ 10:236	— —Rehearing en banc on petition by a party
§ 10:237	— —Circulation of en banc petitions and responses
§ 10:238	— —Court-initiated en banc proceedings
§ 10:239	— —Polling
§ 10:240	— —Stay pending en banc review
§ 10:241	— —Supplemental briefing
§ 10:242	— —Order granting or denying en banc review
§ 10:243	— Appeals—How taken
§ 10:244	— —When taken
§ 10:245	— —Stay pending appeal
§ 10:246	— —Motion to transmit the record
§ 10:247	— —Transmitting the record
§ 10:248	— —Oral notification to the court of review
§ 10:249	— Administrative provisions—Duties of the clerk
§ 10:250	— —Office hours
§ 10:251	— —Release of court records
§ 10:252	— —Practice before court

## III. BANK SECRECY ACT

§ 10:253	Bank Secrecy Act—Reports on domestic coins and currency transactions
§ 10:254	Requirements placed upon the secretary
§ 10:255	Mandatory exemptions from reporting requirements
§ 10:256	Discretionary exemptions
§ 10:257	Records and reports on certain foreign transactions
§ 10:258	Reports on foreign currency transactions
§ 10:259	Reports on exporting and importing monetary instruments
§ 10:260	Search and forfeiture of monetary instruments
§ 10:261	Additional remedies
§ 10:262	Other powers of the Secretary

## INFORMATION SECURITY AND PRIVACY

- § 10:263 Reporting of suspicious transactions
- § 10:264 Liability for disclosures
- § 10:265 Anti-money laundering programs
- § 10:266 Concentration accounts
- § 10:267 Private banking restrictions
- § 10:268 Prohibition on United States correspondent accounts with foreign shell banks
- § 10:269 Reporting of certain cross-border transmittals for funds
- § 10:270 Special restrictions in light of primary money laundering concerns
- § 10:271 Classified information
- § 10:272 Availability of reports and requests for injunctive relief
- § 10:273 Civil enforcement
- § 10:274 Negligent violations
- § 10:275 Criminal penalties
- § 10:276 Rewards for informants
- § 10:277 Restrictions on structuring transactions
- § 10:278 Identification requirements for the purchase of certain monetary instruments
- § 10:279 Records of certain domestic coin and currency transactions
- § 10:280 Customer reports
- § 10:281 Whistleblower protections
- § 10:282 Registration of money transmitting businesses
- § 10:283 Civil enforcement
- § 10:284 Reports relating to coins and currency received in nonfinancial trade or business
- § 10:285 Exceptions
- § 10:286 Bulk cash smuggling into or out of the United States

## IV. OVERVIEW OF SURVEILLANCE IN THE UNITED STATES

- § 10:287 Understanding the executive's authority
- § 10:288 Deconflicting presidential power
- § 10:289 The sources of the President's authority
- § 10:290 The Fourth Amendment and the history of domestic versus foreign intelligence and warrantless wiretaps
- § 10:291 The Fourth Amendment applied
- § 10:292 The Leon warrant exception and wiretap warrants
- § 10:293 Executive order 12333 and surveillance pre- and post-9/11

## TABLE OF CONTENTS

§ 10:294	The National Security Council and the Director of National Intelligence
§ 10:295	Duties of the intelligence community
§ 10:296	Conduct of intelligence activities
§ 10:297	Collection techniques
§ 10:298	Attorney General approval for the FBI
§ 10:299	Pre-9/11 surveillance by the NSA
§ 10:300	The President's surveillance program
§ 10:301	Presidential Policy Directive 28 (PPD-28)
§ 10:302	Electronic Communications Privacy Act (ECPA)
§ 10:303	Obtaining subscriber information
§ 10:304	Warshak and Section 2703(b)
§ 10:305	Section 2703(d) orders
§ 10:306	The Foreign Intelligence Surveillance Act—An overview
§ 10:307	What and who does FISA cover?
§ 10:308	Electronic surveillance under FISA
§ 10:309	FISA—Electronic surveillance authorization without court order
§ 10:310	—Surveillance with a court order
§ 10:311	FISA Section 215/50 U.S.C. Section 1861
§ 10:312	FISA Section 702/50 USC Section 1881a
§ 10:313	FISA Section 702 certification
§ 10:314	Recipients of directives and rights of challenge

## **CHAPTER 11. CONTROLLING THE ASSAULT OF NON-SOLICITED PORNOGRAPHY AND MARKETING ACT (CAN-SPAM)**

§ 11:1	Overview
§ 11:2	Defining an Internet access provider CAN-SPAM
§ 11:3	Primary purpose
§ 11:4	CAN-SPAM rules
§ 11:5	—Prohibition on charging a fee or placing other requirements on recipients who wish to opt out
§ 11:6	—Sexually oriented emails and labeling
§ 11:7	Defining senders of email
§ 11:8	Affiliate issues and defining a “sender”
§ 11:9	Affiliates and “intent” for “senders”
§ 11:10	Other vicarious liability holdings
§ 11:11	Purchase of leads and liability
§ 11:12	“Procuring” emails, conscious avoidance, and knowledge
§ 11:13	Header and subject line information

- § 11:14 Use of other names in the header of an email
- § 11:15 Requirements of commercial emails
- § 11:16 What is “clear and conspicuous?”
- § 11:17 Other labeling concerns
- § 11:18 Adult-oriented emails
- § 11:19 Liability for violation of adult labeling rule by affiliates
- § 11:20 Opt-out requests
- § 11:21 Role of affirmative consent
- § 11:22 Actual harm requirement
- § 11:23 Email a friend issues
- § 11:24 No misrepresentation in emails
- § 11:25 Spam as a defense to criminal charges
- § 11:26 CAN-SPAM and mitigation defenses
- § 11:27 Standing to sue and enforcement
- § 11:28 Do-not-email list
- § 11:29 Inapplicability of header restrictions to statements in body of email
- § 11:30 Other vicarious liability issues
- § 11:31 Mere advertising insufficient to establish liability
- § 11:32 Registration of email accounts
- § 11:33 Automated scripts
- § 11:34 Restrictions upon wireless messaging
- § 11:35 Form of authorization
- § 11:36 Additional restrictions upon CMRS providers
- § 11:37 Penalties and damages
- § 11:38 Pleading CAN-SPAM violations with particularity
- § 11:39 Assignment of claims
- § 11:40 Preemption
- § 11:41 Specificity requirements
- § 11:42 Seeking out spam as a defense

## **CHAPTER 12. STATE E-MAIL LAWS**

- § 12:1 Generally
- § 12:2 Apparent authority and emails

### **A. ALASKA**

- § 12:3 Overview

### **B. ARIZONA**

- § 12:4 Overview
- § 12:5 Damages and enforcement

### **C. ARKANSAS**

- § 12:6 Overview

## TABLE OF CONTENTS

- § 12:7 Damages and enforcement
- § 12:8 Additional electronic mail restrictions

## D. CALIFORNIA

- § 12:9 Commercial email law
- § 12:10 —Prohibited conduct
- § 12:11 —Unlawful activities related to advertising
- § 12:12 —Persons permitted to bring and enforcement action for violation of Section 17529.5
- § 12:13 —Impact of the body of an email on header claims and allegedly misleading subject lines
- § 12:14 —Defining a bona fide ISP
- § 12:15 —Procuring an email under California law
- § 12:15.1 —Defining who is an advertiser and pleading requirements of state law
- § 12:16 —Remedies generally
- § 12:17 —E-mails sent pursuant to a preexisting or current business relationship
- § 12:18 —California’s spam law and mitigation of damages
- § 12:19 —Falsified headers under California law
- § 12:20 —Preemption of commercial email laws
- § 12:21 Restrictions on text message advertisements
- § 12:22 Electronic mail service providers—Termination of electronic mail service
- § 12:23 —Policies regarding unsolicited electronic mail advertisements
- § 12:24 — —Enforcement
- § 12:25 —Restrictions on other laws
- § 12:26 Fraudulent misrepresentation under California law

## E. COLORADO

- § 12:27 Spam law
- § 12:28 Civil immunity
- § 12:29 Immunity for transmission
- § 12:30 Application of law
- § 12:31 Legislative findings
- § 12:32 Electronic mail fraud
- § 12:33 Repeal of other laws
- § 12:34 Effective date
- § 12:35 Prior laws

## F. CONNECTICUT

- § 12:36 Overview

§ 12:37 Damages and enforcement

§ 12:38 Do-not-email

## **G. DELAWARE**

§ 12:39 Overview

§ 12:40 Damages and enforcement

## **H. FLORIDA**

§ 12:41 Commercial email law

§ 12:42 Enforcement

## **I. GEORGIA**

§ 12:43 Commercial email law

§ 12:44 Civil enforcement

## **J. IDAHO**

§ 12:45 Overview

§ 12:46 Damages and enforcement

## **K. ILLINOIS**

§ 12:47 Overview

§ 12:48 Damages and enforcement

## **L. INDIANA**

§ 12:49 Overview

§ 12:50 Damages and enforcement

## **M. IOWA**

§ 12:51 Transmission of unsolicited bulk electronic mail

§ 12:52 Sale or offer of direct sale of prescription drugs

§ 12:53 Use of encryption

§ 12:54 Civil relief and forfeiture

## **N. KANSAS**

§ 12:55 Overview

§ 12:56 Damages and enforcement

## **O. LOUISIANA**

§ 12:57 Offenses against electronic mail service providers

§ 12:58 Commercial emails



## TABLE OF CONTENTS

§ 12:59 Civil enforcement

### **P. MAINE**

§ 12:60 Overview

§ 12:61 Damages and enforcement

### **Q. MARYLAND**

§ 12:62 Overview

§ 12:63 Damages and enforcement

### **R. MASSACHUSETTS**

§ 12:64 Overview

### **S. MICHIGAN**

§ 12:65 Overview

§ 12:66 Misuse of domain names

§ 12:67 Restrictions on software

§ 12:68 Immunity for service providers

§ 12:69 Enforcement

§ 12:70 Child protection registry

§ 12:71 Restrictions upon emails

§ 12:72 Restrictions upon disclosure of registry information

§ 12:73 Child registry law

§ 12:74 Forfeiture and enhancements

§ 12:75 Criminal enforcement

§ 12:76 Civil enforcement

### **T. MINNESOTA**

§ 12:77 Overview

§ 12:78 Damages and enforcement

### **U. MISSOURI**

§ 12:79 Overview

§ 12:80 Blocking by an interactive computer service

§ 12:81 Damages and enforcement

### **V. NEVADA**

§ 12:82 Overview

§ 12:83 Damages and enforcement

### **W. NEW MEXICO**

§ 12:84 Overview

§ 12:85 Damages and enforcement

## **X. NEW YORK**

§ 12:86 Overview

## **Y. NORTH CAROLINA**

§ 12:87 Overview

§ 12:88 Damages and enforcement

§ 12:89 Civil action

## **Z. NORTH DAKOTA**

§ 12:90 Overview

§ 12:91 Immunity for interactive computer services

§ 12:92 Fraudulent or misleading communications

§ 12:93 Preemption

§ 12:94 Damages and enforcement

## **AA. OHIO**

§ 12:95 Overview

§ 12:96 Damages and enforcement

§ 12:97 Liability under Ohio's law

## **BB. OKLAHOMA**

§ 12:98 Overview

§ 12:99 Damages and enforcement

## **CC. OREGON**

§ 12:100 Overview

§ 12:101 Damages and enforcement

## **DD. PENNSYLVANIA**

§ 12:102 Overview

§ 12:103 Damages and enforcement

## **EE. RHODE ISLAND**

§ 12:104 Overview

§ 12:105 Damages and enforcement

## **FF. SOUTH DAKOTA**

§ 12:106 Spam law

## TABLE OF CONTENTS

- § 12:107 Exemptions for ISPs
- § 12:108 Restrictions on collection of email addresses
- § 12:109 Collection of email addresses through automated means
- § 12:110 Civil enforcement
- § 12:111 Additional restrictions on spam
- § 12:112 Additional restrictions on commercial email

## GG. TENNESSEE

- § 12:113 Overview
- § 12:114 Damages and enforcement

## HH. TEXAS

- § 12:115 Transmission of certain commercial electronic mail messages prohibited
- § 12:116 Requirement for transmission of unsolicited commercial electronic mail messages
- § 12:117 Selling or providing certain electronic mail addresses prohibited
- § 12:118 Transmission of message containing obscene material or material depicting sexual conduct; criminal penalty
- § 12:119 Violation of chapter: general civil penalty and injunctive relief
- § 12:120 Violation of chapter: deceptive trade practice
- § 12:121 Violation of chapter: civil action for damages
- § 12:122 Alternative recovery for persons other than electronic mail service providers
- § 12:123 Alternative recovery for electronic mail service providers
- § 12:124 Required notice of civil action to attorney general; civil penalty
- § 12:125 Intervention in civil action by attorney general
- § 12:126 Certification as class action prohibited
- § 12:127 Protection of secrecy or security
- § 12:128 Immunity from liability: commercial electronic mail message transmitted by error or accident
- § 12:129 Immunity from liability: telecommunications utilities and electronic mail service providers
- § 12:130 Qualified immunity from liability of senders
- § 12:131 Authority to block certain commercial electronic mail messages; qualified immunity

## II. UTAH

- § 12:132 Child protection registry

§ 12:133 Criminal remedies

## **JJ. VIRGINIA**

§ 12:134 Overview

§ 12:135 Damages and enforcement

§ 12:136 Constitutionality of Virginia's antispam law

## **KK. WASHINGTON**

§ 12:137 Unpermitted or misleading electronic mail

§ 12:138 Enforcement

§ 12:139 Blocking of emails by an ISP

§ 12:140 Commercial electronic text message

§ 12:141 Violation of this law is a deceptive trade practice

§ 12:142 Enforcement and damages

§ 12:143 Preemption of Washington's spam law

## **LL. WEST VIRGINIA**

§ 12:144 Overview

§ 12:145 Damages and enforcement

## **MM. WISCONSIN**

§ 12:146 Overview

## **NN. WYOMING**

§ 12:147 Overview

§ 12:148 Damages and enforcement

# **CHAPTER 13. SPYWARE AND PHISHING**

## **I. OVERVIEW**

§ 13:1 Introduction

§ 13:2 Spyware, phishing, and pharming defined

§ 13:3 Federal Trade Commission and spyware

§ 13:4 Spyware litigation

§ 13:5 Federal Deposit Insurance Corporation guidance on spyware

## **II. SPECIFIC STATE PROVISIONS**

### **A. ALASKA**

§ 13:6 Overview

## TABLE OF CONTENTS

### B. ARIZONA

- § 13:7 Modification of Internet settings
- § 13:8 Computer spyware—Generally prohibited activities
- § 13:9 Collection of personally identifiable information
- § 13:10 Blocking of software installation
- § 13:11 Taking control of another’s computer
- § 13:12 Modifying settings
- § 13:13 Inducing installation of software
- § 13:14 Exemptions
- § 13:15 Civil enforcement

### C. ARKANSAS

- § 13:16 Spyware
- § 13:17 Prohibited conduct
- § 13:18 Exceptions for ISPs and authorized software upgrades
- § 13:19 Enforcement
- § 13:20 Phishing
- § 13:21 Spyware monitoring fund

### D. CALIFORNIA

- § 13:22 Consumer Protection Against Computer Spyware Act
- § 13:23 Prevention of blocking of software installation
- § 13:24 Other prohibited conduct
- § 13:25 Anti-Phishing Act of 2005
- § 13:26 Enforcement

### E. GEORGIA

- § 13:27 The Georgia Computer Security Act of 2005
- § 13:28 Regulations on the installation of software
- § 13:29 Modification of Internet settings
- § 13:30 Preventing software blocks
- § 13:31 Inducement of software installation
- § 13:32 Criminal penalties for violations
- § 13:33 Attorney General actions
- § 13:34 Actions by ISPs
- § 13:35 Exceptions to liability
- § 13:36 Inapplicability to ISPs
- § 13:37 Phishing
- § 13:38 Exemptions from liability

F. HAWAII

- § 13:39 Overview

G. ILLINOIS

- § 13:40 Anti-Phishing Act
- § 13:41 Enforcement

H. INDIANA

- § 13:42 Prohibited conduct
- § 13:43 Gathering of personal information
- § 13:44 Blocking or disabling of software
- § 13:45 Taking control of a computer
- § 13:46 Modification of computer settings
- § 13:47 Inducing installation of software
- § 13:48 Exemptions
- § 13:49 Civil enforcement

I. IOWA

- § 13:50 Overview of spyware statute
- § 13:51 Modification of Internet settings
- § 13:52 Restrictions on collection of personally identifiable information
- § 13:53 Disabling or installing software
- § 13:54 Taking control of a computer
- § 13:55 Modifying Internet settings
- § 13:56 Other restrictions
- § 13:57 Exceptions for ISPs
- § 13:58 Criminal penalties

J. LOUISIANA

- § 13:59 Spyware

K. MARYLAND

- § 13:60 Phishing

L. NEW HAMPSHIRE

- § 13:61 Spyware defined
- § 13:62 Taking control of a user's computer
- § 13:63 Modifying Internet settings
- § 13:64 Collection of personal information
- § 13:65 Blocking of software

## TABLE OF CONTENTS

- § 13:66 Other violations
- § 13:67 Exemptions
- § 13:68 Enforcement

### M. NEW YORK

- § 13:69 Phishing
- § 13:70 Spyware and clickwrap

### N. TENNESSEE

- § 13:71 Anti-Phishing Act
- § 13:72 Unlawful conduct
- § 13:73 Civil enforcement
- § 13:74 Exemptions

### O. UTAH

- § 13:75 The Utah E-commerce Integrity Act
- § 13:76 Phishing and pharming
- § 13:77 Removal of domain name or content—Liability
- § 13:78 Application of law
- § 13:79 Preemption
- § 13:80 Prohibition on the use of software—Spyware
- § 13:81 Other prohibited conduct
- § 13:82 Exceptions
- § 13:83 Enforcement

### P. WASHINGTON

- § 13:84 Antiphishing
- § 13:85 Spyware—Installation or removal of software
- § 13:86 —Collection of personally identifiable information
- § 13:87 —Blocking installation or execution of software
- § 13:88 —Misrepresenting software
- § 13:89 —Exemptions
- § 13:90 —Civil enforcement

## Volume 2

## CHAPTER 14. RESTRICTIONS ON TELEPHONES

### I. OVERVIEW

- § 14:1 Telephone regulation introduction

## II. FEDERAL LAWS

- § 14:2 Telecommunications Act of 1996
- § 14:3 Confidentiality of carrier information
- § 14:4 Customer proprietary network information
- § 14:5 Exceptions to privacy restrictions
- § 14:6 Disclosure of subscriber list information
- § 14:7 Wireless location information
- § 14:8 Disclosure of information in connection with  
emergency services
- § 14:9 Private right of action under the Telecommunications  
Act of 1996
- § 14:10 Telephone record regulations
- § 14:11 Use of customer proprietary network information  
without customer approval
- § 14:12 Approval required for use of customer proprietary  
network information
- § 14:13 Use of opt-out and opt-in approval process
- § 14:14 Notice for use of customer proprietary network  
information
- § 14:15 Notice requirements for opt outs
- § 14:16 Additional burdens on email notice
- § 14:17 Notice requirements for opt-in requests
- § 14:18 Notice requirements for one-time use of CPNI
- § 14:19 Safeguards on use of CPNI
- § 14:20 Compliance statements
- § 14:21 Notices to the commission regarding opt outs
- § 14:22 Safeguards on the disclosure of CPNI—Password  
requirements
- § 14:23 —General requirements
- § 14:24 —Telephone access
- § 14:25 —Online access
- § 14:26 —In-store access
- § 14:27 —Notification of account changes
- § 14:28 —Business customer exception
- § 14:29 Notification of CPNI security breaches
- § 14:30 —What is a breach?
- § 14:31 —Notice requirements
- § 14:32 —Preemption
- § 14:33 Federal Do-Not-Call law
- § 14:34 Exception for the Health Insurance Portability and  
Accountability Act (HIPAA)
- § 14:35 TCPA and Pharmacy Benefit Managers
- § 14:36 Federal Do-Not-Call law—Defenses
- § 14:37 —Calling times



## TABLE OF CONTENTS

§ 14:38	—Required disclosures
§ 14:39	— —Charitable solicitations
§ 14:40	— —Recordkeeping requirements
§ 14:41	TCPA’s application to SMS
§ 14:42	Text messaging and stop message
§ 14:43	When are faxes advertisements
§ 14:44	Auto-dialer and facsimile restrictions
§ 14:45	Auto-dialer litigation
§ 14:46	Artificial or prerecorded messages
§ 14:47	Improper initiation of telephone solicitations
§ 14:48	Exemptions
§ 14:49	Additional requirements
§ 14:50	Additional auto-dialer issues
§ 14:51	TCPA and debt collection
§ 14:52	TCPA and providing phone numbers
§ 14:53	FCC TCPA Declaratory Ruling and Order in 2015
§ 14:54	—Consent—A summary
§ 14:55	—What is an auto-dialer
§ 14:56	—Who initiates or makes a “call”
§ 14:57	—Application of the Autodialer ruling
§ 14:58	—Application to SMS
§ 14:59	—Application to internet-to-phone text messages
§ 14:60	—Exemption of certain proconsumer messages
§ 14:61	In the Matter of AT&T Services, Inc.
§ 14:62	Federal Do-Not-Fax law
§ 14:63	Do-Not-Fax—The established business relationship in the business context
§ 14:64	Federal Do-Not-Fax law—Opt-outs
§ 14:65	Application to efaxes
§ 14:66	Faxes promoting job placement services are advertisements
§ 14:67	Auto-dialers and established business relationship
§ 14:68	TCPA and commercial definition
§ 14:69	Communications Assistance for Law Enforcement Act and broadband access and VoIP
§ 14:70	Slamming
§ 14:71	Instant messaging and SMS technology
§ 14:72	Secondary liability
§ 14:73	Vicarious liability for lead generation and the TCPA
§ 14:74	Revocation of consent under TCPA
§ 14:75	TCPA and broadcasts
§ 14:76	Smartphones and the TCPA

## III. STATE SPECIFIC LAWS

### A. CALIFORNIA

§ 14:77	Do-Not-Call law
---------	-----------------

## INFORMATION SECURITY AND PRIVACY

- § 14:78 Telephone solicitor law
- § 14:79 Exceptions
- § 14:80 Exception for express written permission
- § 14:81 Sale of lists
- § 14:82 Enforcement
- § 14:83 Solicitation of sales through the mail
- § 14:84 Civil enforcement
- § 14:85 Telephonic seller law—Defining a “telephonic seller”
- § 14:86 —Burden of proof
- § 14:87 —Requirements for telephonic sellers
- § 14:88 —Contents of filings
- § 14:89 —Filings related to exemptions
- § 14:90 —Disclosures regarding loans
- § 14:91 —Additional requirements
- § 14:92 —Irrevocable consent
- § 14:93 —No representations
- § 14:94 —Soliciting prospective purchasers on behalf of  
unregistered telephonic sellers
- § 14:95 —Enforcement
- § 14:96 —Bond requirement
- § 14:97 Restrictions on telephone, Internet, mail order, or  
catalog sales or leases
- § 14:98 —Requirements of open-end credit plans
- § 14:99 —Other restrictions
- § 14:100 —Exceptions
- § 14:101 Do-Not-Fax law
- § 14:102 —Preemption

### B. COLORADO

- § 14:103 Telecommunications crime
- § 14:104 —Civil enforcement
- § 14:105 Unlawful use of information
- § 14:106 Telephone lines and hostage situations
- § 14:107 Automated dialing systems

### C. CONNECTICUT

- § 14:108 Do-not-fax

### D. GEORGIA

- § 14:109 Telephone records privacy protection act
- § 14:110 Restrictions on telecommunications companies
- § 14:111 Directory restrictions

TABLE OF CONTENTS

**E. NEW MEXICO**

§ 14:112 Telephone laws

**F. PENNSYLVANIA**

§ 14:113 Publication of cell phone numbers

**G. WASHINGTON**

§ 14:114 Disclosure of cell phone numbers

**CHAPTER 15. PRETEXTING**

**I. OVERVIEW**

- § 15:1 Pretexting—In general
- § 15:2 Attorney liability for pretexting
- § 15:3 New regulations regarding pretexting
- § 15:4 Telephone Records and Privacy Act
- § 15:5 —Obtaining telephone records
- § 15:6 —Prohibitions on sales or transfers of records
- § 15:7 —Prohibition on purchase or receipt of confidential  
phone records
- § 15:8 —Enhanced penalties
- § 15:9 —Exceptions

**II. STATE PRETEXTING RESTRICTIONS**

**A. CALIFORNIA**

- § 15:10 Restrictions on pretexting
- § 15:11 Enforcement
- § 15:12 Exclusion from evidence
- § 15:13 Employer liability

**B. FLORIDA**

- § 15:14 Pretexting of telephone records
- § 15:15 Exemptions

**C. GEORGIA**

- § 15:16 Restrictions on release of telephone records
- § 15:17 Restrictions upon private investigators

**D. ILLINOIS**

- § 15:18 Pretexting

§ 15:19 Civil remedies for pretexting

**E. MARYLAND**

§ 15:20 Telephone Privacy Act of 2006

§ 15:21 Pretexting prohibitions

§ 15:22 Exemptions

§ 15:23 Criminal enforcement

§ 15:24 Civil enforcement

**F. MICHIGAN**

§ 15:25 Pretexting of telephone records

**G. MONTANA**

§ 15:26 Pretexting

**H. NEW YORK**

§ 15:27 Consumer communication records privacy act

§ 15:28 Pretexting of financial information

§ 15:29 Unauthorized disclosures by officers or employees

**I. NORTH CAROLINA**

§ 15:30 Pretexting

§ 15:31 Exceptions

§ 15:32 Enforcement

## **CHAPTER 16. FINANCIAL PRIVACY**

### **I. INTRODUCTION**

§ 16:1 Financial privacy and security in general

### **II. GRAMM-LEACH-BLILEY ACT**

§ 16:2 Application in general

§ 16:3 Statutory requirements of GLB

§ 16:4 Financial privacy rule

§ 16:5 Privacy of Consumer Financial Information

§ 16:6 Model privacy form and examples

§ 16:7 Initial privacy notice

§ 16:8 Annual privacy notice

§ 16:9 Information to be included in privacy notices

§ 16:10 Short-form initial notice with opt-out notice for  
noncustomers

## TABLE OF CONTENTS

§ 16:11	Form of opt-out notice to consumers; opt-out methods
§ 16:12	Joint relationships
§ 16:13	Revised privacy notices
§ 16:14	Delivering privacy and opt-out notices
§ 16:15	Retention or accessibility of notices for customers
§ 16:16	Limits on disclosure of nonpublic personal information to nonaffiliated third parties
§ 16:17	Limits on redisclosure and reuse of information
§ 16:18	Exception to opt-out requirements for service providers and joint marketing
§ 16:19	Exceptions to notice and opt-out requirements for processing and servicing transactions
§ 16:20	Other exceptions to notice and opt-out requirements
§ 16:21	Protection of FCRA
§ 16:22	Relation to State laws
§ 16:23	Model forms
§ 16:24	Federal Financial Institutions Examinations Council requirements
§ 16:25	Security provisions
§ 16:26	GLB and government disclosures
§ 16:27	Pretexting provisions
§ 16:28	Disclosure of class action discovery under GLB
§ 16:29	The interplay of GLB and FCRA
§ 16:30	The FCRA and the First Amendment

## III. FAIR CREDIT REPORTING ACT

§ 16:31	Overview of FCRA
§ 16:32	Misuse of credit reports and jurisdiction
§ 16:33	What do credit reporting agencies do?
§ 16:34	FCRA inapplicable to independent contractors
§ 16:35	Furnishing of consumer reports
§ 16:36	Protection of medical information
§ 16:37	Disclosures to governmental entities
§ 16:38	Disclosures to consumers
§ 16:39	Disclosures to governmental agencies for counterterrorism purposes
§ 16:40	Disclosure to the FBI
§ 16:41	Affiliate sharing
§ 16:42	Exclusions for individuals reporting “first hand” experience
§ 16:43	Defining what a “offer of credit is under FCRA”
§ 16:44	Identity theft
§ 16:45	Restrictions upon credit card receipts
§ 16:46	Electronic receipt and truncation of credit card numbers

## INFORMATION SECURITY AND PRIVACY

- § 16:47 Civil liability
- § 16:48 FCRA and litigation
- § 16:49 Being deterred from credit is not damage under the FCRA
- § 16:50 FCRA and online services
- § 16:51 Liability for dissemination of truthful information
- § 16:52 Recovery of emotional distress under the FCRA
- § 16:53 The FCRA and accurate reporting defenses under section 1681i(1)(a)
- § 16:54 Expert testimony regarding violations of the FCRA
- § 16:55 Regulations regarding medical information
- § 16:56 FACT Act rules on affiliate marketing
  - § 16:57 —Defining a “pre-existing” relationship
  - § 16:58 —Initial notice and opt-out requirements
  - § 16:59 —Who can provide notice
  - § 16:60 —Use of eligibility information from an affiliate
  - § 16:61 —Use of eligibility information by a service provider
  - § 16:62 —Writing requirements
  - § 16:63 —Exceptions to eligibility information regulations
  - § 16:64 —Scope and duration of opt out
  - § 16:65 —Notice following termination of all continuing relationships
  - § 16:66 —Contents of an opt-out notice
  - § 16:67 —Reasonable opportunity to opt out
  - § 16:68 —Reasonable and simple methods of opting out
  - § 16:69 —Delivery of opt-out notices
  - § 16:70 —Renewal of opt out
  - § 16:71 —Timing of renewal notice
  - § 16:72 —Effective date
- § 16:73 FACT Act regulations regarding address discrepancies
- § 16:74 FACT Act and red flag regulations
- § 16:75 Periodic identification of covered accounts
- § 16:76 Establish an identity theft prevention program
- § 16:77 Administration of the program
- § 16:78 Effective date
- § 16:79 The role of the guidelines in Appendix J
- § 16:80 Regulations on card issuers regarding changes of address
- § 16:81 Form of notice
- § 16:82 Regulations regarding medical information—Office of comptroller of currency regulations
- § 16:83 —Other FCRA regulations
- § 16:84 Administrative enforcement
- § 16:85 FCRA and preemption of state law claims

## TABLE OF CONTENTS

- § 16:86 Regulation S-P
- § 16:87 FCRA preemption and mortgage-trigger lists

## IV. RIGHT TO FINANCIAL PRIVACY

- § 16:88 General restrictions
- § 16:89 Exceptions permitting disclosure
- § 16:90 Nonidentifiable information and other exceptions
- § 16:91 Challenges by customers to disclosures
- § 16:92 Inapplicability of notice requirements when limited information is sought
- § 16:93 Transfer of records

## CHAPTER 17. STATE FINANCIAL PRIVACY LAWS

### I. INTRODUCTION

- § 17:1 State financial privacy laws, generally
- § 17:2 Understanding State FCRA and Investigative Consumer Reporting Agency (ICRA) laws

### II. STATE PRIVACY LAWS

#### A. ALABAMA

- § 17:3 Tax payor privilege

#### B. ARKANSAS

- § 17:4 Privacy of account information

#### C. CALIFORNIA

- § 17:5 Financial Information Privacy Act
- § 17:6 —Disclosures to nonaffiliated third parties
- § 17:7 —Disclosures to affiliates
- § 17:8 —Additional permitted disclosures
- § 17:9 —Remedies
- § 17:10 Consumer credit reports—Inspection rights
- § 17:11 —Exemptions
- § 17:12 —Furnishing consumer reports
- § 17:13 —Notification system
- § 17:14 —Reports to government agencies
- § 17:15 —Restrictions on certain forms of information
- § 17:16 —Open-end credit account
- § 17:17 —Medical information

## INFORMATION SECURITY AND PRIVACY

- § 17:18 —Child and spousal support information
- § 17:19 —Documents acting as liens or encumbrances
- § 17:20 —Procedures
- § 17:21 —Accuracy
- § 17:22 —Restrictions on nondisclosure requirements
- § 17:23 —Notices to suppliers of information
- § 17:24 —Supplying files and information
- § 17:25 —Credit scores and key factors
- § 17:26 —Credit scoring model
- § 17:27 —Fees
- § 17:28 —Statement of rights
- § 17:29 —Removal of names from credit card solicitation lists
- § 17:30 —Disputes regarding accuracy
- § 17:31 —Submission of police report
- § 17:32 —Waiver of disclosures of credit scores
- § 17:33 —Deletion of inquiries with respect to identity theft
- § 17:34 —Sale of consumer debt to debt collector
- § 17:35 —Consumer reporting agencies as resellers
- § 17:36 —Fees
- § 17:37 —Matters of public record
- § 17:38 —Civil penalties
- § 17:39 —Procedures to prevent use of data for marketing purposes
- § 17:40 Investigative consumer reports
- § 17:41 —Availability of report to consumer
- § 17:42 —Furnishing consumer reports
- § 17:43 —Reports to government agencies
- § 17:44 —Procurement or preparation of report
- § 17:45 —Exceptions
- § 17:46 —Prohibited information
- § 17:47 —Verification of information
- § 17:48 —Restrictions on personal interviews
- § 17:49 —Reporting and other procedures
- § 17:50 —Notice provided by investigative consumer reporting agency
- § 17:51 —Supplying files and information
- § 17:52 —Disputes regarding accuracy and completeness of files
- § 17:53 —Termination of reinvestigation
- § 17:54 —Rectification
- § 17:55 —Additional requirements on consumer reporting agencies under the FCRA
- § 17:56 —Fees
- § 17:57 —Public records
- § 17:58 —Notice of adverse action regarding insurance



## TABLE OF CONTENTS

§ 17:59 —Subsequent reports

### D. CONNECTICUT

§ 17:60 Banking law of Connecticut

§ 17:61 Disclosure for audits and tax reporting

§ 17:62 Disclosures pursuant to a warrant

§ 17:63 Other exceptions

§ 17:64 Enforcement

§ 17:65 Compliance with GLB

### E. DELAWARE

§ 17:66 Right to file a police report regarding identity theft

### F. GEORGIA

§ 17:67 Tax information

### G. HAWAII

§ 17:68 Employer's use of credit history

§ 17:69 Employer inquiries into conviction record

### H. ILLINOIS

§ 17:70 Public utility and credit restrictions

§ 17:71 Receipt of police reports

§ 17:72 Employer's use of credit information

§ 17:73 Retaliatory or discriminatory acts

§ 17:74 Waivers

§ 17:75 Enforcement

§ 17:76 Effect of FCRA

### I. KANSAS

§ 17:77 Payment card scanning

### J. LOUISIANA

§ 17:78 Disclosure of reports

§ 17:79 Fees

§ 17:80 Procedures

§ 17:81 Disputes regarding accuracy of information

§ 17:82 Copy of report after denial of credit

§ 17:83 Records of recipients

§ 17:84 Enforcement

§ 17:85 Dissemination of specific credit information

## INFORMATION SECURITY AND PRIVACY

- § 17:86 Disclosure of financial information
- § 17:87 Disclosures by banks
- § 17:88 Disclosure due to authorization
- § 17:89 Authorized disclosures
- § 17:90 Exemption from liability

### K. MARYLAND

- § 17:91 Employer's use of credit information
- § 17:92 Enforcement
- § 17:93 Exceptions
- § 17:94 Effective date

### L. MASSACHUSETTS

- § 17:95 Restrictions on consumer reports
- § 17:96 Consumer's decision to exclude name from consumer reporting agency list
- § 17:97 Notification systems
- § 17:98 Use of consumer reports in certain credit transactions
- § 17:99 Information that cannot be placed in a report
- § 17:100 Child support issues
- § 17:101 Investigative consumer reports
- § 17:102 Procedures to be maintained by consumer reporting agencies
- § 17:103 Procedures to ensure accuracy of information reported to consumer reporting agencies
- § 17:104 Disputed information
- § 17:105 Notice of closure of certain accounts
- § 17:106 Furnishing of information regarding delinquent accounts
- § 17:107 Liability for violations of furnishing of certain information
- § 17:108 Furnishing of information to governmental agencies
- § 17:109 Disclosures to consumers
- § 17:110 Procedures for disclosures
- § 17:111 Action related to procedures for disclosures
- § 17:112 Completeness or accuracy of information
- § 17:113 Charges for disclosures
- § 17:114 Reports for employment purposes
- § 17:115 Procedures for accurate reporting of public record information
- § 17:116 Adverse information
- § 17:117 Denial of credit or employment
- § 17:118 Pretexting

## TABLE OF CONTENTS

§ 17:119	Introducing false information into a reporting agency's files
§ 17:120	Providing unauthorized access
§ 17:121	Enforcement
§ 17:122	Restrictions on credit services organizations
§ 17:123	Required disclosures to buyers of credit services
§ 17:124	Requirements for contracts between a buyer and a credit services organization
§ 17:125	Liability for violation of credit services restrictions
§ 17:126	Employment restrictions
§ 17:127	Enforcement

## M. MINNESOTA

§ 17:128	Access to consumer reports
§ 17:129	Restrictions on the sale of certain information
§ 17:130	Disclosure and use of consumer reports for employment purposes
§ 17:131	Exceptions
§ 17:132	Notice of adverse action

## N. NEW MEXICO

§ 17:133	Disclosure of information to the public
§ 17:134	Correction to consumer bureau's reports
§ 17:135	Disclosure of information to governmental entities
§ 17:136	Disclosure of information to businesses, professions, and individuals
§ 17:137	Personnel reporting
§ 17:138	Limitations on information reports
§ 17:139	Civil enforcement
§ 17:140	Criminal enforcement

## O. NEW YORK

§ 17:141	Disclosure of reports
§ 17:142	Investigative consumer reports
§ 17:143	Disclosures to consumers
§ 17:144	Exception regarding disclosures
§ 17:145	Form and conditions of disclosure
§ 17:146	Procedures for resolving disputes
§ 17:147	Public record information
§ 17:148	Restrictions on investigative consumer reports
§ 17:149	Requirements on users of consumer reports
§ 17:150	Prohibited information
§ 17:151	Compliance procedures

## INFORMATION SECURITY AND PRIVACY

- § 17:152 Theft of identity
- § 17:153 Civil enforcement for willful noncompliance
- § 17:154 Civil enforcement for negligent noncompliance
- § 17:155 Limitations period
- § 17:156 Obtaining or introducing information under false pretenses
- § 17:157 Unauthorized disclosures by officers or employees
- § 17:158 Disclosure of medical information
- § 17:159 Disclosures to government agencies

## P. OREGON

- § 17:160 Employer's use of credit information
- § 17:161 Enforcement
- § 17:162 Regulation on credit history
- § 17:163 Enforcement

## Q. SOUTH CAROLINA

- § 17:164 Financial privacy
- § 17:165 Corrections to consumer reports

## R. TEXAS

- § 17:166 Permissible purposes for the furnishing of consumer reports
- § 17:167 Disclosure to the consumer by the user of a consumer report
- § 17:168 Use of Social Security numbers
- § 17:169 Disclosures by check verification services
- § 17:170 Disclosures by consumer reporting agencies
- § 17:171 Prohibited information
- § 17:172 Exceptions to prohibited information
- § 17:173 Medical information
- § 17:174 Dispute procedure
- § 17:175 Frivolous disputes
- § 17:176 Deletion of information that cannot be verified
- § 17:177 Procedures governing reinsertion of deleted information
- § 17:178 Correction of inaccurate information
- § 17:179 Consumer's right to file action in court or arbitrate disputes
- § 17:180 Arbitration actions
- § 17:181 Civil liability
- § 17:182 Enforcement by the Attorney General
- § 17:183 Deceptive trade practice

TABLE OF CONTENTS

§ 17:184 Venue

S. WASHINGTON

§ 17:185 Use of consumer reports

**CHAPTER 18. SECURITY FREEZE LAWS**

§ 18:1 Credit freezes generally

**A. ALASKA**

§ 18:2 Security freeze  
§ 18:3 Timing of freeze  
§ 18:4 Effect of freeze  
§ 18:5 Changes to information  
§ 18:6 Removal of freeze  
§ 18:7 Fees  
§ 18:8 Notices  
§ 18:9 Notice of violation  
§ 18:10 Resellers  
§ 18:11 Exemptions  
§ 18:12 Enforcement

**B. ARIZONA**

§ 18:13 Security freeze  
§ 18:14 Timing of freeze  
§ 18:15 Lifting of freeze  
§ 18:16 Fees  
§ 18:17 Changes to certain information  
§ 18:18 Exceptions  
§ 18:19 Enforcement  
§ 18:20 Effective date  
§ 18:21 Liability

**C. ARKANSAS**

§ 18:22 Legislation  
§ 18:23 Placement of a security freeze  
§ 18:24 Access to consumer reports  
§ 18:25 Removal of a security freeze  
§ 18:26 Effect of a security freeze  
§ 18:27 Consumer request for removal of a security freeze  
§ 18:28 Exceptions  
§ 18:29 Fees  
§ 18:30 Changes to certain information

- § 18:31 Exemptions from placing a security freeze
- § 18:32 Notice
- § 18:33 Civil remedies
- § 18:34 Effective date

## **D. CALIFORNIA**

- § 18:35 Security alerts
- § 18:36 —Effect
- § 18:37 —Penalties
- § 18:38 Placement by consumer
- § 18:39 Timing of freeze
- § 18:40 Lifting of freeze
- § 18:41 Development of procedures
- § 18:42 Effect
- § 18:43 Exemptions
- § 18:44 Fees
- § 18:45 Changes to consumer credit report
- § 18:46 Resellers of information
- § 18:47 Exemptions from placing security alerts or security freezes
- § 18:48 Disclosure of public record information
- § 18:49 Unconstitutionality of California's security freeze law

## **E. COLORADO**

- § 18:50 Credit freeze
- § 18:51 Timing of freeze
- § 18:52 Changes to certain information
- § 18:53 Lifting of freeze
- § 18:54 Development of contact methods
- § 18:55 Exceptions
- § 18:56 Fees
- § 18:57 Notice

## **F. CONNECTICUT**

- § 18:58 Credit freeze
- § 18:59 Timing of freeze
- § 18:60 Development of procedures
- § 18:61 Lifting of a freeze
- § 18:62 Fees
- § 18:63 Exceptions

## **G. DELAWARE**

- § 18:64 Credit freeze

## TABLE OF CONTENTS

§ 18:65	Security freeze
§ 18:66	Timing of freeze
§ 18:67	Lifting of freeze
§ 18:68	Development of procedures
§ 18:69	Effect of freeze
§ 18:70	Exceptions
§ 18:71	Fees
§ 18:72	Notices
§ 18:73	Enforcement

## H. FLORIDA

§ 18:74	Security freeze
§ 18:75	Effect of freeze
§ 18:76	Development of procedures
§ 18:77	Timing of freeze
§ 18:78	Lifting of freeze
§ 18:79	Other disclosures
§ 18:80	Exceptions
§ 18:81	Fees
§ 18:82	Changes to information
§ 18:83	Enforcement
§ 18:84	Notices

## I. GEORGIA

§ 18:85	Security freeze
§ 18:86	Effect of freeze
§ 18:87	Timing of freeze
§ 18:88	Lifting of freeze
§ 18:89	Exemptions
§ 18:90	Changes to information
§ 18:91	Fees
§ 18:92	Enforcement
§ 18:93	Notice requirement

## J. HAWAII

§ 18:94	Security freeze
§ 18:95	Effect of freeze
§ 18:96	Timing of freeze
§ 18:97	Development of procedures
§ 18:98	Exceptions
§ 18:99	Duties of a consumer reporting agency
§ 18:100	Fees
§ 18:101	Enforcement

## **K. IDAHO**

- § 18:102 Security freeze
- § 18:103 Effect of security freeze
- § 18:104 Development of contact methods
- § 18:105 Removal of a security freeze
- § 18:106 Exceptions
- § 18:107 Fees
- § 18:108 Changes to certain forms of information
- § 18:109 Enforcement

## **L. ILLINOIS**

- § 18:110 Security freeze
- § 18:111 Timing of freeze
- § 18:112 Lifting
- § 18:113 Development of contact methods
- § 18:114 Effect of security freeze
- § 18:115 Exemptions
- § 18:116 Fees
- § 18:117 Changes to information
- § 18:118 Exemptions
- § 18:119 Enforcement

## **M. INDIANA**

- § 18:120 Placement of a security freeze
- § 18:121 Development of procedures
- § 18:122 Timing of freeze
- § 18:123 Removal of security freezes
- § 18:124 Additional procedures for release of freezes
- § 18:125 Requests by third parties
- § 18:126 Length of freeze
- § 18:127 Restrictions on removal of security freezes
- § 18:128 Permitted disclosures
- § 18:129 Exemptions from placing a security freeze
- § 18:130 Changes to information
- § 18:131 Notices to consumers
- § 18:132 Fees
- § 18:133 Civil enforcement

## **N. IOWA**

- § 18:134 Security freeze
- § 18:135 Timing of freeze
- § 18:136 Temporary lift freeze



## TABLE OF CONTENTS

§ 18:137	Removal of freeze
§ 18:138	Fees
§ 18:139	Effect of freeze
§ 18:140	Exceptions
§ 18:141	Changes to certain information
§ 18:142	Waiver
§ 18:143	Enforcement

## O. KANSAS

§ 18:144	Security freeze
§ 18:145	Timing of freeze
§ 18:146	Provision of unique ID
§ 18:147	Effect of freeze
§ 18:148	Lifting of freeze
§ 18:149	Duration of a freeze
§ 18:150	Nonapplicability of freeze
§ 18:151	Exemptions
§ 18:152	Fees
§ 18:153	Changes to certain information
§ 18:154	Civil remedies

## P. KENTUCKY

§ 18:155	Placement of a security freeze
§ 18:156	Timing of freeze
§ 18:157	Effect
§ 18:158	Entities exempt from placing freezes
§ 18:159	Personal identification numbers and disclosure of process
§ 18:160	Requests for information when a security freeze is in place
§ 18:161	Lifting of freeze
§ 18:162	Length
§ 18:163	Disclosure of information during security freeze
§ 18:164	Fees
§ 18:165	Changes to information
§ 18:166	Civil remedies

## Q. LOUISIANA

§ 18:167	Security alert
§ 18:168	Toll-free number
§ 18:169	Exemptions
§ 18:170	Placing
§ 18:171	Notice

## INFORMATION SECURITY AND PRIVACY

- § 18:172 Effect
- § 18:173 Lifting of freeze
- § 18:174 Inapplicability
- § 18:175 Fees
- § 18:176 Changes to information
- § 18:177 Enforcement
- § 18:178 Limitations on use of consumer's credit report

## R. MARYLAND

- § 18:179 Security freeze
- § 18:180 Timing of freeze
- § 18:181 Exceptions
- § 18:182 Temporary lifting of security freezes
- § 18:183 Lifting of freeze
- § 18:184 Effect of freeze
- § 18:185 Length of freeze
- § 18:186 Fees
- § 18:187 Other notices
- § 18:188 Notification of release of information
- § 18:189 Enforcement
- § 18:190 Protected consumers

## S. MASSACHUSETTS

- § 18:191 Security freezes—Consumer requests
- § 18:192 Timing and lifting of freezes
- § 18:193 Changes to information
- § 18:194 Exemptions
- § 18:195 Fees
- § 18:196 Regulations
- § 18:197 Enforcement for willful noncompliance
- § 18:198 Enforcement for negligent noncompliance

## T. MINNESOTA

- § 18:199 Security freeze
- § 18:200 Timing of freeze
- § 18:201 Lifting of freeze
- § 18:202 Additional procedures
- § 18:203 Effect of freeze
- § 18:204 Exceptions
- § 18:205 Fees
- § 18:206 Changes to information
- § 18:207 Other exceptions
- § 18:208 Enforcement

## TABLE OF CONTENTS

### **U. MISSISSIPPI**

- § 18:209 Credit freeze
- § 18:210 Changes in information
- § 18:211 Lifting of freeze
- § 18:212 Development of procedures
- § 18:213 Fees
- § 18:214 Exceptions

### **V. MISSOURI**

- § 18:215 Security freezes
- § 18:216 Credit freeze
- § 18:217 Timing of freeze
- § 18:218 Fees
- § 18:219 Exceptions
- § 18:220 Restrictions on changes to report
- § 18:221 Temporary lift of freeze
- § 18:222 Removal of freeze
- § 18:223 Notices
- § 18:224 Exceptions

### **W. MONTANA**

- § 18:225 Security freeze
- § 18:226 Timing of freeze
- § 18:227 Temporary lifting of freeze
- § 18:228 Removal of a freeze
- § 18:229 Effect of freeze
- § 18:230 Removal procedures
- § 18:231 Other notices
- § 18:232 Exemptions
- § 18:233 Fees
- § 18:234 Enforcement

### **X. NEBRASKA**

- § 18:235 Credit freeze
- § 18:236 Effect of freeze
- § 18:237 Timing of freeze
- § 18:238 Temporary lift of freeze
- § 18:239 Removal of freeze
- § 18:240 Fees
- § 18:241 Changes to information
- § 18:242 Effect of freeze
- § 18:243 Exemptions

§ 18:244 Enforcement

## **Y. NEW HAMPSHIRE**

- § 18:245 Security freeze—Placement of a freeze
- § 18:246 Timing of freeze
- § 18:247 Temporary lift of freeze
- § 18:248 Development of procedures
- § 18:249 Denial of access
- § 18:250 Disclosure requirements
- § 18:251 Length of freeze
- § 18:252 Removal of freeze
- § 18:253 Requirement of proper identification
- § 18:254 Exceptions
- § 18:255 Duties of a consumer reporting agency if a security freeze is in effect
- § 18:256 Persons not required to place a security freeze
- § 18:257 Rights of victims of identity theft
- § 18:258 Consumer report files of deceased persons
- § 18:259 Police report regarding identity theft
- § 18:260 Fees
- § 18:261 Amended civil penalties
- § 18:262 Notice to consumers

## **Z. NEW YORK**

- § 18:263 Security freeze
- § 18:264 Effect of freeze
- § 18:265 Written confirmation
- § 18:266 Disclosures regarding security freezes
- § 18:267 Temporary lifting of freezes
- § 18:268 Standards for lifting a freeze
- § 18:269 Development of procedures
- § 18:270 Monitoring by the consumer protection board
- § 18:271 Requests for access and treatment of applications as incomplete
- § 18:272 Length and permanent removal of a security freeze
- § 18:273 Requirement for proper identification
- § 18:274 Exemptions
- § 18:275 Fees
- § 18:276 Changes to information
- § 18:277 Other disclosures and requests for information
- § 18:278 Written notification of improper releases of information
- § 18:279 Enforcement

## TABLE OF CONTENTS

### **AA. NORTH CAROLINA**

§ 18:280	Security freeze for protected consumers
§ 18:281	Duration of freeze
§ 18:282	Fees
§ 18:283	Exceptions
§ 18:284	Exclusions from placing freezes
§ 18:285	Enforcement
§ 18:286	Credit freeze
§ 18:287	Timing of freeze
§ 18:288	Effect on changes to report
§ 18:289	Lifting of freeze
§ 18:290	Development of procedures
§ 18:291	Exceptions to application of law
§ 18:292	Fees
§ 18:293	Minors
§ 18:294	Effect on credit applications
§ 18:295	Additional notices
§ 18:296	Credit Monitoring Services Act
§ 18:297	Enforcement
§ 18:298	Effective date

### **BB. OKLAHOMA**

§ 18:299	Security freeze
§ 18:300	Timing of freeze
§ 18:301	Additional disclosures
§ 18:302	Temporary lift of freeze
§ 18:303	Development of procedures
§ 18:304	Effect of freeze
§ 18:305	Length of freeze
§ 18:306	Exceptions
§ 18:307	Fees
§ 18:308	Changes to information
§ 18:309	Exemptions from placement of security freezes
§ 18:310	Notice requirements
§ 18:311	Enforcement

### **CC. OREGON**

§ 18:312	Placement of freeze
§ 18:313	Effect of freeze
§ 18:314	Timing of freeze
§ 18:315	Temporary lift of freeze
§ 18:316	Removal of freeze
§ 18:317	Effect of freeze

## INFORMATION SECURITY AND PRIVACY

- § 18:318 Duration of freeze for protected records
- § 18:319 Fees
- § 18:320 Exceptions to security freezes
- § 18:321 Changes to certain information

### **DD. PENNSYLVANIA**

- § 18:322 Credit freeze
- § 18:323 Timing
- § 18:324 Entities not required to place freezes
- § 18:325 Effect
- § 18:326 Requests for frozen information
- § 18:327 Duration of freeze
- § 18:328 Exceptions to nondisclosure of information
- § 18:329 Required actions by consumer reporting agency
- § 18:330 Notification of freeze
- § 18:331 Temporary access and removal of a security freeze
- § 18:332 Secure procedures
- § 18:333 Fees
- § 18:334 Changes to information during freeze
- § 18:335 Civil enforcement

### **EE. SOUTH CAROLINA**

- § 18:336 Security freeze
- § 18:337 Timing of freeze
- § 18:338 Changes to certain information
- § 18:339 Lifting of freeze
- § 18:340 Fees
- § 18:341 Exceptions
- § 18:342 Effective date

### **FF. SOUTH DAKOTA**

- § 18:343 Credit freeze
- § 18:344 Timing of freeze
- § 18:345 Additional disclosures
- § 18:346 Temporary lift
- § 18:347 Development of procedures
- § 18:348 Effect of freeze
- § 18:349 Lift of freeze
- § 18:350 Exceptions
- § 18:351 Changes to information

### **GG. TENNESSEE**

- § 18:352 Security freeze

## TABLE OF CONTENTS

§ 18:353	Timing of freeze
§ 18:354	Temporary lift of freeze
§ 18:355	Development of procedures
§ 18:356	Lift of freeze
§ 18:357	Effect of freeze
§ 18:358	Procedures
§ 18:359	Length of freeze
§ 18:360	Changes to information
§ 18:361	Fees
§ 18:362	Exceptions
§ 18:363	Enforcement
§ 18:364	Notices

## HH. TEXAS

§ 18:365	Request by consumer
§ 18:366	Notification of changes to information
§ 18:367	Notification of security freeze
§ 18:368	Removal or temporary lifting of security freeze
§ 18:369	Fees
§ 18:370	Exemptions
§ 18:371	Exemptions from placing security alerts or security freezes
§ 18:372	Honoring of security freezes
§ 18:373	Applicable fees
§ 18:374	Security alert—Timing
§ 18:375	—Notification
§ 18:376	—Toll-free security alert request number
§ 18:377	—Verification of consumer identity

## II. UTAH

§ 18:378	Security freeze
§ 18:379	Restrictions on conduct
§ 18:380	Development of policies
§ 18:381	Removal of security freeze
§ 18:382	Timing of lift of freeze
§ 18:383	Exceptions
§ 18:384	Fees for security freeze
§ 18:385	Changes to information in a credit report
§ 18:386	Enforcement

## JJ. VIRGINIA

§ 18:387	Placement of security freeze
§ 18:388	Temporary lift of freeze

## INFORMATION SECURITY AND PRIVACY

- § 18:389 Removal of freeze
- § 18:390 Development of procedures
- § 18:391 Affect of freeze
- § 18:392 Length of freeze
- § 18:393 Exceptions
- § 18:394 Fees
- § 18:395 Changes to information
- § 18:396 Exceptions
- § 18:397 Additional notices
- § 18:398 Enforcement

## **KK. WASHINGTON**

- § 18:399 Credit freeze
- § 18:400 Timing of freeze
- § 18:401 Temporary lift of freeze
- § 18:402 Development of procedures
- § 18:403 Effect of freeze
- § 18:404 Lifting of freeze
- § 18:405 Exceptions
- § 18:406 Changes to information

## **LL. WISCONSIN**

- § 18:407 Security freeze
- § 18:408 Timing of freeze
- § 18:409 Effect of freeze
- § 18:410 Temporary lift of freeze
- § 18:411 Lift of freeze
- § 18:412 Exceptions
- § 18:413 Change to information
- § 18:414 Notice obligations
- § 18:415 Enforcement

## **MM. WYOMING**

- § 18:416 Security freeze
- § 18:417 Effect of freeze
- § 18:418 Timing of freeze
- § 18:419 Development of procedures
- § 18:420 Removal or temporary lift of security freeze
- § 18:421 Exceptions
- § 18:422 Exemptions
- § 18:423 Fees
- § 18:424 Changes to information during a security freeze
- § 18:425 Enforcement



TABLE OF CONTENTS

**CHAPTER 19. RESTRICTIONS ON CREDIT CARDS**

§ 19:1 Restrictions on credit card numbers

**A. ALASKA**

§ 19:2 Restrictions on credit card receipts

§ 19:3 Enforcement

**B. ARIZONA**

§ 19:4 Credit card receipt law

**C. CALIFORNIA**

§ 19:5 Song-Beverly Credit Card Act (“Song Beverly”)—  
Restrictions on credit card receipts

§ 19:6 —Restrictions on collection of information with credit  
card transactions

§ 19:7 Exceptions

§ 19:8 —Collection of information after conclusion of credit  
card transaction

§ 19:9 —Civil enforcement

§ 19:10 —Statute of limitations for claims under section  
1747.08

§ 19:11 —Pineda v. Williams-Sonoma Stores—Zip codes and  
section 1747.08

§ 19:12 —Retroactivity

§ 19:13 —Forms on the Internet and section 1747.08

§ 19:14 —Online purchases to be picked up in store

§ 19:15 —Collection of birthdate for alcoholic beverages

§ 19:16 —Returns not subject to section 1747.08

§ 19:17 —Jury trials

§ 19:18 —Timing of collection

**D. COLORADO**

§ 19:19 Credit card receipt law

**E. CONNECTICUT**

§ 19:20 Restrictions on receipts

§ 19:21 Enforcement

**F. DELAWARE**

§ 19:22 Credit card receipt law

**G. FLORIDA**

§ 19:23 Restrictions on receipts

§ 19:24 Enforcement

**H. GEORGIA**

§ 19:25 Restrictions on credit card receipts

§ 19:26 Powers of administrator

§ 19:27 Enforcement

**I. ILLINOIS**

§ 19:28 Restrictions on issuance of credit cards

§ 19:29 Restrictions on credit card receipts

**J. KANSAS**

§ 19:30 Restrictions on credit card receipts

**K. LOUISIANA**

§ 19:31 Restrictions on credit card receipts

**L. MAINE**

§ 19:32 Restrictions upon credit card receipts

**M. MASSACHUSETTS**

§ 19:33 Massachusetts credit card law

**N. MICHIGAN**

§ 19:34 Restrictions on credit card receipts

**O. MINNESOTA**

§ 19:35 Credit card offers

**P. MONTANA**

§ 19:36 Restrictions upon credit cards

§ 19:37 Restrictions on telephone companies

**Q. NEVADA**

§ 19:38 Restrictions on credit cards

§ 19:39 Restrictions on credit card receipts

**R. NEW JERSEY**

§ 19:40 Restrictions on credit card receipts

TABLE OF CONTENTS

**S. NEW YORK**

- § 19:41 Requirement of carbonless credit and debit card forms
- § 19:42 Restrictions on personal checks, gift certificates, traveler's checks, or money orders
- § 19:43 Restrictions on credit card receipts

**T. NORTH CAROLINA**

- § 19:44 Restrictions on credit card receipts
- § 19:45 Sale of cash registers and other receipt printing machines

**U. OHIO**

- § 19:46 Restrictions on credit card receipts
- § 19:47 Enforcement

**V. OREGON**

- § 19:48 Overview

**W. RHODE ISLAND**

- § 19:49 Restrictions on credit card receipts

**X. SOUTH CAROLINA**

- § 19:50 Credit and debit card receipts
- § 19:51 —Enforcement

**Y. TENNESSEE**

- § 19:52 Restrictions on credit card receipts

**Z. TEXAS**

- § 19:53 Restrictions on credit card receipts

**AA. VIRGINIA**

- § 19:54 Restrictions on credit card receipts
- § 19:55 Enforcement

**BB. WASHINGTON**

- § 19:56 Restrictions on credit card receipts
- § 19:57 Washington D.C. litigation

**CC. WISCONSIN**

- § 19:58 Restrictions on credit card receipts

## **CHAPTER 20. INSURANCE PRIVACY**

- § 20:1 Introduction
- § 20:2 California Insurance Code—Restrictions upon disclosure
- § 20:3 —Disclosure to health care institutions
- § 20:4 —Other exceptions
- § 20:5 —Disclosures for research studies
- § 20:6 —Disclosures related to mergers
- § 20:7 —Disclosures for marketing
- § 20:8 —Disclosures to affiliates
- § 20:9 —Restrictions upon disclosures by state agencies

## **CHAPTER 21. FAMILY EDUCATION RIGHTS AND PRIVACY ACT**

- § 21:1 Overview
- § 21:2 Application
- § 21:3 Rights of parents
- § 21:4 Rights of students
- § 21:5 Annual notification requirements
- § 21:6 Records of law-enforcement units
- § 21:7 Rights of parents or eligible students to inspect and review records
- § 21:8 Charges for copies of education records
- § 21:9 Limitations on inspection and review
- § 21:10 Requesting amendment of records
- § 21:11 Right to a hearing
- § 21:12 Prior consent and disclosure
- § 21:13 Disclosures without consent
- § 21:14 Anonymized records
- § 21:15 Nonmandatory disclosures
- § 21:16 Authentication
- § 21:17 Record retention
- § 21:18 Inspection rights
- § 21:19 Restrictions on redisclosure
- § 21:20 Conditions on disclosure
- § 21:21 Disclosure related to federal or state programs
- § 21:22 Disclosure of information in health and safety emergencies
- § 21:23 Directory information
- § 21:24 Conditions on disclosure of information regarding juvenile justice systems
- § 21:25 Delegations of authority
- § 21:26 Conflicts of laws
- § 21:27 Submissions to the Office

## TABLE OF CONTENTS

- § 21:28 Complaints
- § 21:29 Investigative procedures
- § 21:30 Form of notice of investigations
- § 21:31 Enforcement process
- § 21:32 Enforcement
- § 21:33 FERPA litigation and disclosure of information
- § 21:34 Kentucky

## CHAPTER 22. IDENTITY THEFT

### I. INTRODUCTION

- § 22:1 Introduction

### II. FEDERAL LAW

- § 22:2 Federal Identity Theft and Assumption Deterrence Act
- § 22:3 —Intent under section 1028(a)(1)
- § 22:4 —Use of a forged signature
- § 22:5 —Application to deceased individuals

### III. SPECIFIC STATE LAWS

#### A. ALABAMA

- § 22:6 Identity theft
- § 22:7 Trafficking in stolen identities
- § 22:8 Obstructing justice using false identity
- § 22:9 Restitution
- § 22:10 Block on false information in credit reports
- § 22:11 —Enforcement
- § 22:12 Order to correct records
- § 22:13 Civil enforcement generally

#### B. ALASKA

- § 22:14 Overview
- § 22:15 Factual declaration of innocence
- § 22:16 Establishment of database
- § 22:17 Right to file police report regarding identity theft
- § 22:18 Criminal impersonation

#### C. ARIZONA

- § 22:19 Identity theft

D. ARKANSAS

- § 22:20 Financial identity fraud

E. CALIFORNIA

- § 22:21 Obtaining and using personal identifying information
- § 22:22 Investigation and court action for identity theft
- § 22:23 Disclosures of credit information
- § 22:24 Sale of deceptive identification documents
- § 22:25 Civil cause of action for identity theft

F. COLORADO

- § 22:26 Identity theft and factual innocence finding
- § 22:27 Forgery
- § 22:28 Criminal possession of forgery devices
- § 22:29 Identity theft
- § 22:30 Criminal possession of a financial device
- § 22:31 Gathering identity information by deception
- § 22:32 Possession of identity theft tools

G. CONNECTICUT

- § 22:33 Identity theft

H. DELAWARE

- § 22:34 Identity theft
- § 22:35 —Passports

I. FLORIDA

- § 22:36 Fraudulent use of personal identification information
- § 22:37 Harassment by use of personal information
- § 22:38 Use of personal information of deceased individuals
- § 22:39 Use of fictitious personal information
- § 22:40 Enhancements and reductions in sentences
- § 22:41 Exceptions to liability
- § 22:42 Restitution
- § 22:43 Correction of public records

J. GEORGIA

- § 22:44 Identity fraud
- § 22:45 Restrictions on fraudulent identification documents
- § 22:46 —Enforcement
- § 22:47 Civil actions

TABLE OF CONTENTS

- § 22:48 Use of scanning devices and reencoders
- § 22:49 —Enforcement

K. HAWAII

- § 22:50 Identity theft

L. IDAHO

- § 22:51 Identity theft

M. ILLINOIS

- § 22:52 Unauthorized acquisition of personal information
- § 22:53 Identity theft crimes
- § 22:54 Credit and public utility service—Identity theft

N. INDIANA

- § 22:55 Identity deception

O. IOWA

- § 22:56 Identity theft

P. KANSAS

- § 22:57 Identity theft

Q. KENTUCKY

- § 22:58 Identity theft

R. LOUISIANA

- § 22:59 Identity theft

S. MAINE

- § 22:60 Misuse of identification

T. MARYLAND

- § 22:61 Identity fraud
- § 22:62 Enforcement

U. MASSACHUSETTS

- § 22:63 Identity theft
- § 22:64 Police reporting requirements

V. MICHIGAN

- § 22:65 Crimes related to personal identifying information
- § 22:66 Identity theft
- § 22:67 Offenses related to use of personal information
- § 22:68 Obtaining or possessing personal identifying information of another person
- § 22:69 Verification of information for victims of identity theft
- § 22:70 Denial or reduction of credit or public utility services to victim of identity theft

W. MINNESOTA

- § 22:71 Identity theft
- § 22:72 Electronic use of false pretenses to obtain identity

X. MISSISSIPPI

- § 22:73 Fraudulent use of Social Security number or identifying information to obtain goods
- § 22:74 Identity theft investigations

Y. MISSOURI

- § 22:75 Identity theft
- § 22:76 Additional rights in security freeze bill
- § 22:77 Identity theft report
- § 22:78 Manufacture of means of forged identification
- § 22:79 Insurance identification cards

Z. MONTANA

- § 22:80 Identity theft

AA. NEBRASKA

- § 22:81 Criminal impersonation
- § 22:82 Application of Nebraska's law to court actions
- § 22:83 Unauthorized use of a financial transaction device

BB. NEVADA

- § 22:84 Identity theft

CC. NEW HAMPSHIRE

- § 22:85 Identity fraud

DD. NEW JERSEY

- § 22:86 Identity theft



## TABLE OF CONTENTS

- § 22:87 Obtaining information under false pretenses
- § 22:88 Sale of false documents
- § 22:89 Enforcement
- § 22:90 Correction of records
- § 22:91 Police reporting
- § 22:92 Effect of rejected requests
- § 22:93 Scanning and reencoding devices

## EE. NEW MEXICO

- § 22:94 Identity theft

## FF. NEW YORK

- § 22:95 Identity theft
- § 22:96 —First, second, and third degree
- § 22:97 Unlawful possession of personal identification information in the third degree
- § 22:98 Defenses based upon misrepresentations of age
- § 22:99 Other identity theft crimes
- § 22:100 Unlawful possession of a skimmer device
- § 22:101 Other identity theft laws

## GG. NORTH CAROLINA

- § 22:102 Identity theft
- § 22:103 Trafficking in stolen identities
- § 22:104 Other remedies
- § 22:105 Investigation of offenses

## HH. NORTH DAKOTA

- § 22:106 Identity theft

## II. OHIO

- § 22:107 Identity theft
- § 22:108 Civil remedies

## JJ. OKLAHOMA

- § 22:109 Identity theft

## KK. OREGON

- § 22:110 Identity theft

LL. PENNSYLVANIA

§ 22:111 Identity theft

MM. RHODE ISLAND

§ 22:112 Impersonation and identity fraud

NN. SOUTH CAROLINA

§ 22:113 Personal Financial Security Act

§ 22:114 Identity theft

§ 22:115 Identity fraud

§ 22:116 Effective date

§ 22:117 Correction of public records

§ 22:118 Identity theft database

§ 22:119 Household garbage

OO. SOUTH DAKOTA

§ 22:120 Identity theft

PP. TENNESSEE

§ 22:121 Identity Theft Deterrence Act

QQ. TEXAS

§ 22:122 Identity theft

§ 22:123 Identity theft by electronic device

RR. UTAH

§ 22:124 Identity fraud

SS. VERMONT

§ 22:125 Identity theft

TT. VIRGINIA

§ 22:126 Identity theft

§ 22:127 Blocking of information

UU. WASHINGTON

§ 22:128 Identity theft

§ 22:129 Remote identification scanning

VV. WASHINGTON D.C.

§ 22:130 Identity theft

## TABLE OF CONTENTS

§ 22:131 Correction of public records

### WW. WEST VIRGINIA

§ 22:132 Identity theft

### XX. WISCONSIN

§ 22:133 Identity theft

### YY. WYOMING

§ 22:134 Identity theft

§ 22:135 Factual declaration of innocence after identity theft

## **CHAPTER 23. RESTRICTIONS UPON THE USE OF SOCIAL SECURITY NUMBERS**

### **I. IN GENERAL**

§ 23:1 Introduction

§ 23:2 Social Security number discrimination

§ 23:3 Discovery regarding Social Security numbers

§ 23:4 Constitutional right of protection for Social Security  
numbers

§ 23:5 The Privacy Act of 1974

§ 23:6 Litigation issues and the Privacy Act

§ 23:7 The Intelligence Reform and Terrorism Prevention Act  
of 2004

### **II. SPECIFIC STATE PROVISIONS**

#### **A. ALABAMA**

§ 23:8 Overview

#### **B. ALASKA**

§ 23:9 Overview

§ 23:10 Exceptions

§ 23:11 Additional restrictions on collection

§ 23:12 Enforcement

§ 23:13 Disclosure of Social Security numbers

§ 23:14 Interagency disclosures of Social Security numbers

§ 23:15 General exceptions

§ 23:16 Agency regulations

§ 23:17 Enforcement

C. ARIZONA

- § 23:18 Overview
- § 23:19 Exemptions
- § 23:20 Restrictions on state entities
- § 23:21 Enforcement
- § 23:22 Restrictions on use of sequential numbers

D. ARKANSAS

- § 23:23 Overview

E. CALIFORNIA

- § 23:24 Overview
- § 23:25 Defining “access” to a website
- § 23:26 Restrictions on recording
- § 23:27 Creation of task force
- § 23:28 Amendments to disclosure requirements
- § 23:29 Restrictions on county recorders
- § 23:30 Use of fees
- § 23:31 Reporting requirements
- § 23:32 Fees
- § 23:33 Restrictions in California’s election code

F. COLORADO

- § 23:34 Overview

G. CONNECTICUT

- § 23:35 Overview
- § 23:36 Public policy for Social Security numbers
- § 23:37 Enforcement
- § 23:38 Exceptions

H. DELAWARE

- § 23:39 Overview

I. FLORIDA

- § 23:40 Overview

J. GEORGIA

- § 23:41 Overview
- § 23:42 Restrictions on Social Security numbers

## TABLE OF CONTENTS

### K. GUAM

- § 23:43 Restrictions on Social Security numbers
- § 23:44 Exceptions
- § 23:45 Enforcement

### L. HAWAII

- § 23:46 Overview
- § 23:47 Additional restrictions on Social Security numbers
- § 23:48 Enforcement
- § 23:49 Government reporting

### M. IDAHO

- § 23:50 Protection of personal information

### N. ILLINOIS

- § 23:51 Overview
- § 23:52 Use of Social Security numbers on insurance cards
- § 23:53 Use of Social Security numbers on licenses
- § 23:54 Other restrictions

### O. INDIANA

- § 23:55 Overview
- § 23:56 Restrictions on the recording of documents
- § 23:57 Government Social Security numbers
- § 23:58 Enforcement of Social Security number laws
- § 23:59 Restrictions on Social Security numbers

### P. KANSAS

- § 23:60 Social Security number restrictions—Insurers
- § 23:61 —Postsecondary educational institutions
- § 23:62 Public filings
- § 23:63 Exceptions
- § 23:64 Other restrictions
- § 23:65 Exceptions
- § 23:66 Enforcement

### Q. LOUISIANA

- § 23:67 Overview

### R. MAINE

- § 23:68 Restrictions on Social Security numbers

§ 23:69 Enforcement

S. MARYLAND

§ 23:70 Overview

§ 23:71 Restrictions on printing of Social Security numbers  
on checks

T. MICHIGAN

§ 23:72 Overview

§ 23:73 Exceptions

§ 23:74 Privacy policy requirements related to the collection  
of Social Security numbers

§ 23:75 Exemption from disclosure under the Freedom of  
Information Act

§ 23:76 Enforcement

§ 23:77 Restrictions on recording of documents with Social  
Security numbers

U. MINNESOTA

§ 23:78 Overview

V. MISSOURI

§ 23:79 Overview

W. NEBRASKA

§ 23:80 Restrictions on Social Security numbers

X. NEVADA

§ 23:81 Overview

§ 23:82 Additional restrictions on Social Security numbers

Y. NEW JERSEY

§ 23:83 Restrictions on Social Security numbers generally

§ 23:84 Exemptions and exceptions

§ 23:85 Restrictions upon Social Security numbers in publicly  
recorded documents

§ 23:86 Restrictions upon institutions of higher education

§ 23:87 Restrictions on Social Security numbers

Z. NEW MEXICO

§ 23:88 Overview

## TABLE OF CONTENTS

### AA. NEW YORK

- § 23:89 Social Security number law
- § 23:90 Exemptions
- § 23:91 Preemption
- § 23:92 Exemption for the state
- § 23:93 Data security and Social Security numbers
- § 23:94 Waiver of New York’s Social Security number law
- § 23:95 Enforcement
- § 23:96 Defenses to enforcement actions
- § 23:97 Disclosure of Social Security number
- § 23:98 Exceptions
- § 23:99 Enforcement
- § 23:100 Defenses
- § 23:101 Restrictions on government disclosure of Social Security numbers
- § 23:102 Restrictions on public filings
- § 23:103 Employee personal identifying information
- § 23:104 —Enforcement

### BB. NORTH CAROLINA

- § 23:105 Restrictions upon Social Security numbers
- § 23:106 Restrictions upon governmental use of Social Security numbers
- § 23:107 Restrictions upon the filing of documents
- § 23:108 Removal of information
- § 23:109 Posting of notices
- § 23:110 Removal by clerks

### CC. OKLAHOMA

- § 23:111 Overview

### DD. OREGON

- § 23:112 Restrictions on personal information held by district attorneys
- § 23:113 Restrictions upon the disclosure of Social Security numbers

### EE. PENNSYLVANIA

- § 23:114 Social Security Number Privacy Act
- § 23:115 Duties of the department
- § 23:116 Prohibitions on use of Social Security numbers
- § 23:117 Requirement to apply for an exemption

## INFORMATION SECURITY AND PRIVACY

- § 23:118 Exclusion
- § 23:119 Other restrictions on the disclosure of Social Security numbers
- § 23:120 Continuing use of Social Security numbers
- § 23:121 Opt-out requests
- § 23:122 Opt-out requests and denial of services
- § 23:123 Exceptions
- § 23:124 Enforcement

### FF. RHODE ISLAND

- § 23:125 Overview
- § 23:126 Additional Social Security number restrictions
- § 23:127 Enforcement
- § 23:128 Other restrictions
- § 23:129 Enforcement

### GG. SOUTH CAROLINA

- § 23:130 Overview
- § 23:131 Enforcement
- § 23:132 Removal of images
- § 23:133 South Carolina—Posting of signs
- § 23:134 Effective date

### HH. SOUTH DAKOTA

- § 23:135 Overview
- § 23:136 Restrictions on Social Security numbers

## II. TENNESSEE

- § 23:137 Overview
- § 23:138 Social Security/Taxpayer ID numbers
- § 23:139 Social Security number restrictions
- § 23:140 Enforcement

### JJ. TEXAS

- § 23:141 Requirement of a privacy policy
- § 23:142 Exceptions
- § 23:143 Enforcement
- § 23:144 Restrictions on Social Security numbers in official business
- § 23:145 Property
- § 23:146 Certain uses of Social Security Numbers Business and Commerce Code section 501.001



## TABLE OF CONTENTS

- § 23:147 Exceptions
- § 23:148 Other restrictions

### KK. UTAH

- § 23:149 Overview

### LL. VERMONT

- § 23:150 Overview
- § 23:151 Restrictions upon state agencies
- § 23:152 Enforcement

### MM. VIRGINIA

- § 23:153 Overview

### NN. WASHINGTON

- § 23:154 Overview
- § 23:155 Exemption from public inspection
- § 23:156 Presentation of documents

### OO. WEST VIRGINIA

- § 23:157 Limitation on release of certain personal information maintained by state agencies and entities regarding state employees
- § 23:158 Personal information maintained by state entities
- § 23:159 Resale or redisclosure
- § 23:160 Use of student Social Security numbers
- § 23:161 Authority to utilize scanner technology in sales; authority to execute contracts relating thereto

### PP. WISCONSIN

- § 23:162 Overview

### QQ. WYOMING

- § 23:163 Official registry list information

## **CHAPTER 24. DATA SECURITY, CYBERSECURITY, AND DATA DESTRUCTION**

### **I. INTRODUCTION**

- § 24:1 In general

## II. FEDERAL LAW

- § 24:2 Impact of Sarbanes-Oxley and federal obstruction laws on data destruction and privacy
- § 24:3 SEC Division of Corporate Finance CF Disclosure Guidance: Topic No. 2 Cybersecurity
- § 24:4 SEC Division of Investment Management Guidance update on cybersecurity for funds and advisors
- § 24:5 Interaction of SOX and international law
- § 24:6 Executive Order on improving critical infrastructure cybersecurity (February 12, 2013)
- § 24:7 —Defining critical infrastructure
- § 24:8 —Information sharing
- § 24:9 —Consultative process
- § 24:10 —Cybersecurity framework
- § 24:11 —Privacy and civil liberties
- § 24:12 Executive Order on cybersecurity and information sharing (February 13, 2015)
- § 24:13 Incentives under the Executive Order on cybersecurity
- § 24:14 DoD cybersecurity reporting
- § 24:15 NIST Framework
- § 24:16 Document retention issues for broker-dealers
- § 24:17 Gramm-Leach-Bliley Act—Safeguards rule for customer information
- § 24:18 Security and incident response guidelines
- § 24:19 Development and implementation of information security program
- § 24:20 —Involve the board of directors
- § 24:21 —Assess risk
- § 24:22 —Manage and control risk
- § 24:23 —Oversee service provider arrangements
- § 24:24 —Adjust the program
- § 24:25 —Report to the board
- § 24:26 Guidelines on cell phone and personal digital assistants security
- § 24:27 FTC security suggestions
- § 24:28 FACT Act document destruction rule

## III. SPECIFIC STATE PROVISIONS

### A. ALABAMA (RE-ALPHABETIZE FOLLOWING ALPHA HIERARCHY HEADINGS ACCORDINGLY)

- § 24:29 Data breach

## TABLE OF CONTENTS

### B. ALASKA

- § 24:30 Disposal of records
- § 24:31 Adoption of policies and procedures
- § 24:32 Exemptions
- § 24:33 Enforcement

### C. ARIZONA

- § 24:34 Data destruction
- § 24:35 Enforcement
- § 24:36 Exceptions

### D. ARKANSAS

- § 24:37 Overview
- § 24:38 Exemptions

### E. CALIFORNIA

- § 24:39 Data security law
- § 24:40 Auto dealers and data security
- § 24:41 Restrictions on computer vendors
- § 24:42 Restrictions on network security

### F. COLORADO

- § 24:43 Overview
- § 24:44 Protection of personal identifying information

### G. CONNECTICUT

- § 24:45 Data destruction
- § 24:46 Enforcement
- § 24:47 Exceptions
- § 24:48 Government contractors
- § 24:49 Employers
- § 24:50 Connecticut health insurers

### H. DELAWARE

- § 24:51 Safe destruction of documents
- § 24:52 Violations
- § 24:53 Exemptions
- § 24:54 Employers
- § 24:55 Data security

### I. DISTRICT OF COLUMBIA

- § 24:56 Security requirements

§ 24:57 Disposal

## J. FLORIDA

§ 24:58 Requirements for data security

§ 24:59 Requirements for disposal of customer records

§ 24:60 Enforcement

§ 24:61 No private cause of action

## K. GEORGIA

§ 24:62 Data destruction

§ 24:63 Powers of administrator

§ 24:64 Enforcement

## L. HAWAII

§ 24:65 Data destruction

§ 24:66 Exceptions

§ 24:67 Enforcement

§ 24:68 Reporting requirements of government agencies

## M. ILLINOIS

§ 24:69 Disposal of materials containing personal information

§ 24:70 Data security

§ 24:71 Entities subject to the federal Health Insurance  
Portability and Accountability Act of 1996

§ 24:72 Biometric Information Privacy Act

§ 24:73 —Exceptions

§ 24:74 —Enforcement

## N. INDIANA

§ 24:75 Overview

§ 24:76 Data security

§ 24:77 Enforcement

§ 24:78 Health care providers

## O. KANSAS

§ 24:79 Data security

## P. KENTUCKY

§ 24:80 Data destruction

§ 24:81 Data security

TABLE OF CONTENTS

Q. LOUISIANA

§ 24:82 Data security

R. MARYLAND

§ 24:83 Data destruction

§ 24:84 Data security

§ 24:85 Exceptions

S. MASSACHUSETTS

§ 24:86 Data destruction

§ 24:87 Enforcement

§ 24:88 Data security regulations

§ 24:89 Standards for the protection of personal information  
of residents of the commonwealth

§ 24:90 Duty to protect and standards for protecting personal  
information

§ 24:91 Computer system security requirements

§ 24:92 Effective date

§ 24:93 Commonwealth of Massachusetts v. TD Bank

T. MICHIGAN

§ 24:94 Data destruction

§ 24:95 —Enforcement

U. MINNESOTA

§ 24:96 Liability for retention of security or identification  
information

V. MONTANA

§ 24:97 Data destruction

§ 24:98 Insurance data security requirements

W. NEBRASKA

§ 24:99 Data security

X. NEW MEXICO

§ 24:100 Data security

Y. NEVADA

§ 24:101 Overview

## INFORMATION SECURITY AND PRIVACY

- § 24:102 Data security
- § 24:103 Safe harbor
- § 24:104 Exceptions
- § 24:105 Enforcement
- § 24:106 Effective date
- § 24:107 Injunctive relief

### Z. NEW JERSEY

- § 24:108 Overview
- § 24:109 Proposed data security regulations
- § 24:110 Enforcement
- § 24:111 New Jersey health security law

### AA. NEW YORK

- § 24:112 Data destruction
- § 24:113 Enforcement
- § 24:114 Data destruction—New York City
- § 24:115 Reasonable security requirement
- § 24:116 Enforcement
- § 24:117 Cybersecurity requirements for financial services companies (23 NYCRR 500)—Cybersecurity program
- § 24:118 —Cybersecurity policy
- § 24:119 —Chief Information Security Officer
- § 24:120 —Penetration Testing and Vulnerability Assessments
- § 24:121 —Audit Trail
- § 24:122 Cybersecurity requirements for financial services companies (23 NYCRR 500)—Access privileges
- § 24:123 Cybersecurity requirements for financial services companies (23 NYCRR 500)—Application security
- § 24:124 —Risk assessment
- § 24:125 —Cybersecurity personnel and intelligence
- § 24:126 —Third party service provider security policy
- § 24:127 —Multi-Factor Authentication
- § 24:128 —Limitations on data retention
- § 24:129 —Training and monitoring
- § 24:130 —Encryption of nonpublic information
- § 24:131 —Incident response plan
- § 24:132 —Notices to superintendent
- § 24:133 —Confidentiality
- § 24:134 —Exemptions
- § 24:135 —Enforcement
- § 24:136 —Effective date

## TABLE OF CONTENTS

- § 24:137 —Transitional periods
- § 24:138 —Severability

### BB. NORTH CAROLINA

- § 24:139 Overview

### CC. OREGON

- § 24:140 Data security
- § 24:141 Enforcement

### DD. RHODE ISLAND

- § 24:142 Risk-based information security program
- § 24:143 Exceptions
- § 24:144 Data destruction
- § 24:145 —Exceptions
- § 24:146 —Enforcement

### EE. SOUTH CAROLINA

- § 24:147 Data destruction
- § 24:148 Enforcement

### FF. TENNESSEE

- § 24:149 Overview

### GG. TEXAS

- § 24:150 Overview
- § 24:151 Effective date
- § 24:152 Document retention and reproductions
- § 24:153 Disposal of documents containing PII
- § 24:154 Exceptions
- § 24:155 Enforcement

### HH. UTAH

- § 24:156 Maintenance of personal information
- § 24:157 Data destruction

### II. VERMONT

- § 24:158 Overview

### JJ. WASHINGTON

- § 24:159 Overview

- § 24:160 Security breaches and credit cards
- § 24:161 Effective date

#### KK. WISCONSIN

- § 24:162 Disposal of records containing personal information

### IV. COMMON SECURITY-RELATED ISSUES

- § 24:163 Loss of laptop computers
- § 24:164 What are “reasonable” technological safeguards
- § 24:165 Payment card industry compliance
- § 24:166 Putting it together
- § 24:167 Incident response
- § 24:168 Addressing data destruction/retention conundrum

## CHAPTER 25. NOTICE OF SECURITY BREACHES

### I. INTRODUCTION

- § 25:1 Introduction
- § 25:2 Overview of notice of security breach laws
- § 25:3 State data breach laws “At a Glance”
- § 25:4 Data security legislation
- § 25:5 Theft of laptop computers
- § 25:6 Steps to comply with notice of security breach laws
- § 25:7 Access
- § 25:8 Form of notice

### II. GLB ACT REQUIREMENTS

- § 25:9 Response programs for unauthorized access to customer information and customer notice
- § 25:10 Notice to customers of unauthorized access, content and delivery

### III. HIPAA AND PERSONAL HEALTH RECORD BREACHES

- § 25:11 HIPAA and Personal Health Records Breaches
- § 25:12 Defining a “breach”
- § 25:13 Statutory requirements
- § 25:14 Timing of notice
- § 25:15 Form of notice
- § 25:16 Notice to other entities



## TABLE OF CONTENTS

§ 25:17	Report to Congress on breaches
§ 25:18	Requirement to issue regulations
§ 25:19	Temporary breach notification requirement for vendors of personal health records and other non-HIPAA covered entities
§ 25:20	Notification by third-party service providers
§ 25:21	Application of requirements for timeliness, method, and content of notifications
§ 25:22	Notification of the Secretary
§ 25:23	Enforcement
§ 25:24	Regulations and effective date

## **IV. CYBER INCIDENT REPORTING FOR CRITICAL INFRASTRUCTURE ACT OF 2022 (CIRCA)**

§ 25:25	Applicability
§ 25:26	Required reporting on covered cyber incidents and ransom payments
§ 25:27	Exceptions to required reporting on covered cyber incidents and ransom payments
§ 25:28	CIRCA Report submission deadlines
§ 25:29	Required manner and form of CIRCA Reports
§ 25:30	Required information for CIRCA Reports
§ 25:31	Required information for Covered Cyber Incident Reports
§ 25:32	Required information for Ransom Payment Reports
§ 25:33	Required information for Joint Covered Cyber Incident and Ransom Payment Reports
§ 25:34	Required information for Supplemental Reports
§ 25:35	Third party reporting procedures and requirements
§ 25:36	Data and records preservation requirements
§ 25:37	Request for information and subpoena procedures
§ 25:38	Civil enforcement of subpoenas
§ 25:39	Referral to the Department of Homeland Security Suspension and Debarment Official
§ 25:40	Referral to Cognizant Contracting Official or Attorney General
§ 25:41	Treatment of information and restrictions on use
§ 25:42	Procedures for protecting privacy and civil liberties
§ 25:43	Other procedural measures

## **V. HIPAA BREACH REGULATIONS**

§ 25:44	Applicability
§ 25:45	Notification to individuals
§ 25:46	Discovery of breaches

- § 25:47 Timing of notice
- § 25:48 Form of notice
- § 25:49 Notification to the media
- § 25:50 Issues to consider with the HIPAA media notice
- § 25:51 Notification to the Secretary
- § 25:52 Notification by a business associate
- § 25:53 Timing of notice—Business associate
- § 25:54 Form of notice
- § 25:55 Administrative requirements and burdens of proof
- § 25:56 FTC PHR Breach Rule
- § 25:57 Breach notification requirements
- § 25:58 Timing of notice
- § 25:59 Form of notice
- § 25:60 Notice to other entities
- § 25:61 Enforcement
- § 25:62 Effective date
- § 25:63 Centers for Medicare & Medicaid Services requirements

## **VI. GENERAL**

- § 25:64 Veterans Administration security breach and data security regulations

## **VII. SPECIFIC STATE PROVISIONS**

### **A. ALABAMA**

- § 25:65 Notice of security breach
- § 25:66 Timing of notice
- § 25:67 Form of notice
- § 25:68 Notice to other entities
- § 25:69 Entities that maintain data
- § 25:70 Enforcement
- § 25:71 Government entities
- § 25:72 Preemption

### **B. ALASKA**

- § 25:73 Notice of security breach
- § 25:74 Timing of disclosures
- § 25:75 Entities that maintain data
- § 25:76 Form of disclosures
- § 25:77 Notice to other entities
- § 25:78 Enforcement
- § 25:79 Effective date

## TABLE OF CONTENTS

### C. ARIZONA

- § 25:80 Notice of security breaches
- § 25:81 Timing of disclosures
- § 25:82 Notice to Attorney General
- § 25:83 Notice to others
- § 25:84 Form of disclosures
- § 25:85 Entities that maintain data
- § 25:86 Existing security policies
- § 25:87 Exemptions from disclosures
- § 25:88 Enforcement
- § 25:89 Preemption
- § 25:90 Effective date

### D. ARKANSAS

- § 25:91 Notice of security breaches
- § 25:92 Timing of notice
- § 25:93 Attorney general notice
- § 25:94 Entities that maintain data
- § 25:95 Existing security policies
- § 25:96 Enforcement

### E. CALIFORNIA

- § 25:97 Notice of security breaches
- § 25:98 Timing of disclosures
- § 25:99 Form of disclosures
- § 25:100 Notice to other entities
- § 25:101 Entities that maintain data
- § 25:102 Existing security policies
- § 25:103 Enforcement
- § 25:104 Preemption
- § 25:105 Additional burdens
- § 25:106 California's Office of Privacy Protection's  
recommendations
- § 25:107 State agency notice law—Notice of security breaches
- § 25:108 Timing of disclosures
- § 25:109 Form of disclosures
- § 25:110 Entities that maintain data
- § 25:111 Existing security policies
- § 25:112 California Department of Insurance guidance/notice

### F. COLORADO

- § 25:113 Notice of security breaches

## INFORMATION SECURITY AND PRIVACY

- § 25:114 Timing of disclosures
- § 25:115 Form of disclosures
- § 25:116 Entities that maintain data
- § 25:117 Existing security policies
- § 25:118 Exemption from disclosure
- § 25:119 Notice to other entities
- § 25:120 Enforcement
- § 25:121 Preemption
- § 25:122 Effective date

### G. CONNECTICUT

- § 25:123 Notice of security breaches
- § 25:124 Timing of disclosures
- § 25:125 Form of disclosures
- § 25:126 Notice to other entities
- § 25:127 Credit monitoring
- § 25:128 Entities that maintain data
- § 25:129 Existing security policies
- § 25:130 Exemptions from disclosures
- § 25:131 Enforcement
- § 25:132 Insurance data security law—Department of Insurance notice
- § 25:133 Insurance data security law—Implementation of written information security program
- § 25:134 Insurance data security law—Notice of security breach

### H. DELAWARE

- § 25:135 Notice of data security breaches
- § 25:136 Timing of disclosures
- § 25:137 Form of disclosures
- § 25:138 Entities that maintain data
- § 25:139 Existing security policies
- § 25:140 Notice to other entities
- § 25:141 Preemption
- § 25:142 Enforcement

### I. FLORIDA

- § 25:143 Notice of security breach
- § 25:144 Timing of disclosures
- § 25:145 Entities that maintain data
- § 25:146 Form of notice
- § 25:147 Preemption

## TABLE OF CONTENTS

- § 25:148 Notice to other entities
- § 25:149 Enforcement

### J. GEORGIA

- § 25:150 Notice of security breaches
- § 25:151 Timing of disclosures
- § 25:152 Form of notice
- § 25:153 Entities that maintain data
- § 25:154 Notice to other entities
- § 25:155 Telephone security breach
- § 25:156 Enforcement

### K. GUAM

- § 25:157 Notice of security breach
- § 25:158 Timing of notice
- § 25:159 Form of notice
- § 25:160 Entities that maintain data
- § 25:161 Existing security policies
- § 25:162 Preemption
- § 25:163 Enforcement

### L. HAWAII

- § 25:164 Notice of security breaches
- § 25:165 Timing of disclosures
- § 25:166 Form of disclosures
- § 25:167 Entities that maintain data
- § 25:168 Notice to other entities
- § 25:169 Enforcement
- § 25:170 Preemption
- § 25:171 Effective date

### M. IDAHO

- § 25:172 Notice of security breaches
- § 25:173 Timing of disclosures
- § 25:174 Form of disclosures
- § 25:175 Entities that maintain data
- § 25:176 Existing security policies
- § 25:177 Enforcement
- § 25:178 Preemption

### N. ILLINOIS

- § 25:179 Notice of security breach

## INFORMATION SECURITY AND PRIVACY

- § 25:180 Timing of disclosures
- § 25:181 Form of notice
- § 25:182 Entities that maintain data
- § 25:183 Form of notice
- § 25:184 Existing security policies
- § 25:185 State agency requirements
- § 25:186 Entities subject to the federal Health Insurance  
Portability and Accountability Act of 1996
- § 25:187 Enforcement

### O. INDIANA

- § 25:188 Notice of security breaches—State agencies
- § 25:189 Timing of disclosures—State agencies
- § 25:190 Form of disclosures—State agencies
- § 25:191 Notice to other entities—State agencies
- § 25:192 Notice of security breaches
- § 25:193 Timing of disclosures
- § 25:194 Entities that maintain data
- § 25:195 Form of disclosures
- § 25:196 Notice to other entities
- § 25:197 Existing security policies
- § 25:198 Enforcement

### P. IOWA

- § 25:199 Notice of security breach
- § 25:200 Entities that maintain data
- § 25:201 Timing of notice
- § 25:202 Form of notice
- § 25:203 Notice to other entities
- § 25:204 Exceptions
- § 25:205 Enforcement

### Q. KANSAS

- § 25:206 Notice of security breaches
- § 25:207 Timing of disclosures
- § 25:208 Form of disclosures
- § 25:209 Entities that maintain data
- § 25:210 Existing security policies
- § 25:211 Notice to other entities
- § 25:212 Enforcement
- § 25:213 Preemption

### R. KENTUCKY

- § 25:214 Notice of security breach

## TABLE OF CONTENTS

§ 25:215	Timing of disclosures
§ 25:216	Entities that maintain data
§ 25:217	Form of disclosures
§ 25:218	Notice to other entities
§ 25:219	Existing security policies
§ 25:220	Preemption

### S. LOUISIANA

§ 25:221	Notice of security breaches
§ 25:222	Entities that maintain data
§ 25:223	Exemptions from disclosures
§ 25:224	Timing of disclosures
§ 25:225	Form of disclosures
§ 25:226	Notice to other entities
§ 25:227	Existing policies
§ 25:228	Enforcement
§ 25:229	Preemption
§ 25:230	Effective date
§ 25:231	Litigation under Louisiana security breach law

### T. MAINE

§ 25:232	Notice of security breaches
§ 25:233	Timing of disclosures
§ 25:234	Form of disclosures
§ 25:235	Entities that maintain data
§ 25:236	Notice to other entities
§ 25:237	Preemption
§ 25:238	Enforcement

### U. MARYLAND

§ 25:239	Notice of security breaches
§ 25:240	Timing of disclosures
§ 25:241	Entities that maintain data
§ 25:242	Form of notice
§ 25:243	Notice to other entities
§ 25:244	Waiver of law
§ 25:245	Preemption
§ 25:246	Enforcement

### V. MASSACHUSETTS

§ 25:247	Notice of security breaches
§ 25:248	Form of notice

## INFORMATION SECURITY AND PRIVACY

- § 25:249 Entities that maintain data
- § 25:250 Notice to other entities
- § 25:251 Additional requirements on state agencies
- § 25:252 Timing of notice
- § 25:253 Effect of existing policies
- § 25:254 Enforcement
- § 25:255 Additional rulemaking

### W. MICHIGAN

- § 25:256 Notice of security breaches
- § 25:257 Entities that maintain data
- § 25:258 Timing of notice
- § 25:259 Form of disclosures
- § 25:260 Notice to other entities
- § 25:261 Exemptions from disclosures
- § 25:262 Enforcement
- § 25:263 Effective date
- § 25:264 Improper advertising of security breaches
- § 25:265 —Enforcement

### X. MINNESOTA

- § 25:266 Notice of security breaches
- § 25:267 Timing of disclosures
- § 25:268 Form of disclosures
- § 25:269 Entities that maintain data
- § 25:270 Existing security policies
- § 25:271 Preemption
- § 25:272 Notice to other entities
- § 25:273 Enforcement

### Y. MISSISSIPPI

- § 25:274 Notice of security breaches
- § 25:275 Timing of disclosures
- § 25:276 Entities that maintain data
- § 25:277 Form of notice
- § 25:278 Existing security policies
- § 25:279 Preemption
- § 25:280 Enforcement
- § 25:281 Effective date

### Z. MISSOURI

- § 25:282 Notice of security breach



## TABLE OF CONTENTS

§ 25:283	Timing of disclosures
§ 25:284	Entities that maintain data
§ 25:285	Form of notice
§ 25:286	Exemptions from disclosures
§ 25:287	Notice to other entities
§ 25:288	Existing security policies
§ 25:289	Preemption
§ 25:290	Enforcement

### AA. MONTANA

§ 25:291	Notice of security breaches
§ 25:292	Timing of disclosures
§ 25:293	Form of disclosures
§ 25:294	Entities that maintain data
§ 25:295	Notice to other entities
§ 25:296	Existing security policies
§ 25:297	Enforcement
§ 25:298	Effective date
§ 25:299	Insurance security breaches—Notice of security breaches
§ 25:300	—Entities that maintain data
§ 25:301	—Notice to other entities
§ 25:302	—Timing of notice
§ 25:303	—Development of procedures
§ 25:304	—Montana guidance

### BB. NEBRASKA

§ 25:305	Notice of security breaches
§ 25:306	Timing of disclosures
§ 25:307	Form of disclosures
§ 25:308	Notice to other entities
§ 25:309	Entities that maintain data
§ 25:310	Existing security policies
§ 25:311	Enforcement
§ 25:312	Preemption

### CC. NEVADA

§ 25:313	Notice of security breaches
§ 25:314	Timing of disclosures
§ 25:315	Form of disclosures
§ 25:316	Entities that maintain data
§ 25:317	Existing security policies
§ 25:318	Preemption

## INFORMATION SECURITY AND PRIVACY

- § 25:319 Notice to other entities
- § 25:320 Data collector's private right of action
- § 25:321 Enforcement
- § 25:322 Notice requirements on government entities

### DD. NEW HAMPSHIRE

- § 25:323 Notice of security breaches
- § 25:324 Timing of disclosures
- § 25:325 Form of disclosures
- § 25:326 Entities that maintain data
- § 25:327 Notice to other entities
- § 25:328 Enforcement
- § 25:329 Preemption
- § 25:330 Effective date
- § 25:331 Unauthorized disclosure of PHI
- § 25:332 Enforcement

### EE. NEW JERSEY

- § 25:333 Notice of security breaches
- § 25:334 Timing of disclosures
- § 25:335 Form of disclosures
- § 25:336 Entities that maintain data
- § 25:337 Exemptions from disclosure
- § 25:338 Existing security policies
- § 25:339 Notice to other entities
- § 25:340 Enforcement

### FF. NEW MEXICO

- § 25:341 Notice of security breach
- § 25:342 Timing of notice
- § 25:343 Entities that maintain data
- § 25:344 Form of notice
- § 25:345 Notice requirements
- § 25:346 Exemptions
- § 25:347 Notice to other entities
- § 25:348 Enforcement

### GG. NEW YORK

- § 25:349 Businesses
- § 25:350 Timing of disclosures
- § 25:351 Form of disclosures
- § 25:352 Entities that maintain data

## TABLE OF CONTENTS

§ 25:353	Notice to other entities
§ 25:354	Enforcement
§ 25:355	State agencies
§ 25:356	New York City security breaches

### HH. NORTH CAROLINA

§ 25:357	Notice of security breaches
§ 25:358	Timing of disclosures
§ 25:359	Form of disclosures
§ 25:360	Entities that maintain data
§ 25:361	Notice to other entities
§ 25:362	Existing security policies
§ 25:363	Enforcement

### II. NORTH DAKOTA

§ 25:364	Notice of security breaches
§ 25:365	Timing of disclosures
§ 25:366	Form of disclosures
§ 25:367	Notice to other entities
§ 25:368	Entities that maintain data
§ 25:369	Existing security policies
§ 25:370	Enforcement

### JJ. OHIO

§ 25:371	Notice of security breach
§ 25:372	Timing of disclosures
§ 25:373	Form of disclosures
§ 25:374	Entities that maintain data
§ 25:375	Notice to other entities
§ 25:376	Enforcement
§ 25:377	Preemption
§ 25:378	Ohio guidance
§ 25:379	Governmental entities—Notice of security breach
§ 25:380	—Timing of disclosures
§ 25:381	—Form of disclosures
§ 25:382	—Entities that maintain data
§ 25:383	—Notice to other entities
§ 25:384	—Enforcement

### KK. OKLAHOMA

§ 25:385	Notice of security breach
§ 25:386	Timing of disclosures

## INFORMATION SECURITY AND PRIVACY

- § 25:387 Form of disclosures
- § 25:388 Entities that maintain data
- § 25:389 Existing security policies
- § 25:390 Enforcement
- § 25:391 Effective date

### LL. OREGON

- § 25:392 Notice of security breach
- § 25:393 Timing of notice
- § 25:394 Entities that maintain data
- § 25:395 Form of notice
- § 25:396 Notice to other entities
- § 25:397 Exceptions
- § 25:398 Enforcement

### MM. PENNSYLVANIA

- § 25:399 Notice of security breach
- § 25:400 Timing of notice
- § 25:401 Form of notice
- § 25:402 Entities that maintain data
- § 25:403 Notice to other entities
- § 25:404 Preemption
- § 25:405 Existing security policies
- § 25:406 Enforcement

### NN. PUERTO RICO

- § 25:407 Notice of security breach
- § 25:408 Timing of notice
- § 25:409 Notice to other entities
- § 25:410 Entities that maintain data
- § 25:411 Form of notice
- § 25:412 Existing security policies
- § 25:413 Public entities
- § 25:414 Enforcement
- § 25:415 Regulations
- § 25:416 Regulations—Entities that maintain data
- § 25:417 Regulations—Timing of notice
- § 25:418 Regulations—Form of notice
- § 25:419 Regulations—Enforcement

### OO. RHODE ISLAND

- § 25:420 Notification of breach

## TABLE OF CONTENTS

§ 25:421	Timing of notice
§ 25:422	Notice to other entities
§ 25:423	Form of notice
§ 25:424	Effect of other policies
§ 25:425	Preemption
§ 25:426	Enforcement
§ 25:427	Rhode Island Division of Insurance

### PP. SOUTH CAROLINA

§ 25:428	Private entities—Notice of security breach
§ 25:429	—Timing of disclosure
§ 25:430	—Entities that maintain data
§ 25:431	—Form of notice
§ 25:432	—Existing security policies
§ 25:433	—Enforcement
§ 25:434	—Preemption
§ 25:435	—Notice to other entities
§ 25:436	—Effective date
§ 25:437	Agencies—Notice of security breach
§ 25:438	—Timing of disclosure
§ 25:439	—Entities that maintain data
§ 25:440	—Form of notice
§ 25:441	—Effect of existing procedures
§ 25:442	—Enforcement
§ 25:443	—Notice to other entities
§ 25:444	—Effective date
§ 25:445	Consumer-credit-reporting agency—Enforcement

### QQ. SOUTH DAKOTA

§ 25:446	Notice of security breach
§ 25:447	Timing of disclosures
§ 25:448	Notice to other entities
§ 25:449	Form of notice
§ 25:450	Existing security policies
§ 25:451	Enforcement
§ 25:452	Preemption

### RR. TENNESSEE

§ 25:453	Notice of security breaches
§ 25:454	Timing of disclosures
§ 25:455	Form of disclosures
§ 25:456	Entities that maintain data
§ 25:457	Existing security policies

## INFORMATION SECURITY AND PRIVACY

- § 25:458 Notice to other entities
- § 25:459 Exemptions from disclosures
- § 25:460 Enforcement

### SS. TEXAS

- § 25:461 Notice of security breaches
- § 25:462 Timing of disclosures
- § 25:463 Form of disclosures
- § 25:464 Entities that maintain data
- § 25:465 Existing security policies
- § 25:466 Notification to other entities
- § 25:467 Enforcement
- § 25:468 State and local agency breach notification requirements

### TT. UTAH

- § 25:469 Notice of security breach
- § 25:470 Timing of notice
- § 25:471 Entities that maintain data
- § 25:472 Form of notice
- § 25:473 Effect of existing policies
- § 25:474 Preemption
- § 25:475 Enforcement

### UU. VERMONT

- § 25:476 Notice of security breaches
- § 25:477 Timing of disclosures
- § 25:478 Entities that maintain data
- § 25:479 Form of disclosures
- § 25:480 Notice to other entities
- § 25:481 Preemption
- § 25:482 Enforcement
- § 25:483 Enforcement against government entities
- § 25:484 Vermont Attorney General guidance

### VV. VIRGIN ISLANDS

- § 25:485 Notice of security breach
- § 25:486 Timing of notice
- § 25:487 Form of notice
- § 25:488 Entities that maintain data
- § 25:489 Existing security policies

### WW. VIRGINIA

- § 25:490 Notice of security breaches

## TABLE OF CONTENTS

§ 25:491	Timing of notice
§ 25:492	Form of disclosure
§ 25:493	Entities that maintain data
§ 25:494	Notice to other entities
§ 25:495	Existing security policies
§ 25:496	Exemptions from notice
§ 25:497	Employers and payroll service providers
§ 25:498	Enforcement
§ 25:499	Preemption
§ 25:500	Breach of medical information notification—Notice of security breach
§ 25:501	—Timing of disclosures
§ 25:502	—Form of disclosures
§ 25:503	—Entities that maintain data
§ 25:504	—Notice to other entities
§ 25:505	—Preemption

## XX. WASHINGTON

§ 25:506	Notice of security breaches
§ 25:507	Timing of disclosures
§ 25:508	Form of disclosures
§ 25:509	Notice to other entities
§ 25:510	Entities that maintain data
§ 25:511	Existing security policies
§ 25:512	Enforcement
§ 25:513	Other requirements

## YY. WASHINGTON D.C.

§ 25:514	Notice of security breach
§ 25:515	Timing of disclosures
§ 25:516	Form of notice
§ 25:517	Entities that maintain data
§ 25:518	Existing security policies
§ 25:519	Exemptions from disclosures
§ 25:520	Notice to other entities
§ 25:521	Enforcement

## ZZ. WEST VIRGINIA

§ 25:522	Notice of security breach
§ 25:523	Timing of notice
§ 25:524	Form of notice
§ 25:525	Entities that maintain data
§ 25:526	Notice to other entities

- § 25:527 Existing security policies
- § 25:528 Enforcement

### AAA. WISCONSIN

- § 25:529 Notice of security breach
- § 25:530 Entities that maintain data
- § 25:531 Timing of notice
- § 25:532 Form of notice
- § 25:533 Notice to other entities
- § 25:534 Preemption
- § 25:535 Wisconsin insurance guidance

### BBB. WYOMING

- § 25:536 Notice of security breaches
- § 25:537 Timing of disclosures
- § 25:538 Form of disclosures
- § 25:539 Enforcement
- § 25:540 Entities that maintain data
- § 25:541 Preemption

## Volume 3

## CHAPTER 26. VIDEO PRIVACY

### I. VIDEO PRIVACY ISSUES GENERALLY

- § 26:1 Introduction
- § 26:2 Video privacy and the Internet

### II. FEDERAL PROVISIONS

- § 26:3 Federal Video Privacy Protection Act (VPPA)
- § 26:4 VPPA—Requirements of court orders
- § 26:5 —Data destruction
- § 26:6 —Enforcement and damages
- § 26:7 —Litigation
- § 26:8 —Limitations on litigation
- § 26:9 —Vicarious liability
- § 26:10 —Who is a subscriber?
- § 26:11 —Are UDIDs PII?
- § 26:12 —Application to streaming video
- § 26:13 —Knowledge of violations under the VPPA/internet video



## TABLE OF CONTENTS

- § 26:14 Federal Cable TV Privacy Act of 1984
- § 26:15 —Restrictions on disclosure
- § 26:16 —Governmental entities' right to obtain information
- § 26:17 —Subscriber access to information
- § 26:18 —Destruction of information
- § 26:19 —Enforcement
- § 26:20 —Disclosure
- § 26:21 VPPA—Third-party transfers and intra-corporate transfers—No duty of minimization under the VPPA
- § 26:22 —No transfer to third parties based upon joint account

## III. SPECIFIC STATE PROVISIONS

### A. CALIFORNIA

- § 26:23 Restrictions on satellite and cable television corporations
- § 26:24 Prohibition of disclosure by persons providing video recording sales or rentals without written consent
- § 26:25 Enforcement

### B. CONNECTICUT

- § 26:26 Videotape privacy

### C. MICHIGAN

- § 26:27 Michigan video protection law—A summary of differences from the VPPA
- § 26:28 Michigan video protection law
- § 26:29 Standing under Michigan's video protection law

### D. MINNESOTA

- § 26:30 Videotape privacy laws
- § 26:31 Form of consent
- § 26:32 Exclusion from evidence
- § 26:33 Destruction of information
- § 26:34 Refusal of service
- § 26:35 Civil liability

### E. NEW JERSEY

- § 26:36 Cable Subscriber Privacy Protection Act
- § 26:37 Restrictions on disclosures
- § 26:38 Civil enforcement
- § 26:39 Revocation of consent

## INFORMATION SECURITY AND PRIVACY

- § 26:40 Notice requirements
- § 26:41 Destruction of personally identifiable information
- § 26:42 Disclosure of names and addresses
- § 26:43 Disclosures at the request of the customer
- § 26:44 Correction of information
- § 26:45 Upstream communications
- § 26:46 Permitted monitoring
- § 26:47 Use of information to collect debts
- § 26:48 Examination of aggregated data
- § 26:49 Civil enforcement

### F. NEW YORK

- § 26:50 Video tape rental records
- § 26:51 Video tape sales records
- § 26:52 Enforcement of the restrictions upon disclosure of video tape rental and sales records

### G. TENNESSEE

- § 26:53 Video Consumer Privacy Act

### H. WASHINGTON D.C.

- § 26:54 Cable privacy law

## IV. CABLE PRIVACY AND ISPS

- § 26:55 Cable privacy and ISPs

## CHAPTER 27. RESTRICTIONS UPON STATE AGENCIES

### I. OVERVIEW

- § 27:1 Introduction
- § 27:2 Use of email by public employees
- § 27:3 First Amendment issues and spam filters
- § 27:4 Public records acts and privacy
- § 27:5 Public records acts and the attorney-client privilege
- § 27:6 Metadata as a public record
- § 27:7 Cell phone records do not fall within FOIA
- § 27:8 Public records and cell phones—Potentially a different answer in some states
- § 27:9 —Application to personal devices if texts used for work purposes

## TABLE OF CONTENTS

### II. FEDERAL RESTRICTIONS

- § 27:10 FOIA/Public Records Acts
- § 27:11 Glomar exceptions
- § 27:12 Privacy Act of 1974—Conditions of disclosure
- § 27:13 —Accounting of disclosures
- § 27:14 —Access to records
- § 27:15 —Agency requirements
- § 27:16 —Agency regulations
- § 27:17 —Civil enforcement
- § 27:18 —Litigation issues and the Privacy Act
- § 27:19 —Privacy Act and damages
- § 27:20 —Legal guardians
- § 27:21 —Criminal enforcement
- § 27:22 —General exemptions
- § 27:23 —Archival records
- § 27:24 —Government contractors
- § 27:25 —Mailing lists
- § 27:26 —Matching agreements
- § 27:27 —Verification and opportunity to contest findings
- § 27:28 —Sanctions
- § 27:29 —Reporting requirements
- § 27:30 —Effect of other laws
- § 27:31 —Data Integrity Boards
- § 27:32 Privacy Act regulations—Application to the Bureau of  
Consumer Financial Protection
- § 27:33 —Intent of Act
- § 27:34 —Procedures for requests pertaining to individual  
records
- § 27:35 —Times, places and requirements for identification of  
the individual making the request
- § 27:36 —Request for corrections or amendments
- § 27:37 —Notification of dispute
- § 27:38 —Disclosure of records to third parties
- § 27:39 —Accounting of disclosures
- § 27:40 —Fees
- § 27:41 Rehabilitation Act Amendments of 1986—Electronic  
and information technology
- § 27:42 — —Electronic and information technology standards
- § 27:43 — —Exemption for national security systems
- § 27:44 — —Construction of the law
- § 27:45 — —Technical assistance
- § 27:46 — —Agency evaluations
- § 27:47 — —Reports
- § 27:48 — —Cooperation

## INFORMATION SECURITY AND PRIVACY

- § 27:49 — —Enforcement
- § 27:50 Driver's Privacy Protection Act
- § 27:51 —Resale or redisclosure of information
- § 27:52 —Criminal and civil enforcement
- § 27:53 —Union activity
- § 27:54 —Liquidated damages under the DPPA
- § 27:55 —Knowledge of impermissible purpose under the DPPA
- § 27:56 —Multiple purposes under the DPPA can create a violation
- § 27:57 —No requirement of actual damages under the DPPA
- § 27:58 —Litigation—Reseller liability
- § 27:59 The Privacy Protection Act
- § 27:60 —Work product materials
- § 27:61 —Other documents
- § 27:62 —Civil remedies
- § 27:63 —No exclusion of evidence
- § 27:64 —Attorney General regulations
- § 27:65 Rehabilitation Act of 1973 and electronic and information technology accessibility regulations
- § 27:66 —Exceptions
- § 27:67 —Software applications and operating systems
- § 27:68 —Web-based Intranet and Internet information and applications
- § 27:69 —Telecommunications products
- § 27:70 —Video and multimedia products
- § 27:71 —Self-contained, closed products
- § 27:72 —Desktop and portable computers
- § 27:73 —Information, documentation, and support
- § 27:74 —Additional requirements

### III. STATE SPECIFIC PROVISIONS

#### A. ARIZONA

- § 27:75 Anti-identification procedures
- § 27:76 Internet privacy for state agencies and disclosures on websites

#### B. ARKANSAS

- § 27:77 E-mails and public record laws
- § 27:78 Postsecondary institution electronic communication privacy policy

#### C. CALIFORNIA

- § 27:79 Information Practices Act of 1977

## TABLE OF CONTENTS

§ 27:80	—Contents of records
§ 27:81	—Notice
§ 27:82	—Maintenance of records
§ 27:83	—Contracts for the operation and maintenance of records
§ 27:84	—Rules of conduct
§ 27:85	—Safeguards
§ 27:86	—Designation of employee responsible for agency compliance
§ 27:87	—Department of Justice review
§ 27:88	—Disclosure of personal information
§ 27:89	—Exceptions to disclosures
§ 27:90	—Disclosures related to advocacy for persons with disabilities
§ 27:91	—Accounting for disclosures
§ 27:92	—Motor vehicles
§ 27:93	—Retention of accounting and original documents
§ 27:94	—Maintenance of records
§ 27:95	—Costs and fees for records
§ 27:96	—Inspection of personal information in records
§ 27:97	—Amendment of records
§ 27:98	—Confidentiality of sources
§ 27:99	—Exceptions for records regarding property rights
§ 27:100	—Restrictions on disclosure to subject of information
§ 27:101	—Exceptions to access
§ 27:102	—Disclosure of personal information relating to others
§ 27:103	—Civil remedies
§ 27:104	—Remedies for failure to maintain records
§ 27:105	—Litigation related to personnel actions
§ 27:106	—Criminal enforcement
§ 27:107	—Restrictions on commercial distribution
§ 27:108	—Disclosure of license holder's information
§ 27:109	—Removal from mailing requests
§ 27:110	—Requirements placed on the Director of General Services
§ 27:111	—Disclosure of information related to liens
§ 27:112	—Disclosure of information to the district attorney
§ 27:113	—Release of information by the State Board of Equalization
§ 27:114	—Discovery by law enforcement
§ 27:115	—Restrictions on modifications
§ 27:116	—Exemptions for other laws
§ 27:117	The Brown Act
§ 27:118	—Teleconferencing requirements

## INFORMATION SECURITY AND PRIVACY

- § 27:119 —Secret votes
- § 27:120 —Reimbursement
- § 27:121 —Additional requirements and exemptions
- § 27:122 Public Records Act
- § 27:123 —Elected officials
- § 27:124 —Inspection requirements
- § 27:125 —Notification of denial of request
- § 27:126 —Additional voluntary requirements
- § 27:127 —Assistance to members of the public
- § 27:128 —Exemption for certain records
- § 27:129 —Education employees and disclosures of addresses and phone numbers
- § 27:130 —Voter registration information and confidentiality
- § 27:131 —Disclosure of public records
- § 27:132 —Disclosure of employment contracts
- § 27:133 —Computer software
- § 27:134 —Broker-dealer license information
- § 27:135 —Information regarding corporate facilities
- § 27:136 —Disclosure of utility customer information
- § 27:137 —Exemption from disclosure related to reproductive health services facilities
- § 27:138 —Enforcement
- § 27:139 —Interaction with California’s electronically collected personal information law
- § 27:140 —Disclosure of legal memorandum
- § 27:141 —Justification for withholding records
- § 27:142 —Purpose of request irrelevant
- § 27:143 —Enforcement
- § 27:144 —Exemption of records of complaints
- § 27:145 —District attorneys and inspection or copying nonexempt public records
- § 27:146 —Libraries supported by public funds
- § 27:147 —Sale, exchange or otherwise providing records subject to disclosure to private entities
- § 27:148 —Electronically collected personal information
- § 27:149 —Closed sessions law
- § 27:150 —Special requirements regarding the Public Utilities Commission
- § 27:151 —Closed sessions based upon advice of counsel
- § 27:152 —Record of topics discussed and decisions made at closed sessions
- § 27:153 —Closed sessions and responses to confidential final draft audit reports
- § 27:154 —Disclosure of nature of closed session
- § 27:155 —Closed session of the Gambling Control Commission

## TABLE OF CONTENTS

§ 27:156	—Disorderly conduct
§ 27:157	—Fees
§ 27:158	Restrictions upon Internet use on state computer
§ 27:159	Disclosure of private information—Appointed officials
§ 27:160	Privacy policy—State departments and agencies
§ 27:161	Rules of court regarding access to trial court records
§ 27:162	—Application and scope of rules
§ 27:163	—General right of access
§ 27:164	—Remote electronic access in extraordinary criminal cases
§ 27:165	—Access on a case-by-case basis
§ 27:166	—Bulk distribution
§ 27:167	—Off-site access
§ 27:168	—Limitations and conditions
§ 27:169	—Conditions of use by persons accessing records
§ 27:170	—Notices to persons accessing records
§ 27:171	—Access policy
§ 27:172	—Contracts with vendors
§ 27:173	—Fees for access
§ 27:174	—Electronic access to court calendars
§ 27:175	—Minimum contents for electronically accessible court calendars, indexes, and registers of actions
§ 27:176	—Information that must be excluded from court calendars, indexes, and registers of actions
§ 27:177	City of San Francisco private information law
§ 27:178	—Enforcement

## D. COLORADO

§ 27:179	Information security
§ 27:180	Privacy policy

## E. DELAWARE

§ 27:181	Privacy policy requirements
----------	-----------------------------

## F. IDAHO

§ 27:182	Inmate access to personal information
----------	---------------------------------------

## G. ILLINOIS

§ 27:183	Internet Privacy Task Force
----------	-----------------------------

## H. IOWA

§ 27:184	Fair Information Practices Act
----------	--------------------------------

I. MAINE

§ 27:185 Information technology leadership

J. MARYLAND

§ 27:186 Requests for changes to public records

§ 27:187 Review

§ 27:188 Civil enforcement

§ 27:189 Criminal enforcement

§ 27:190 Immunity

K. MICHIGAN

§ 27:191 Retention and disclosure of personally identifiable information

L. MINNESOTA

§ 27:192 Restrictions

M. MONTANA

§ 27:193 Collection of personally identifiable information

§ 27:194 —Requirements

N. NEVADA

§ 27:195 Disclosure of personal information

O. NEW YORK

§ 27:196 Collection and disclosure of personal information

P. NORTH CAROLINA

§ 27:197 Government restrictions

Q. OHIO

§ 27:198 Disclosure of personally identifiable information

§ 27:199 Restrictions on use of personal information

§ 27:200 Rights of individuals

§ 27:201 Enforcement

R. SOUTH CAROLINA

§ 27:202 Family Privacy Protection Act of 2002

§ 27:203 Restrictions on websites



## TABLE OF CONTENTS

- § 27:204 Obtaining personal information from a state agency for commercial solicitation

### S. UTAH

- § 27:205 Collection of personally identifiable information
- § 27:206 Restrictions on court websites

### T. VIRGINIA

- § 27:207 Government data collection and dissemination

### U. WASHINGTON

- § 27:208 Disclosure of personal information
- § 27:209 Personal information under Washington law

## CHAPTER 28. CONSTITUTIONAL AND STATUTORY ISSUES—PRIVACY RIGHTS AND RESTRICTIONS

- § 28:1 Introduction

### I. FEDERAL PROVISIONS

- § 28:2 Fourth Amendment and privacy
- § 28:3 —Geolocation data—*U.S. v. Jones*
- § 28:4 The *Leon* warrant exception and wiretap warrants
- § 28:5 Searches of cell phones, including incident to arrest and probationary exceptions
- § 28:6 Cell phone privacy and third parties
- § 28:7 Text message privacy
- § 28:8 Limitations on collection of email
- § 28:9 Metadata and photos
- § 28:10 International email issues and ISPs
- § 28:11 Information from devices in cars
- § 28:12 Fourteenth Amendment and privacy
- § 28:13 Computer searches of home computers
- § 28:14 Fourth Amendment and an “untimely” search of a computer
- § 28:15 Defendant’s right to computer searches
- § 28:16 Providing a computer to a third party for repairs as a waiver of privacy
- § 28:17 Anonymous computers and warrants
- § 28:18 Peer-to-peer and privacy
- § 28:19 Computer searches and special needs exceptions to the warrant requirement

## INFORMATION SECURITY AND PRIVACY

- § 28:20 Warrantless search of computers of probationers
- § 28:21 Location data in a cell phone—Cell cite geolocation information—Post *U.S. v. Jones*
- § 28:22 GPS tracking by a public employer under the workplace exception
- § 28:23 Seizure of information beyond a warrant
- § 28:24 Reasonable expectation of privacy and false identities
- § 28:25 Rental cars and warrants
- § 28:26 Access to hotel records and warrants
- § 28:27 Requests for identification of online book purchasers
- § 28:28 Discovery of email addresses
- § 28:29 IP addresses and expectations of privacy
- § 28:30 Decryption and the Fifth Amendment
- § 28:31 Expungement of criminal records
- § 28:32 Warrants and videotaping
- § 28:33 Disclosure of health records
- § 28:34 Constitutional issues and collection of prescription information
- § 28:35 OTC medications and privacy
- § 28:36 Implied consent in a dispute resolution process
- § 28:37 Federal regulations of personnel records
- § 28:38 Federal Video Voyeur Act
- § 28:39 Videotaping
- § 28:40 Searches due to terrorist concerns on public transportation
- § 28:41 Border searches generally
- § 28:42 Searches of computers at borders

## II. STATE PROVISIONS

### A. ALASKA

- § 28:43 Constitutional right of privacy

### B. ARIZONA

- § 28:44 Constitutional right to privacy
- § 28:45 Posting of personal information on the World Wide Web
- § 28:46 Enforcement

### C. CALIFORNIA

- § 28:47 Common law and constitutional bases of privacy
- § 28:48 Reproductive health service facility employees—  
Posting of information
- § 28:49 —Exceptions due to the CDA

## TABLE OF CONTENTS

- § 28:50 —Enforcement
- § 28:51 —Sale or trade of information regarding employees of reproductive health services facilities
- § 28:52 —Enforcement
- § 28:53 Information encoded on a driver's license
- § 28:54 Physical invasion of privacy
- § 28:55 Personnel records of peace officers
- § 28:56 Restrictions on local summary criminal history
- § 28:57 —Exception for public utilities
- § 28:58 — —Enforcement
- § 28:59 —Compelling need
- § 28:60 —Fingerprint records
- § 28:61 —Fees for providing information
- § 28:62 —Exceptions
- § 28:63 —Other provisions
- § 28:64 The California Consumer Privacy Act of 2018 is discussed in greater detail in chapter 29.

### D. FLORIDA

- § 28:65 Constitutional right to privacy

### E. HAWAII

- § 28:66 Constitutional right of privacy

### F. ILLINOIS

- § 28:67 Constitutional right of privacy
- § 28:68 Disclosure of customer information to law-enforcement agencies
- § 28:69 Biometric Information Privacy Act
- § 28:70 —Enforcement
- § 28:71 —Construction with other laws

### G. LOUISIANA

- § 28:72 Constitutional right of privacy

### H. MINNESOTA

- § 28:73 Constitutional right of privacy

### I. MISSOURI

- § 28:74 Posting of information on the Internet

J. MONTANA

§ 28:75 Constitutional right of privacy

K. NEW JERSEY

§ 28:76 Constitutional right of privacy

§ 28:77 Restrictions on recording devices in cars

L. NEW YORK

§ 28:78 Statutory right of privacy

M. OREGON

§ 28:79 Personal information regarding public investigators

N. RHODE ISLAND

§ 28:80 Statutory right of privacy

§ 28:81 Interaction with government disclosure laws

§ 28:82 Civil enforcement

O. SOUTH CAROLINA

§ 28:83 Constitutional right of privacy

P. TEXAS

§ 28:84 Restrictions on disclosure of information regarding  
attorneys

§ 28:85 Capture or use of biometric identifier

§ 28:86 —Enforcement

Q. WASHINGTON

§ 28:87 Constitutional right of privacy

§ 28:88 Unlawful release of court and law-enforcement  
employee information

R. WISCONSIN

§ 28:89 Statutory right of privacy

§ 28:90 Wisconsin GPS law

TABLE OF CONTENTS

**CHAPTER 29. U.S. STATE GENERAL  
PRIVACY LAWS**

**I. CALIFORNIA CONSUMER PRIVACY ACT OF 2018  
(THE “CCPA”)**

§ 29:1	General rights
§ 29:2	Consumer rights
§ 29:3	Employee Exemption
§ 29:4	Response to consumer request
§ 29:5	Business disclosure to service provider exemption
§ 29:6	Collection or retention of personal information not otherwise collected or retained in ordinary course of business
§ 29:7	Rights and freedoms of other consumers
§ 29:8	B-to-B exemption
§ 29:9	Civil action—Remedies
§ 29:10	—Requirements to bring action
§ 29:11	Attorney General guidance; civil action brought by Attorney General; amount and allocation of penalties
§ 29:12	Adoption of regulations; public participation; subject matter; enforcement actions
§ 29:13	Void and unenforceable provisions of contract or agreement
§ 29:14	Liberal construction of title
§ 29:15	Construction with federal law, United States Constitution, and California Constitution
§ 29:16	Operative date
§ 29:17	Severability
§ 29:18	CCPA regulations—Title and scope
§ 29:19	—Overview of required notices
§ 29:20	—Notice at collection of personal information
§ 29:21	—Notice of right to opt-out of sale of personal information
§ 29:22	—Notice of financial incentive
§ 29:23	—Privacy policy
§ 29:24	—Methods for submitting requests to know and requests to delete
§ 29:25	—Responding to requests to know and requests to delete
§ 29:26	—Responding to requests to know
§ 29:27	—Responding to requests to delete
§ 29:28	—Service providers
§ 29:29	—Requests to opt-out

## INFORMATION SECURITY AND PRIVACY

- § 29:30 —Requests to opt-in after opting out of the sale of personal information
- § 29:31 —Training; record-keeping
- § 29:32 —Requests to access or delete household information
- § 29:33 —General rules regarding verification
- § 29:34 —Verification for password-protected accounts
- § 29:35 —Verification for non-accountholders
- § 29:36 —Authorized agent
- § 29:37 —Minors under 13 years of age—Process for opting-in to sale of personal information
- § 29:38 —Minors 13 to 16 years of age
- § 29:39 —Notices to minors under 16 years of age
- § 29:40 —Discriminatory practices
- § 29:41 —Calculating the value of consumer data
- § 29:42 —Severability

## II. CALIFORNIA PRIVACY RIGHTS AND ENFORCEMENT ACT OF 2020 (THE “CPRA”)

- § 29:43 Overview

## III. COLORADO CONSUMER PROTECTION ACT

- § 29:44 Applicability
- § 29:45 Obligations
- § 29:46 Consumer personal data rights
- § 29:47 —The right to opt out
- § 29:48 —Right of access
- § 29:49 —Right to correction
- § 29:50 —Right to deletion
- § 29:51 —Right to data portability
- § 29:52 —Responding to consumer requests
- § 29:53 Processing de-identified data
- § 29:54 Duties of controllers—Duty of transparency
- § 29:55 —Duty of purpose specification
- § 29:56 —Duty of data minimization
- § 29:57 —Duty to avoid secondary use
- § 29:58 —Duty of care
- § 29:59 —Duty to avoid unlawful discrimination
- § 29:60 —Duty regarding sensitive data
- § 29:61 Data protection assessments—Attorney general access and evaluation—Definition
- § 29:62 Liability
- § 29:63 Enforcement—Penalties
- § 29:64 Rules
- § 29:65 Effective date

TABLE OF CONTENTS

**IV. VIRGINIA CONSUMER DATA PROTECTION  
ACT**

- § 29:66 Scope
- § 29:67 Personal data rights; consumers
- § 29:68 Data controller responsibilities; transparency
- § 29:69 Responsibility according to role; controller and processor
- § 29:70 Data protection assessments
- § 29:71 Processing de-identified data; exemptions
- § 29:72 Limitations
- § 29:73 Violations of chapter; civil penalties
- § 29:74 Enforcement; civil penalty
- § 29:75 Consumer Privacy Fund
- § 29:76 Effective date

**CHAPTER 30. RADIO FREQUENCY  
IDENTIFICATION AND TRACKING DEVICES**

- § 30:1 Introduction

**I. FEDERAL PROVISIONS**

- § 30:2 Mobile tracking devices
- § 30:3 Auto blackbox regulations

**II. STATE PROVISIONS**

**A. CALIFORNIA**

- § 30:4 Radio frequency identification law
- § 30:5 —Exceptions
- § 30:6 Subcutaneous tracking devices
- § 30:7 —Enforcement
- § 30:8 Automated license plate readers

**B. DELAWARE**

- § 30:9 Installation of car tracking devices

**C. MISSOURI**

- § 30:10 Employee microchips

**D. NORTH CAROLINA**

- § 30:11 Sex offender monitoring—Global positioning system requirements

- § 30:12 — —Enrollment requirements
- § 30:13 — —Court orders
- § 30:14 — —Request for termination of monitoring
- § 30:15 — —Failure to enroll—Tampering with devices
- § 30:16 — —Fees

#### E. TEXAS

- § 30:17 Unlawful installation of a tracking device

## CHAPTER 31. HEALTH INFORMATION AND PRIVACY AND SECURITY

- § 31:1 A preliminary matter—Health Information Technology for Economic and Clinical Health Act of 2009
- § 31:2 Health Information Technology for Economic and Clinical Health Act—Increased civil penalties

### I. INTRODUCTION

- § 31:3 Importance of health privacy
- § 31:4 Health record interoperability
- § 31:5 An overview of California’s approach
- § 31:6 Thoughts on interoperability models
- § 31:7 Personal health records
- § 31:8 Restrictions on disclosure of prescription drug information
- § 31:9 Disclosure of medical and prescription information to law enforcement
- § 31:10 HIPAA and discovery
- § 31:11 Liability for medical records disclosed outside the course and scope of employment
- § 31:12 Federal jurisdiction in HIPAA

### II. HIPAA

#### A. IN GENERAL

- § 31:13 Background
- § 31:14 Compliance dates for implementation of new or modified standards and implementation specifications
- § 31:15 Overview of HIPAA
- § 31:16 Inapplicability to employers
- § 31:17 An overview of recent changes to HIPAA
- § 31:18 Other rulemaking and guidance
- § 31:19 Changes to the definition of business associate



## TABLE OF CONTENTS

§ 31:20	Changes to the definition of electronic media
§ 31:21	Enforcement for business associates
§ 31:22	Time for compliance
§ 31:23	45 CFR §§ 160.306, 160.308, 160.310, and 160.402 regarding complaints to the secretary, compliance reviews, restrictions on certain conduct, and civil monetary penalties
§ 31:24	Factors for assessing civil monetary penalties
§ 31:25	Affirmative defenses and waiver of penalties
§ 31:26	Changes to the applicability language
§ 31:27	Changes regarding hybrid entities—Organizational requirements
§ 31:28	Security and safeguards
§ 31:29	Agreements with business associates
§ 31:30	Physical and technical safeguards
§ 31:31	Organizational requirements
§ 31:32	Policies procedures and documentation requirements
§ 31:33	Changes to the definition of electronic media
§ 31:34	Applicability of 45 CFR § 164.500
§ 31:35	Use and disclosures of protected health information
§ 31:36	Sale of protected health information and minimum necessary
§ 31:37	Satisfactory assurances and decedent's information
§ 31:38	Organizational requirements
§ 31:39	Uses and disclosures for treatment, payment, or health care operations
§ 31:40	Uses and disclosures for which authorization is required
§ 31:41	Genetic information
§ 31:42	Uses and disclosures requiring an opportunity to agree or to object
§ 31:43	Uses and disclosures for which an authorization or opportunity to agree or to object is not required
§ 31:44	Other requirements relating to uses and disclosures of protected health information
§ 31:45	Notice of privacy practices
§ 31:46	Rights to request privacy protection for protected health information
§ 31:47	Access of individuals to protected health information
§ 31:48	Administrative requirements
§ 31:49	Transition provisions
§ 31:50	Costs and benefits
§ 31:51	Privacy and security requirements
§ 31:52	New statutory requirements under ARRA
§ 31:53	Annual guidance

## INFORMATION SECURITY AND PRIVACY

- § 31:54 Education on health information privacy
- § 31:55 Application of knowledge elements associated with contracts
- § 31:56 Application of civil and criminal penalties
- § 31:57 Business associate contracts required for certain entities
- § 31:58 Improved enforcement under the Social Security Act
- § 31:59 Effective date and regulations
- § 31:60 Distribution of certain civil monetary penalties collected
- § 31:61 Establishment of methodology to distribute percentage of CMPS collected to harmed individuals
- § 31:62 Effective date
- § 31:63 Audits
- § 31:64 Relationship to other laws—HIPAA state preemption
- § 31:65 —HIPAA
- § 31:66 Construction of law
- § 31:67 Reports on compliance
- § 31:68 Study and report on application of privacy and security requirements to non-HIPAA covered entities
- § 31:69 Guidance on implementation specification to de-identify protected health information
- § 31:70 GAO report on treatment disclosures
- § 31:71 Report required
- § 31:72 Study
- § 31:73 Restrictions on certain disclosures and sales of health information; accounting of certain protected health information disclosures; access to certain information in electronic format
- § 31:74 Disclosures required to be limited to the limited data set or the minimum necessary
- § 31:75 Determination of minimum necessary
- § 31:76 Application of exceptions
- § 31:77 Exception
- § 31:78 Accounting of certain protected health information disclosures required if covered entity uses electronic health record
- § 31:79 Regulations
- § 31:80 Response to requests for accounting
- § 31:81 Effective date
- § 31:82 Prohibition on sale of EHRs or PHI
- § 31:83 Regulations regarding the prohibition of sale
- § 31:84 Effective date
- § 31:85 Access to certain information in electronic format
- § 31:86 Conditions on certain contacts as part of health care operations—Marketing

## TABLE OF CONTENTS

- § 31:87 Refill reminders
- § 31:88 Opportunity to opt out of fundraising
- § 31:89 Effective date
- § 31:90 Duties under HIPAA and state law
- § 31:91 Intent and violations of HIPAA
- § 31:92 Government violations of the Rehabilitation Act

### B. SCOPE OF HIPAA REGULATIONS AND ENFORCEMENT

- § 31:93 Statutory basis and purpose
- § 31:94 Applicability
- § 31:95 Modifications
- § 31:96 General rule and exceptions—Preemption
- § 31:97 Process for requesting exception determinations
- § 31:98 Duration of effectiveness of exception determinations
- § 31:99 Applicability
- § 31:100 Principles for achieving compliance
- § 31:101 Complaints to the Secretary
- § 31:102 Compliance reviews
- § 31:103 Responsibilities of covered entities and business associates
- § 31:104 Secretarial action regarding complaints and compliance reviews
- § 31:105 Investigational subpoenas and inquiries
- § 31:106 Investigational inquiries are non-public investigational proceedings conducted by the Secretary
- § 31:107 Refraining from intimidation or retaliation
- § 31:108 Basis for a civil money penalty
- § 31:109 Amount of a civil money penalty
- § 31:110 Violations of an identical requirement or prohibition
- § 31:111 Factors considered in determining the amount of a civil money penalty
- § 31:112 Affirmative defenses
- § 31:113 Waiver
- § 31:114 Limitations
- § 31:115 Authority to settle
- § 31:116 Penalty not exclusive
- § 31:117 Notice of proposed determination
- § 31:118 Failure to request a hearing
- § 31:119 Collection of penalty
- § 31:120 Notification of the public and other agencies
- § 31:121 Selected recent enforcement matters—In the Matter of Providence Health & Services

# INFORMATION SECURITY AND PRIVACY

- § 31:122 —In the Matter of CVS Pharmacy
- § 31:123 —In the Matter of Rite Aid
- § 31:124 —In the Matter of Management Services  
Organization Washington, Inc.
- § 31:125 —In the Matter of Cignet Health Center
- § 31:126 —In the Matter of the General Hospital Corporation  
and Massachusetts General Physicians  
Organization, Inc.
- § 31:127 —In the Matter of the Regents of the University of  
California, on behalf of the University of California  
at Los Angeles
- § 31:128 —In the Matter of BCBST
- § 31:129 —In the Matter of Phoenix Cardiac Surgery, P.C.
- § 31:130 —In the Matter of Alaska Department of Health and  
Human Services (DHSS)
- § 31:131 —In the Matter of Massachusetts Eye and Ear  
Infirmary
- § 31:132 —In the Matter of Hospice of North Idaho
- § 31:133 —In the Matter of Idaho State University
- § 31:134 —In the Matter of Shasta Regional Medical Center
- § 31:135 —In the Matter of WellPoint, Inc.
- § 31:136 —Affinity Health Plan, Inc.
- § 31:137 —Adult & Pediatric Dermatology, P.C.
- § 31:138 —In the Matter of Skagit County, Washington
- § 31:139 —In the Matter of QCA Health Plan, Inc.
- § 31:140 —In the Matter of Concentra Health Services
- § 31:141 —In the Matter of Columbia University in the City  
of New York
- § 31:142 —In the Matter of the New York and Presbyterian  
Hospital
- § 31:143 —In the Matter of Parkview Health System, Inc.
- § 31:144 —In the Matter of Anchorage Community Mental  
Health Services, Inc.
- § 31:145 —In the Matter of Cornell Prescription Pharmacy
- § 31:146 —In the Matter of St. Elizabeth's Medical Center
- § 31:147 —In the Matter of Cancer Care Group
- § 31:148 —In the Matter of Lahey Clinic Hospital, Inc.
- § 31:149 —In the Matter of Triple-S Management  
Corporation
- § 31:150 —In the Matter of the Board of Regents of the  
University of Washington
- § 31:151 —In the Matter of Lincare, Inc.
- § 31:152 —In the Matter of P.T., Pool & Land Physical  
Therapy, Inc.
- § 31:153 —In the Matter of North Care Memorial Health  
Care

## TABLE OF CONTENTS

§ 31:154	—In the Matter of Feinstein Institute for Medical Research
§ 31:155	—In the Matter of Raleigh Orthopaedic Clinic, P.A.
§ 31:156	—In the Matter of New York and Presbyterian Hospital
§ 31:157	—In the Matter of Catholic Health Care Services
§ 31:158	—In the Matter of Oregon Health & Science University
§ 31:159	—In the Matter of the University of Mississippi
§ 31:160	—In the Matter of Advocate Health Care Network
§ 31:161	—In re the Matter of Care New England Health System
§ 31:162	—In the Matter of St. Joseph Health
§ 31:163	—In the Matter of University of Massachusetts Amherst
§ 31:164	—In the Matter of Presence Health Network
§ 31:165	—In the Matter of MAPFRE Life Insurance Company of Puerto Rico
§ 31:166	—In the Matter of Children’s Medical Center of Dallas
§ 31:167	—In the Matter of South Broward Hospital District d/b/a Memorial Healthcare System
§ 31:168	—In the Matter of Metro Community Provider Network
§ 31:169	—In the Matter of Children’s Digestive Health, S.C.
§ 31:170	—In the Matter of CardioNet, Inc.
§ 31:171	—In the Matter of Memorial Herman Health System
§ 31:172	—In the Matter of St Luke’s-Roosevelt Hospital Center Inc.

## C. HEARINGS

§ 31:173	Applicability
§ 31:174	Hearing before an ALJ
§ 31:175	Rights of the parties
§ 31:176	Authority of the ALJ
§ 31:177	Ex parte contacts with the ALJ
§ 31:178	Prehearing conferences
§ 31:179	Authority to settle
§ 31:180	Discovery
§ 31:181	Exchange of witness lists, witness statements, and exhibits
§ 31:182	Subpoenas for attendance at hearing
§ 31:183	Fees
§ 31:184	Form, filing, and service of papers

## INFORMATION SECURITY AND PRIVACY

- § 31:185 Computation of time
- § 31:186 Motions
- § 31:187 Sanctions
- § 31:188 Collateral estoppel
- § 31:189 The hearing
- § 31:190 Statistical sampling
- § 31:191 Witnesses
- § 31:192 Evidence
- § 31:193 The record
- § 31:194 Post hearing briefs
- § 31:195 ALJ's decision
- § 31:196 Appeal of the ALJ's decision
- § 31:197 Stay of the Secretary's decision
- § 31:198 Harmless error

## D. SECURITY

- § 31:199 Statutory basis for security and privacy regulations
- § 31:200 Applicability of regulations
- § 31:201 Organizational requirements—Hybrid entities
- § 31:202 Safeguard requirements for affiliated covered entities
- § 31:203 Documentation
- § 31:204 Relationship to other portions of the regulations
- § 31:205 Applicability
- § 31:206 In general
- § 31:207 Security management process
  - § 31:208 —Risk analysis
  - § 31:209 —Risk management
  - § 31:210 —Sanction policy
  - § 31:211 —Information system activity review
- § 31:212 Assigned security responsibility
- § 31:213 Workforce security
  - § 31:214 —Authorization and/or supervision
  - § 31:215 —Workforce clearance procedure
  - § 31:216 —Termination procedures
- § 31:217 Information access management
  - § 31:218 —Isolating health care clearinghouse functions
  - § 31:219 —Access authorization
  - § 31:220 —Access establishment and modification
  - § 31:221 —Access establishment and modification implementation
- § 31:222 Security awareness and training
  - § 31:223 —Security reminders
  - § 31:224 —Protection from malicious software

## TABLE OF CONTENTS

§ 31:225	—Log-in monitoring
§ 31:226	—Password management
§ 31:227	Security incident procedures
§ 31:228	Contingency plan
§ 31:229	—Data backup plan
§ 31:230	—Disaster recovery plan
§ 31:231	—Emergency mode operation plan
§ 31:232	—Testing and revision procedures
§ 31:233	—Applications and data criticality analysis
§ 31:234	Evaluation
§ 31:235	Business associate contracts and other agreements
§ 31:236	Physical safeguards
§ 31:237	Device and media controls
§ 31:238	Technical safeguards
§ 31:239	Organizational requirements
§ 31:240	—Requirements for group health plans
§ 31:241	Policies and procedures

## E. PRIVACY

§ 31:242	Application of privacy provisions and penalties to business associates
§ 31:243	Applicability
§ 31:244	Application to health care clearinghouses
§ 31:245	Exceptions
§ 31:246	Uses and disclosures of deidentified protected health information
§ 31:247	Deidentification guidance
§ 31:248	Use and disclosure of genetic information for underwriting purposes
§ 31:249	Sale of protected health information
§ 31:250	Minimum necessary
§ 31:251	Uses and disclosures of PHI subject to an agreed upon restriction
§ 31:252	Creation of not individually identifiable information
§ 31:253	Disclosures to business associates
§ 31:254	Deceased individuals
§ 31:255	Personal representatives
§ 31:256	Adults and emancipated minors
§ 31:257	Deceased individuals
§ 31:258	Confidential communications
§ 31:259	Abuse, neglect, endangerment situations
§ 31:260	Processing and disclosures with notice
§ 31:261	Disclosures by whistleblowers and workforce member crime victims

- § 31:262 Substance use records
- § 31:263 Reproductive records
- § 31:264 Gender-affirming care

## F. USES AND DISCLOSURES

- § 31:265 Business associate contracts
- § 31:266 Other arrangements for business associate agreements
- § 31:267 Business associate contracts with subcontractors
- § 31:268 Requirements for group health plans
- § 31:269 Uses and disclosures by group health plans
- § 31:270 Requirements for a covered entity with multiple covered functions
- § 31:271 Uses and disclosures to carry out treatment, payment, or health care operations
- § 31:272 —Treatment, payment, or health care operations
- § 31:273 Uses and disclosures for which an authorization is required
- § 31:274 —Sale of protected health information
- § 31:275 —Valid authorization
- § 31:276 —Other requirements of authorizations
- § 31:277 Uses and disclosures requiring an opportunity for the individual to agree or to object
- § 31:278 Opportunity to object—Emergency circumstances
- § 31:279 Uses and disclosures for involvement in the individual's care and notification purposes
- § 31:280 Uses and disclosures for disaster relief purposes
- § 31:281 Uses and disclosures when the individual is deceased
- § 31:282 Uses and disclosures for which an authorization or opportunity to agree or object is not required
- § 31:283 —Uses and disclosures for public health activities
- § 31:284 —Disclosures about victims of abuse, neglect, or domestic violence
- § 31:285 —Uses and disclosures for health oversight activities
- § 31:286 —Disclosures for judicial and administrative proceedings
- § 31:287 — —Defining satisfactory assurances
- § 31:288 —Disclosures for law-enforcement purposes
- § 31:289 — —Limited information for identification and location purposes
- § 31:290 — —Victims of a crime
- § 31:291 — —Decedents
- § 31:292 — —Crime on premises



## TABLE OF CONTENTS

§ 31:293	— —Reporting crime in emergencies
§ 31:294	—Uses and disclosures about decedents
§ 31:295	—Uses and disclosures for cadaveric organ, eye, or tissue donation purposes
§ 31:296	—Uses and disclosures for research purposes
§ 31:297	— —Documentation of waiver approval
§ 31:298	—Uses and disclosures to avert a serious threat to health or safety
§ 31:299	—Uses and disclosures for specialized government functions—Military and veterans activities
§ 31:300	— —Separation or discharge from military service
§ 31:301	— —Foreign military personnel
§ 31:302	— —National security and intelligence activities
§ 31:303	— —Protective services for the President and others
§ 31:304	— —Medical suitability determinations
§ 31:305	— —Correctional institutions and other law-enforcement custodial situations
§ 31:306	— —Covered entities that are government programs providing public benefits
§ 31:307	—National Instant Criminal Background Check System.
§ 31:308	—Disclosures for workers' compensation
§ 31:309	Other requirements relating to uses and disclosures of protected health information—Deidentified data
§ 31:310	—Reidentification
§ 31:311	—Minimum necessary uses of PHI
§ 31:312	—Minimum necessary disclosures of PHI
§ 31:313	—Minimum necessary requirements for PHI
§ 31:314	—Limited data set
§ 31:315	—Uses for fundraising
§ 31:316	—Uses and disclosures for underwriting and related purposes
§ 31:317	—Verification requirements
§ 31:318	—Verification
§ 31:319	Notice of privacy practices for protected health information—Right to notice of privacy practices for PHI
§ 31:320	—Requirements for electronic notice
§ 31:321	—Joint notice by separate covered entities
§ 31:322	Rights to request privacy protection for PHI
§ 31:323	—Confidential communications requirements
§ 31:324	Access of individuals to PHI
§ 31:325	—Review of denial of access
§ 31:326	—Requests for access and timely action
§ 31:327	—Providing access

## INFORMATION SECURITY AND PRIVACY

- § 31:328 —Time and manner of access
- § 31:329 —Denial of access
- § 31:330 Amendment of PHI
- § 31:331 —Actions on notices of amendment
- § 31:332 —Documentation
- § 31:333 Accounting of disclosures of protected health information
- § 31:334 —Content of the accounting
- § 31:335 —Providing the accounting
- § 31:336 —Documentation
- § 31:337 Administrative requirements—Personal designation
- § 31:338 —Safeguards
- § 31:339 —Complaints to the covered entity
- § 31:340 —Documentation of complaints
- § 31:341 —Mitigation
- § 31:342 —Refraining from intimidating or retaliatory acts
- § 31:343 —Waiver of rights
- § 31:344 —Policies and procedures
- § 31:345 — —Changes to privacy practices stated in the notice
- § 31:346 — —Changes to other policies or procedures
- § 31:347 —Documentation
- § 31:348 —Retention period
- § 31:349 —Group health plans
- § 31:350 Transition provisions—Use and disclosure of information
- § 31:351 —Effect of prior contracts or other arrangements with business associates
- § 31:352 Compliance dates for initial implementation of the privacy standards
- § 31:353 Public records laws and HIPAA protections
- § 31:354 State Medicaid restrictions and HIPAA
- § 31:355 De-identified information
- § 31:356 Disclosures to business associates
- § 31:357 Restrictions and exceptions
- § 31:358 HIPAA and ex parte communications between physicians

## III. PROMOTION OF HEALTH INFORMATION TECHNOLOGY

- § 31:359 Office of the National Coordinator for Health Information Technology
- § 31:360 Certification of HIT
- § 31:361 Reports and publications

## TABLE OF CONTENTS

§ 31:362	Detailing of federal employees
§ 31:363	Appointment of Chief Privacy Officer
§ 31:364	HIT Policy Committee
§ 31:365	HIT Standards Committee
§ 31:366	Role of National Coordinator in the HIT Standards Committee
§ 31:367	Process for adoption of endorsed recommendations
§ 31:368	Adoption of standards, implementation specifications, and certification criteria
§ 31:369	Application and use of adopted standards and implementation specifications by federal agencies
§ 31:370	Voluntary application and use of adopted standards and implementation specifications
§ 31:371	Federal health information technology
§ 31:372	Transitions
§ 31:373	Relation to HIPAA privacy and security law
§ 31:374	Incentives for the use of health information technology
§ 31:375	Immediate funding
§ 31:376	Health information technology implementation assistance—Health information technology extension program
§ 31:377	—Health information technology research center
§ 31:378	Health information technology regional extension centers
§ 31:379	—Application review
§ 31:380	State grants to promote health information technology
§ 31:381	Required match of state grants
§ 31:382	Requirement of a strategic plan
§ 31:383	Use of funds
§ 31:384	Guidance and regulations
§ 31:385	Private sector contributions
§ 31:386	Matching requirements
§ 31:387	Effective date
§ 31:388	Demonstration program to integrate information technology into clinical education
§ 31:389	Financial support, evaluation, and reports
§ 31:390	Information technology professionals in health care
§ 31:391	General grant and loan provisions
§ 31:392	Private right of action—Availability
§ 31:393	First Amendment and restrictions on health data
§ 31:394	Prior restraints and private information
§ 31:395	Enforcement

#### **IV. PATIENT SAFETY AND QUALITY IMPROVEMENT ACT**

- § 31:396 Overview of Act
- § 31:397 Patient safety databases
- § 31:398 Patient safety organizations
- § 31:399 Confidentiality provisions
- § 31:400 Constitutional rights of privacy in certain medical  
records; disclosure to disciplinary boards
- § 31:401 Continued protection of information
- § 31:402 Limitations on disclosures to providers
- § 31:403 Limitations on adverse employment actions
- § 31:404 Civil enforcement
- § 31:405 Regulations

### **CHAPTER 32. STATE HEALTH INFORMATION AND PRIVACY AND SECURITY**

#### **I. INTRODUCTION**

- § 32:1 Importance of health privacy
- § 32:2 No duty on pharmacists related to identity theft

#### **II. SPECIFIC STATE LAWS**

##### **A. ALASKA**

- § 32:3 Electronic medical records

##### **B. ARIZONA**

- § 32:4 Communicable diseases—Confidentiality of  
information
- § 32:5 —Release of information to government entities
- § 32:6 —Form of authorization
- § 32:7 —Restrictions upon redisclosure
- § 32:8 —Applicability to death certificates
- § 32:9 —Disclosure to at-risk third parties
- § 32:10 —Inapplicability to entities governed by title 20
- § 32:11 —Exceptions for investigations
- § 32:12 —Disclosure pursuant to court order
- § 32:13 —Criminal enforcement
- § 32:14 —Civil penalties

##### **C. CALIFORNIA**

- § 32:15 Disclosures of medical information

## TABLE OF CONTENTS

§ 32:16	—Application of chapter
§ 32:17	—Restrictions and required disclosures
§ 32:18	—Permitted disclosures
§ 32:19	— —Disclosures for diagnosis or treatment
§ 32:20	— —Disclosures for billing
§ 32:21	— —Disclosures to committees
§ 32:22	— —Disclosures to the coroner and educational institutions
§ 32:23	— —Employment-related health care services
§ 32:24	— —Disclosures to insurers
§ 32:25	— —Disclosures to a probate investigator and organ procurement organizations
§ 32:26	— —Disclosures based upon federal law
§ 32:27	— —Anonymous data
§ 32:28	— —Disclosure to disease management programs
§ 32:29	— —Disclosure under other laws
§ 32:30	— —Disclosure via ethical conduct
§ 32:31	—Other disclosures
§ 32:32	—Limitations upon disclosures
§ 32:33	—Corporations that maintain medical information
§ 32:34	—Destruction of records
§ 32:35	—Disclosures by pharmaceutical companies
§ 32:36	—Treatment with psychotherapist
§ 32:37	— —Inapplicability to use of information by law enforcement
§ 32:38	—New restrictions on confidentiality effective 2015
§ 32:39	—Enforcement
§ 32:40	—California Medical Information Act (CMIA) litigation
§ 32:41	—Entity for enforcement
§ 32:42	—California data security
§ 32:43	—Creation of new entity
§ 32:44	—Enforcement under section 1280.1 of the Health and Safety Code
§ 32:45	—Restrictions on unauthorized access
§ 32:46	—Reporting obligations
§ 32:47	—Enforcement
§ 32:48	—Enforcement and regulations
§ 32:49	—Restrictions on California government employees
§ 32:50	AIDS status—General provisions
§ 32:51	—Restrictions and enforcement
§ 32:52	—Disclosure to health care providers
§ 32:53	—Preclusion of testing without consent
§ 32:54	—New additions regarding AIDS testing
§ 32:55	—Disclosures without consent

## INFORMATION SECURITY AND PRIVACY

- § 32:56 Requests by businesses for medical information—Oral requests
- § 32:57 —Written requests
- § 32:58 —Exemptions
- § 32:59 Disclosure of medical information to specified individuals
- § 32:60 Disclosure of medical information for disaster relief efforts
- § 32:61 Disclosure of medical information—Public disclosures of limited information
- § 32:62 Online privacy for reproductive health services providers
- § 32:63 —Soliciting or trading in names and private information
- § 32:64 —Exemptions for interactive computer services

### D. CONNECTICUT

- § 32:65 Confidentiality of pharmacy records
- § 32:66 Pharmacy rewards

### E. FLORIDA

- § 32:67 Ownership and control of patient records
- § 32:68 Exceptions
- § 32:69 Transfer of records
- § 32:70 Enforcement
- § 32:71 Fees

### F. HAWAII

- § 32:72 Restrictions on Pharmacy Benefits Managers and marketing

### G. MASSACHUSETTS

- § 32:73 Commonwealth of Massachusetts v. South Shore Hospital, Inc
- § 32:74 Commonwealth of Massachusetts v. Beth Israel Deaconess Medical Center, Inc.

### H. MICHIGAN

- § 32:75 Medical records—Records retention
- § 32:76 —Destruction of records
- § 32:77 —Enforcement
- § 32:78 —Ownership
- § 32:79 Health facilities—Patient records

## TABLE OF CONTENTS

- § 32:80 —Public record status
- § 32:81 —Disciplinary actions against health professionals—  
Reporting requirements
- § 32:82 —Exemption for peer review documents
- § 32:83 —Patient records—Contracting with third parties
- § 32:84 — —Termination of operations
- § 32:85 — —Ownership of medical records
- § 32:86 — —Enforcement

### I. NEW HAMPSHIRE

- § 32:87 Pharmacy disclosures—Restrictions
- § 32:88 — —New Hampshire and Maine laws held  
unconstitutional
- § 32:89 —Disclosures by clearinghouses
- § 32:90 Use and disclosure of PHI—Marketing and  
fundraising
- § 32:91 —Enforcement
- § 32:92 —Breach notice requirements
- § 32:93 Use and Disclosure of PHI—Health information  
organization
- § 32:94 —Unauthorized disclosure

### J. NORTH DAKOTA

- § 32:95 Health Information Organizations
- § 32:96 Voluntary participation in the health information  
organization—Prohibition on withholding care or  
benefits

### K. TENNESSEE

- § 32:97 Litigation protective orders

### L. TEXAS

- § 32:98 Medical records privacy—Health law
- § 32:99 —Applicability
- § 32:100 —Sovereign immunity
- § 32:101 —Covered entity
- § 32:102 —Duties of the executive commissioner
- § 32:103 —Protected health information not public
- § 32:104 —Exemptions—Partial exemption
- § 32:105 — —Processing payment transactions by financial  
institutions
- § 32:106 — —Nonprofit agencies
- § 32:107 — —Workers' compensation

## INFORMATION SECURITY AND PRIVACY

- § 32:108 — —Employee benefit plan
- § 32:109 — —American Red Cross
- § 32:110 — —Information relating to offenders with mental impairments
- § 32:111 — —Education records
- § 32:112 — —Crime victim compensation
- § 32:113 — —Access to and use of protected health information—Training required
- § 32:114 — —Consumer access to EHR
- § 32:115 — —Consumer information website
- § 32:116 — —Consumer complaint report by Attorney General
- § 32:117 — —Prohibited acts—Reidentified information
- § 32:118 — —Marketing uses of information
- § 32:119 — —Sale of protected health information prohibited; exceptions
- § 32:120 — —Notice and authorization required for electronic disclosure of protected health information; Exceptions
- § 32:121 — —Enforcement—Remedies
- § 32:122 — —Disciplinary action
- § 32:123 — —Exclusion from state programs
- § 32:124 — —Mitigation
- § 32:125 — —Audits of covered entities
- § 32:126 — —Funding

## M. VERMONT

- § 32:127 Restrictions on prescription drug marketing
- § 32:128 Enforcement

## N. WISCONSIN

- § 32:129 Healthcare records—Access
- § 32:130 — —Additional restrictions
- § 32:131 — —Preservation or destruction of patient health care records
- § 32:132 — —Preservation or destruction of patient health care record—Exceptions
- § 32:133 — —Applicability
- § 32:134 — —Contents of certain patient health care records
- § 32:135 — —Violations related to patient health care records—Enforcement
- § 32:136 — —Exceptions
- § 32:137 — —Additional restrictions contained in the State Alcohol, Drug Abuse, Developmental Disabilities and Mental Health Act



## TABLE OF CONTENTS

- § 32:138 —Confidentiality of patient health care records
- § 32:139 — —Other exceptions
- § 32:140 — —Other reports made without informed consent
- § 32:141 — —Redisclosure
- § 32:142 Willfulness under Wisconsin’s Medical Privacy Law

## CHAPTER 33. GENETIC PRIVACY

### I. INTRODUCTION

- § 33:1 Overview

### II. FEDERAL STATUTES

- § 33:2 Genetic privacy
- § 33:3 Genetic nondiscrimination in health insurance—  
Amendments to Employee Retirement Income  
Security Act Of 1974
- § 33:4 — —Limitations on genetic testing
- § 33:5 — —Prohibition on collection of genetic information
- § 33:6 — —Scope of application
- § 33:7 — —Genetic information regarding a fetus or embryo
- § 33:8 — —ERISA enforcement
- § 33:9 — —Rulemaking
- § 33:10 — —Effective date
- § 33:11 —Amendments to the Public Health Service Act—  
Discrimination in group premiums based upon  
genetic information
- § 33:12 — —Prohibition on collection of genetic information
- § 33:13 — —Restrictions on the collection of genetic  
information
- § 33:14 — —Application of certain requirements
- § 33:15 — —Applications to genetic information of a fetus or  
embryo
- § 33:16 — —Enforcement authority relating to genetic  
discrimination
- § 33:17 — —Prohibition of health discrimination on the basis  
of genetic information
- § 33:18 — —Prohibition on the use of genetic information in  
setting premium rates
- § 33:19 — —Prohibition on genetic information as preexisting  
condition
- § 33:20 — —Limitation on requesting or requiring genetic  
testing
- § 33:21 — —Research exception
- § 33:22 — —Prohibition on collection of genetic information

## INFORMATION SECURITY AND PRIVACY

- § 33:23 — —Enforcement
- § 33:24 — —Elimination of option of nonfederal governmental plans to be excepted from requirements concerning genetic information
- § 33:25 Regulations—Initial timing
- § 33:26 Genetic nondiscrimination in health insurance—  
Amendments to the Public Health Service Act—  
Effective date
- § 33:27 —Amendments to the Internal Revenue Code of 1986—No group-based discrimination on basis of genetic information
- § 33:28 — —Restrictions on the collection of genetic information
- § 33:29 — —Scope of application
- § 33:30 — —Enforcement
- § 33:31 — —Regulations and effective date
- § 33:32 —Amendments to Title XVII of the Social Security Act relating to medigap
- § 33:33 — —Limitations on genetic testing and genetic information
- § 33:34 — —Prohibition on collection of genetic information
- § 33:35 — —Requirements of group benefits; core group benefits; uniform outline of coverage
- § 33:36 — —Effective date and transiting provisions
- § 33:37 —Privacy and confidentiality—Amendments to HIPAA regulations—Enforcement
- § 33:38 Genetic nondiscrimination in employment—  
Employment discrimination
- § 33:39 —Improper acquisition of genetic information
- § 33:40 —Employment agency practices
- § 33:41 —Labor practices
- § 33:42 —Training programs
- § 33:43 —Confidentiality of genetic information
- § 33:44 —Enforcement
- § 33:45 —Prohibition on retaliation
- § 33:46 —No cause of action based upon disparate impact
- § 33:47 —Formation of a commission to study disparate impact
- § 33:48 —Medical information that is not genetic information
- § 33:49 —Additional regulations
- § 33:50 —Rules of construction

## III. SELECTED REGULATIONS

- § 33:51 Group health plans and genetic information—  
Statutory basis

## TABLE OF CONTENTS

- § 33:52 —Preexisting conditions
- § 33:53 —Discrimination against participants and beneficiaries based upon a health factor
- § 33:54 —Limitations on group health plans
- § 33:55 —Limitation on requesting or requiring genetic testing
- § 33:56 —Prohibitions on the collection of genetic information
- § 33:57 —Collection prior to or in connection with enrollment
- § 33:58 —Exception
- § 33:59 —Additional rules for group health plans
- § 33:60 —Additional restrictions on group health plans and health insurers
- § 33:61 Federal DNA collection laws
- § 33:62 —Collection and use of DNA identification information
- § 33:63 —Additional limitations
- § 33:64 —Enforcement
- § 33:65 —Privacy protection standards
- § 33:66 —Expungement of records
- § 33:67 —Privacy protections

## IV. STATE LAW

### A. ALASKA

- § 33:68 Genetic privacy
- § 33:69 Civil enforcement
- § 33:70 Criminal enforcement

### B. ARIZONA

- § 33:71 Genetic privacy

### C. ARKANSAS

- § 33:72 Genetic privacy

### D. CALIFORNIA

- § 33:73 Genetic privacy

### E. COLORADO

- § 33:74 Genetic privacy
- § 33:75 Application to insurers
- § 33:76 Civil enforcement

F. CONNECTICUT

§ 33:77 Restrictions on genetic testing

G. DELAWARE

§ 33:78 Genetic privacy  
§ 33:79 Retention of samples of genetic information  
§ 33:80 Access to genetic information  
§ 33:81 Conditions for disclosure to third parties  
§ 33:82 Scope of application  
§ 33:83 Parental rights  
§ 33:84 Enforcement

H. FLORIDA

§ 33:85 Genetic privacy

I. GEORGIA

§ 33:86 Genetic testing  
§ 33:87 Civil enforcement

J. HAWAII

§ 33:88 Genetic privacy

K. IDAHO

§ 33:89 Genetic privacy  
§ 33:90 Restrictions on employers  
§ 33:91 Enforcement  
§ 33:92 Insurance

L. ILLINOIS

§ 33:93 Genetic privacy  
§ 33:94 Exceptions  
§ 33:95 Use of genetic testing by employers  
§ 33:96 Disclosure of information  
§ 33:97 Civil enforcement

M. IOWA

§ 33:98 Restrictions on genetic testing  
§ 33:99 Additional restrictions  
§ 33:100 Adoption of rules  
§ 33:101 Enforcement

TABLE OF CONTENTS

§ 33:102 Exceptions

N. KANSAS

§ 33:103 Use of genetics tests in employment

O. LOUISIANA

§ 33:104 Restrictions on prenatal genetic testing

§ 33:105 Other restrictions

§ 33:106 Exemptions

§ 33:107 Enforcement

P. MAINE

§ 33:108 Employment discrimination

§ 33:109 Discrimination on the basis of genetic information or testing

Q. MARYLAND

§ 33:110 Use of genetic tests in employment

§ 33:111 Use of genetic tests

R. MASSACHUSETTS

§ 33:112 Genetic privacy

§ 33:113 Enforcement

§ 33:114 Exceptions

S. MICHIGAN

§ 33:115 Genetic privacy

T. MINNESOTA

§ 33:116 Genetic privacy

§ 33:117 —Exceptions

§ 33:118 Genetic testing in employment

§ 33:119 —Enforcement

U. MISSOURI

§ 33:120 Genetic privacy

V. NEBRASKA

§ 33:121 Restrictions on genetic testing

W. NEVADA

§ 33:122 Genetic privacy

## INFORMATION SECURITY AND PRIVACY

- § 33:123 Disclosure of genetic information
- § 33:124 Genetic information—Procedure to obtain consent
- § 33:125 —Enforcement

### X. NEW HAMPSHIRE

- § 33:126 Genetic information—General restrictions
- § 33:127 Restrictions upon use in employment
- § 33:128 Genetic testing in health insurance
- § 33:129 Civil enforcement

### Y. NEW JERSEY

- § 33:130 Genetic privacy
- § 33:131 —Data destruction requirements
- § 33:132 —Disclosure of identity
- § 33:133 —Notice to person tested
- § 33:134 —Regulations
- § 33:135 —Enforcement
- § 33:136 Genetic information—Insurance restrictions
- § 33:137 —Employment discrimination

### Z. NEW MEXICO

- § 33:138 Genetic privacy
- § 33:139 Genetic discrimination
- § 33:140 Rights of retention
- § 33:141 Enforcement

### AA. NEW YORK

- § 33:142 Genetic information—Restrictions on employment discrimination
- § 33:143 Genetic tests—New York Civil Rights Law
- § 33:144 —Confidentiality
- § 33:145 —Exceptions
- § 33:146 —Enforcement

### BB. NORTH CAROLINA

- § 33:147 Restrictions on genetic testing

### CC. OKLAHOMA

- § 33:148 Genetic nondiscrimination in employment
- § 33:149 —Enforcement
- § 33:150 —Exceptions

## TABLE OF CONTENTS

### DD. OREGON

- § 33:151 Genetic privacy
- § 33:152 —Rights of individuals
- § 33:153 —Inspection right
- § 33:154 —Disclosure of biological specimen or clinical  
individually identifiable health information
- § 33:155 —Disclosure of genetic information
- § 33:156 —Enforcement
- § 33:157 —Other requirements

### EE. RHODE ISLAND

- § 33:158 Genetic privacy

### FF. SOUTH CAROLINA

- § 33:159 Genetic privacy
- § 33:160 Genetic testing
- § 33:161 Enforcement

### GG. SOUTH DAKOTA

- § 33:162 Genetic testing and insurance
- § 33:163 Genetic information and employers

### HH. TEXAS

- § 33:164 Employment discrimination—Genetic privacy
- § 33:165 —Confidentiality of genetic information
- § 33:166 —Disclosure of genetic information with  
authorization
- § 33:167 —Disclosure of genetic test results to the individual
- § 33:168 —Destruction of genetic samples
- § 33:169 Licensing authorities—Uses of genetic information
- § 33:170 —Destruction of genetic material
- § 33:171 —Disclosure of genetic test results
- § 33:172 —Confidentiality of genetic information
- § 33:173 — —Exceptions
- § 33:174 —Disclosure of genetic information with  
authorization
- § 33:175 —Disclosure of genetic information—Enforcement
- § 33:176 Insurance restrictions and genetic privacy
- § 33:177 —Improper use of tests
- § 33:178 —Testing related to pregnancy
- § 33:179 —Destruction of genetic materials
- § 33:180 —Disclosure of genetic test results

## INFORMATION SECURITY AND PRIVACY

- § 33:181 —Confidentiality of genetic information
- § 33:182 — —Exceptions
- § 33:183 —Disclosure of genetic information with  
authorization
- § 33:184 —Enforcement

### II. UTAH

- § 33:185 Genetic privacy
- § 33:186 Restrictions on employers
- § 33:187 Restrictions upon health insurers
- § 33:188 Enforcement

### JJ. VERMONT

- § 33:189 Genetic privacy
- § 33:190 Genetic testing and employers
- § 33:191 Genetic testing and insurance
- § 33:192 Enforcement

### KK. VIRGINIA

- § 33:193 Genetic privacy

### LL. WASHINGTON

- § 33:194 Genetic privacy
- § 33:195 Genetic privacy litigation

### MM. WISCONSIN

- § 33:196 Use of genetic testing in employment situations
- § 33:197 Exceptions

## **CHAPTER 34. FEDERAL TRADE COMMISSION ACT AND ENFORCEMENT UNDER THE ACT**

- § 34:1 The FTC—A historical perspective
- § 34:2 The history of privacy enforcement
- § 34:3 The FTC's jurisdiction
- § 34:4 Understanding the theoretical basis of the FTC  
privacy enforcement
- § 34:5 Understanding Section 5
- § 34:6 Unfair or deceptive acts or practices—Rulemaking  
authority
- § 34:7 Deception



## TABLE OF CONTENTS

§ 34:8	—Likely to mislead
§ 34:9	—The act or practice must be considered from the perspective of the reasonable consumer
§ 34:10	—Materiality
§ 34:11	—Summarizing the deception elements
§ 34:12	—Deception and notice and choice models of enforcement
§ 34:13	Unfairness—Authority
§ 34:14	—The FTC’s December 1980 statement regarding unfairness
§ 34:15	—Consumer injury
§ 34:16	—Violation of public policy
§ 34:17	—Unethical or unscrupulous conduct
§ 34:18	—Distilling the Unfairness Statement
§ 34:19	—Unfairness and harm-based enforcement models
§ 34:20	—Accusearch and unfairness
§ 34:21	Individual liability
§ 34:22	Relief—Overview
§ 34:23	—Relief available under Section 53(b)
§ 34:24	—Remedies
§ 34:25	—FTC injunction limitations
§ 34:26	—Active concert and injunctive relief
§ 34:27	Department of Justice and Federal Trade Commission: Antitrust policy statement on sharing of cybersecurity information
§ 34:28	FTC—Privacy agenda
§ 34:29	Privacy and security cases brought by FTC—Section 5 cases—In the Matter of Geocities—Consumer privacy
§ 34:30	— —In the Matter of Liberty Financial Companies, Inc.—Consumer privacy
§ 34:31	— —FTC v. Rennert—Data security
§ 34:32	— —FTC v. Toysmart.com—Consumer privacy
§ 34:33	— —In the Matter of Eli Lilly and Company—Data security
§ 34:34	— —In the Matter of ReverseAuction.com, Inc.
§ 34:35	— —In the Matter of Microsoft Corporation—Data security
§ 34:36	— —In the Matter of The National Research Center for College and University Admissions, Inc.—Consumer privacy
§ 34:37	— —In the Matter of Educational Research Center of America, Inc.—Consumer privacy
§ 34:38	— —In the Matter of Guess?, Inc.—Data security
§ 34:39	— —In the Matter of MTS, Inc., d/b/a Tower Records/Books/Video—Data security

## INFORMATION SECURITY AND PRIVACY

- § 34:40 — —Bonzi Software, Inc.—Consumer privacy
- § 34:41 — —In the Matter of Gateway Learning—Consumer privacy
- § 34:42 — —In the Matter of Sunbelt Lending Services, Inc.—Data security
- § 34:43 — —In the Matter of Nationwide Mortgage Group, Inc., and John D. Eubank—Data security
- § 34:44 — —In the Matter of Petco Animal Supplies—Data security
- § 34:45 — —In the Matter of Vision I Properties, LLC—Data security
- § 34:46 — —In the Matter of BJ's Wholesale Club, Inc.—Data security
- § 34:47 — —In the Matter of Superior Mortgage Corp.—Data security
- § 34:48 — —In the Matter of CardSystems Solutions, Inc.—Data security
- § 34:49 — —In the Matter of DSW, Inc.—Data security
- § 34:50 — —In the Matter of Nations Title Agency, Inc.—Data security
- § 34:51 — —FTC. v. Integrity Security & Investigation Services, Inc. et al., (E.D. VA 2006)—Consumer privacy
- § 34:52 — —USA v. ChoicePoint Inc.—Data security
- § 34:53 — —FTC. v. Information Search, Inc. and David Kacala, (N.D. Maryland 2007)—Consumer privacy
- § 34:54 — —In the Matter of Guidance Software, Inc.—Data security
- § 34:55 — —In the Matter of American United Mortgage Company—Data security
- § 34:56 — —In the Matter of Sony BMG Music Entertainment—Consumer privacy
- § 34:57 — —United States v. ValueClick, Inc.—Data security
- § 34:58 — —In the Matter of Goal Financial, LLC—Data security
- § 34:59 — —In the Matter of Life is Good Retail, Inc.—Data security
- § 34:60 — —FTC. v. Action Research Group, Inc., et al., (M.D. Fla. 2008)—Consumer privacy
- § 34:61 — —In the Matter of Reed Elsevier Inc. and Seisint, Inc.—Data security
- § 34:62 — —In the Matter of The TJX Companies, Inc.—Data security
- § 34:63 — —In the Matter of Premier Capital Lending, Inc.—Data security
- § 34:64 — —In the Matter of Genica Corporation and Computer Geeks.com—Data security

## TABLE OF CONTENTS

§ 34:65	— —USA v. Rental Research Services, Inc. & Lee Mikkelson, (Minn. 2009)—Data security
§ 34:66	— —Federal Trade Commission v. Accusearch Inc., et al, (10th Cir. 2009)—Consumer privacy
§ 34:67	— —In the Matter of CVS Caremark Corporation—Data security
§ 34:68	— —In the Matter of James B. Nutter & Company—Data security
§ 34:69	— —In the Matter of Sears Holdings Management Corporation—Consumer privacy
§ 34:70	— —In the Matter of Collectify LLC—Consumer privacy
§ 34:71	— —In the Matter of ExpatEdge Partners, LLC—Consumer privacy
§ 34:72	— —In the Matter of Directors Desk LLC (2010)—Consumer privacy
§ 34:73	— —In the Matter of Onyx Graphics—Consumer privacy
§ 34:74	— —FTC. v. Gregory Navone, (Nev. 2008)—Data security
§ 34:75	— —In the Matter of Progressive Gaitways, Inc., (F.T.C. Nov. 9, 2009)—Consumer privacy
§ 34:76	— —In the Matter of World Innovators—Consumer privacy
§ 34:77	— —Federal Trade Commission v. ControlScan, Inc., (N.D. Ga. 2009)—Consumer privacy
§ 34:78	— —USA v. Direct Marketing Associates, Corp.
§ 34:79	— —In the Matter of Dave & Busters, Inc., (May 20, 2010)—Data security
§ 34:80	— —In the Matter of Twitter—Data security
§ 34:81	— —FTC v. EchoMetrix, Inc. (E.D. N.Y. 2010)—Consumer privacy
§ 34:82	— —In the Matter of Rite Aid Corporation (F.T.C. Nov. 12, 2010)—Data security
§ 34:83	— —FTC v. Lifelock, Inc., et al.—Data security
§ 34:84	— —In the Matter of ACRAnet, Inc., (F.T.C. 2010)—Data security
§ 34:85	— —In the Matter of Fajilan and Associates, Inc. also d/b/a Statewide Credit Services, and Robert Fajilan (F.T.C. 2011)—Data security
§ 34:86	— —In the Matter of SettlementOne Credit Corporation & Sackett National Holdings, Inc. (F.T.C. 2011)
§ 34:87	— —In the Matter of U.S. Search—Consumer privacy
§ 34:88	— —In the Matter of Google Inc. (F.T.C. 2011)—Consumer privacy

## INFORMATION SECURITY AND PRIVACY

- § 34:89 — —In the Matter of Ceridian Corporation (F.T.C. 2011)—Data security
- § 34:90 — —In the Matter of Chitika, Inc. (F.T.C. 2011)—Consumer privacy
- § 34:91 — —In the Matter of Lookout Services, Inc. (F.T.C. July 15, 2011)—Data security
- § 34:92 — —FTC v. RockYou, Inc.—Data security
- § 34:93 — —In the Matter of Legacy Learning Systems, Inc. and Smith
- § 34:94 — —In the Matter of Facebook Inc.—Consumer privacy
- § 34:95 — —In The Matter of MySpace LLC—Consumer privacy
- § 34:96 — —In the Matter of ScanScout, Inc.—Consumer privacy
- § 34:97 — —In the Matter of Upromise, Inc.—Data security
- § 34:98 — —United States of America v. Teletrack, Inc.
- § 34:99 — —USA v. Asset Acceptance, LLC
- § 34:100 — —USA v. Spokeo, Inc.
- § 34:101 — —In the Matter of Franklin’s Budget Car Sales, Inc.—Data security
- § 34:102 — —In the Matter of EPN, Inc.—Data security
- § 34:103 — —HireRight Solutions, Inc.
- § 34:104 — —In the Matter of DesignerWare, LLC; Timothy Kelly, and Ronald P. Koller, individually and as officers of DesignerWare, LLC; Aspen Way Enterprises, Inc.; Watershed Development Corp.; Showplace, Inc., d/b/a Showplace Rent-to-Own; J.A.G. Rents, LLC, d/b/a ColorTyme; Red Zone, Inc., d/b/a ColorTyme; B. Stamper Enterprises, Inc., d/b/a Premier Rental Purchase; and C.A.L.M. Ventures, Inc., d/b/a Premier Rental Purchase—Consumer privacy
- § 34:105 — —In the Matter of Compete, Inc.—Data security
- § 34:106 — —In the matter of Epic Marketplace, Inc.—Consumer privacy
- § 34:107 — —In the Matter of CBR Systems, Inc.—Data security
- § 34:108 — —In the Matter of HTC America, Inc.—Data security
- § 34:109 — —In the Matter of PLS Financial Services, Inc., and The Payday Loan Store of Illinois, Inc. (N.D. Ill. 2012)—Data security
- § 34:110 — —In the Matter of Certegy Check Services, Inc. (D.D.C. 2013)
- § 34:111 — —Challenges to jurisdiction—In re the Matter of

## TABLE OF CONTENTS

	LabMD and In the Matter of Wyndham—Data security
§ 34:112	— —In the Matter of TRENDnet, Inc.—Data security
§ 34:113	— —In the Matter of Aaron’s, Inc.—Consumer privacy
§ 34:114	— —In the Matter of Goldenshores Technologies, LLC.—Consumer privacy
§ 34:115	— —In the Matter of Accretive Health, Inc.—Data security
§ 34:116	— —In the Matter of GeneLink Inc., and foru International Corporation—Data security
§ 34:117	— —In the Matter of TeleCheck Services, Inc.
§ 34:118	— —In the Matter of The Receivable Management Services Corporation; Charles River Laboratories International, Inc.; DataMotion, Inc.; DDC Laboratories, Inc., d/b/a DNA Diagnostics Center; Fantage; Level 3 Communications, LLC; Reynolds Consumer Products, Inc.; Apperian, Inc.; Baker Tilly Virchow Krause, LLP; BitTorrent, Inc.; Atlanta Falcons Football Club, LLC; PDB Sports, Ltd., d/b/a Denver Broncos Football Club; and Tennessee Football, Inc.—Safe Harbor
§ 34:119	— —In the Matter of GMR Transcription Services, Inc., (50th case in data security)—Data security
§ 34:120	— —In the Matter of Fantage.com, Inc.—Safe Harbor
§ 34:121	— —In the Matter of American Apparel, Inc.—Safe Harbor
§ 34:122	— —In the Matter of Credit Karma, Inc.—Data security
§ 34:123	— —In the Matter of Fandango, LLC—Data security
§ 34:124	— —In the Matter of Instant Checkmate
§ 34:125	— —In the Matter of InfoTrack
§ 34:126	— —In the Matter of Snapchat, Inc.—Consumer privacy and security
§ 34:127	— —In the Matter of TRUSTe, Inc.—Consumer privacy
§ 34:128	— —In re the Matter of Sitesearch Corporation, doing business as LeapLab
§ 34:129	— —In the Matter of Craig Brittain—Consumer Privacy
§ 34:130	— —In the matter of Jerk, LLC and John Fanning—Consumer Privacy
§ 34:131	— —In the Matter of TES Franchising, LLC—Consumer Privacy/Safe Harbor
§ 34:132	— —In the Matter of American International Mailing, Inc.—Consumer Privacy/Safe Harbor

## INFORMATION SECURITY AND PRIVACY

- § 34:133 — —In the Matter of Nomi Technologies, Inc.—  
Consumer Privacy
- § 34:134 — —In re the Matter of Golf Connect, LLC, Pinger,  
Inc., NAICS Association, LLC, Jubilant Clinsys,  
Inc., IOActive, Inc., Contract Logix, LLC, Forensics  
Consulting Solutions, LLC, Dale Jarrett Racing  
Adventure, SteriMed Medical Waste Solutions,  
California Skate-Line, Just Bagels Mfg., Inc., One  
Industries Corp., and Inbox Group, LLC.—  
Consumer Privacy/Safe Harbor
- § 34:135 — —F.T.C. v. Wyndham—Data security
- § 34:136 — —In the Matter of Ruby Corp./Ashley Madison—  
Data security
- § 34:137 — —In the Matter of Decusoft, Tru Communication,  
Inc., and Md7, LLC—Privacy Shield
- § 34:138 — —In the Matter of Lenovo—Consumer privacy
- § 34:139 — —In the Matter of TaxSlayer, LLC—Consumer  
privacy
- § 34:140 — —In the Matter of Uber—Data security
- § 34:141 — —In the Matter of Turn, Inc.—Consumer privacy
- § 34:142 — —In the Matter of Vizio—Consumer privacy
- § 34:143 — —In the Matter of Practice Fusion, Inc.
- § 34:144 — —In the Matter of Very Incognito Technologies—  
APEC Cross Border Privacy Rule
- § 34:145 — —In the Matter of ASUSTeK Computer, Inc.
- § 34:146 — —In the Matter of InMobi—Consumer privacy  
and COPPA
- § 34:147 — —In the Matter of Henry Schein
- § 34:148 — —In the Matter of Oracle Corporation
- § 34:149 FTC guidelines on protecting personal information
- § 34:150 —Take stock
- § 34:151 —Scale down
- § 34:152 —Lock it
- § 34:153 —Pitch it
- § 34:154 —Plan ahead
- § 34:155 The FTC and the U.S. SAFE Web Act of 2006
- § 34:156 FTC advertising guidelines—The FTC’s dot com  
disclosures
- § 34:157 —Online behavioral advertising guidance
- § 34:158 — —Principle 1—Transparency and consumer  
control
- § 34:159 — —Principle 2—Reasonable security, and limited  
data retention, for consumer data
- § 34:160 — —Principle 3—Affirmative express consent for  
material changes to existing privacy promises
- § 34:161 — —Principle 4—Affirmative express consent to (or

## TABLE OF CONTENTS

	prohibition against) using sensitive data for behavioral advertising
§ 34:162	— —Principle 5—Using tracking data for purposes other than behavioral advertising a call for additional information
§ 34:163	—FTC social media guidance—Background
§ 34:164	— —Treatment of endorsements and testimonials
§ 34:165	— —General considerations
§ 34:166	— —Consumer endorsements
§ 34:167	— —Expert endorsements
§ 34:168	— —Endorsements by organizations
§ 34:169	— —Disclosure of material conditions
§ 34:170	—FTC regulations regarding “free” offers
§ 34:171	FTC Copier Guidance
§ 34:172	FTC security guidance—“Start with Security: A Guide for Business”

## CHAPTER 35. PRIVACY LITIGATION

§ 35:1	Introduction
§ 35:2	Theories of liability
§ 35:3	Conversion of information by deletion
§ 35:4	The Restatement (Second) of Torts view of privacy liability
§ 35:5	Invasion of privacy liability and peer-to-peer networks
§ 35:6	Federal Trade Commission Act as basis for privacy litigation
§ 35:7	Federal Trade Commission Act—Actions
§ 35:8	—Recent FTC consent orders
§ 35:9	Electronic Communications Privacy Act and Computer Fraud and Abuse Act
§ 35:10	Sony data breach
§ 35:11	Security litigation against BJ’s Wholesale Club, Inc. and TJX
§ 35:12	Litigation against third-party consultants
§ 35:13	California—unfair competition law
§ 35:14	—CLRA and UCL dismissed on reliance and no economic injury
§ 35:15	—Pretexting and common law liability in California
§ 35:16	—The media and subterfuge
§ 35:17	—Litigation under California’s constitutional right of privacy
§ 35:18	—Failure to timely notify of data breach—The People of the State of California v. Kaiser Foundation HealthPlan, Inc.

## INFORMATION SECURITY AND PRIVACY

- § 35:19 —Standing under Shine the Light
- § 35:20 New York law
- § 35:21 —Attorney General actions
- § 35:22 —Article 63
- § 35:23 The damage conundrum
- § 35:24 Public access to websites is insufficient to establish a claim
- § 35:25 Litigation resulting from public disclosure of information on the Internet
- § 35:26 Actual misuse of data required to show damage
- § 35:27 Requirement of actual damages under the Privacy Act
- § 35:28 Standing in privacy litigation
- § 35:29 —No Article III standing where Social Security number mailed
- § 35:30 —Article III and loyalty points
- § 35:31 —Alternative standing theories
- § 35:32 California Medical Information Act (CMIA) litigation
- § 35:33 CMIA litigation—Sutter Health
- § 35:34 —Potential for access cases applying Sutter Health
- § 35:35 Encryption and loss of passwords
- § 35:36 Data security litigation
- § 35:37 Enforceability of arbitration clauses in agreements
- § 35:38 Litigation over PCI and limitations on liability
- § 35:39 Aiding and abetting fraud through banks failure to have adequate security systems
- § 35:40 HIPAA and Illinois law does not create a duty to protect that is actionable
- § 35:41 Privacy policy as a contract
- § 35:42 Franchise liability
- § 35:43 Privacy in the context of litigation
- § 35:44 —Production of electronic information
- § 35:45 Redaction in bankruptcy filings
- § 35:46 —Exemptions
- § 35:47 —Filings made under seal
- § 35:48 —Protective orders
- § 35:49 —Option for filing a reference list
- § 35:50 —Waiver of protection of identifiers
- § 35:51 —Utility account numbers are financial account numbers
- § 35:52 Privacy protection for filings made with federal courts
- § 35:53 —Exemptions from the redaction requirement
- § 35:54 —Limitations on remote access to electronic files
- § 35:55 —Filings made under seal or with redactions



## TABLE OF CONTENTS

§ 35:56	—Protective orders
§ 35:57	—Waiver of protection of identifies
§ 35:58	—Public access to papers
§ 35:59	Privacy in the context of litigation—Production of electronic media and trade secrets
§ 35:60	—Requiring the creation of data
§ 35:61	—Electronic discovery and costs
§ 35:62	—Foreign privacy laws/discovery
§ 35:63	Privacy and search engine data
§ 35:64	Facebook terms of service
§ 35:65	BJ's security breach litigation
§ 35:66	Electronic conversion of data
§ 35:67	Application of litigation privilege to privacy claims
§ 35:68	Litigation under the DPPA and § 1983
§ 35:69	Recent DPPA litigation issues
§ 35:70	FACTA litigation and class certification
§ 35:71	Accessibility of information may not destroy a privacy right
§ 35:72	FCRA litigation
§ 35:73	Litigation resulting from public disclosure of information on the Internet
§ 35:74	In the Matter of Pulsepoint, Inc. (2013)
§ 35:75	In the Matter of DealerApp Vantage, LLC—Enforcement by the State of New Jersey
§ 35:76	Class actions—Issues in privacy litigation
§ 35:77	—General issues with privacy class actions
§ 35:78	—Class actions in federal court—The requirements of Rule 23
§ 35:79	— —Rule 23(b)—A general overview
§ 35:80	— — —Examination of 23(b)(1)
§ 35:81	— — —Examination of 23(b)(2)
§ 35:82	— — —Examination of 23(b)(3)
§ 35:83	— — —Notice under Rule 23(b)(3)
§ 35:84	— — —Potential defenses based upon individual reliance
§ 35:85	— — —Examples of cases involving privacy concerns
§ 35:86	—California class action issues
§ 35:87	— —Ascertainable class
§ 35:88	— —Community of interest
§ 35:89	— —Predominant questions of law or fact
§ 35:90	— —Typicality
§ 35:91	— —Adequate representation
§ 35:92	— —Additional showing—Substantial benefit to the court and litigants
§ 35:93	— —No consideration of the merits

- § 35:94 — —Application to privacy litigation
- § 35:95 — —TCPA claims and class certification
- § 35:96 — —Pleading
- § 35:97 — —Discovery
- § 35:98 — —Discovery regarding Penal Code—Section 632 cases
- § 35:99 Privacy litigation under the Lanham Act
- § 35:100 Enforceability of forum selection clauses in emails
- § 35:101 Coverage for computer related incidents
- § 35:102 Joinder of Doe defendants

## CHAPTER 36. JURISDICTION AND THE DORMANT COMMERCE CLAUSE

- § 36:1 Generally
- § 36:2 General versus specific jurisdiction
- § 36:3 Specific jurisdiction
- § 36:4 Purposeful availment
- § 36:5 Forum-related activities
- § 36:6 Reasonableness
- § 36:7 Jurisdiction and emails
- § 36:8 Use of a company's website as establishing jurisdiction
- § 36:9 Posting on a blog establishes jurisdiction
- § 36:10 Personal jurisdiction over individuals
- § 36:11 Ebay jurisdiction
- § 36:12 Service by email
- § 36:13 Swarm joinder
- § 36:14 The dormant Commerce Clause

## CHAPTER 37. ANONYMOUS POSTING AND SUBPOENAS

- § 37:1 Privacy in the context of litigation—Subpoenas
- § 37:2 — —First Amendment issues
- § 37:3 — —Anonymous posting and subpoenas
- § 37:4 — — —2Themart.com
- § 37:5 — — —The Solers and Cablevision tests
- § 37:6 — — —The Dendrite and Cahill standard
- § 37:7 — — —The Northern District of California
- § 37:8 — — —The Illinois standard
- § 37:9 — —Standing regarding subpoenas
- § 37:10 — —Terms of service and privacy policy establishing notice
- § 37:11 — —Wisconsin's application of the Cahill test

## TABLE OF CONTENTS

§ 37:12	— — Anonymous posting and subpoenas—The Mobilisa standard
§ 37:13	— — — The Krinsky standard
§ 37:14	— — — A new standard—The Doe I standard
§ 37:15	— — — The Sony standard
§ 37:16	— — — California’s anti-slapp law
§ 37:17	New York law—Preaction discovery in New York
§ 37:18	Privacy in the context of litigation—Subpoenas—Anonymous posting and subpoenas—Virginia law
§ 37:19	Personal jurisdiction versus subpoena jurisdiction
§ 37:20	Privacy in the context of litigation—Subpoenas—Anonymous posting and subpoenas—Federal court
§ 37:21	— — — Standing
§ 37:22	— — Section 1985.3 of the California Code of Civil Procedure
§ 37:23	— — Blogging
§ 37:24	— — Library records
§ 37:25	— Other subpoenas—First Amendment issues—Admission of reading materials as evidence of intent
§ 37:26	— Employee blogging
§ 37:27	First Amendment concerns and public employee blogging
§ 37:28	Privacy in the context of litigation—Subpoenas—Steps to deal with a subpoena

## CHAPTER 38. PRIVACY 3.0—THE PRINCIPLE OF PROPORTIONALITY

§ 38:1	Introduction
§ 38:2	Privacy 1.0—A historical background
§ 38:3	Privacy 2.0—A historical background
§ 38:4	The weaknesses of common law theories
§ 38:5	The fall of tort theory
§ 38:6	The rise of the FTC—Current enforcement theories and their reliance upon proportionality
§ 38:7	The importance of principle based analysis
§ 38:8	English common law is not the answer
§ 38:9	The United States adoption of EU-like principles
§ 38:10	A current assessment of societal views in the United States on information sharing and management
§ 38:11	Privacy 3.0
§ 38:12	— Tier I—Highly sensitive information
§ 38:13	— Tier II—Sensitive information
§ 38:14	— Tier III—Slightly sensitive information
§ 38:15	— Tier IV—Nonsensitive information
§ 38:16	— Laws that validate the principle of proportionality

- § 38:17 — —CFAA
- § 38:18 — —California’s Invasion of Privacy Act
- § 38:19 — —The Combined DNA Index System (CODIS)
- § 38:20 — —Other restrictions on genetic privacy
- § 38:21 — —Notice of security breach laws
- § 38:22 — —The Videotape Privacy Protection Act
- § 38:23 — —Federal Cable Privacy Act
- § 38:24 — —Credit freeze laws
- § 38:25 — —Identity theft
- § 38:26 — —Restrictions on Social Security numbers
- § 38:27 — —Pretexting
- § 38:28 — —CAN-SPAM
- § 38:29 —Legislatures do not always assess the risks  
correctly
- § 38:30 Conclusion

## **CHAPTER 39. PRIVACY ISSUES FOR PUBLIC UTILITY COMPANIES**

### **I. INTRODUCTION**

- § 39:1 General
- § 39:2 Red Flags
- § 39:3 State regulations—An introduction
- § 39:4 Smart Grid
- § 39:5 Security concerns
- § 39:6 Utilities as an ISP

### **II. SPECIFIC STATE LAWS**

#### **A. CALIFORNIA**

- § 39:7 Disclosures by utilities—In general
- § 39:8 —California utility privacy law regarding usage data
- § 39:9 —Civil enforcement
- § 39:10 —Re Proposed Policies Governing Restructuring  
California’s Electric Services Industry and  
Reforming Regulation Decision 97-10-031
- § 39:11 —Access to computer models and rate setting

#### **B. ILLINOIS**

- § 39:12 Customer records and information
- § 39:13 Disclosure of customer information to law-  
enforcement agencies
- § 39:14 Customer information

## TABLE OF CONTENTS

### C. MINNESOTA

- § 39:15 Municipal utility customer data
- § 39:16 Billing

### D. WISCONSIN

- § 39:17 Information available to customers

## CHAPTER 40. A REFERENCE FOR YOUR COMPANY

- § 40:1 Introduction
- § 40:2 General issues for companies—Marketing concerns
- § 40:3 Two party consent
- § 40:4 Defining the proper scope of investigations
- § 40:5 E-mail footers
- § 40:6 Defining “personally identifiable information”
- § 40:7 Information security requirements
- § 40:8 Insurance, indemnity, and other risk shifting mechanisms
- § 40:9 Computer crime laws—Confidential information concerns
- § 40:10 Anonymous subpoenas
- § 40:11 Blogging and social networking
- § 40:12 Security breaches
- § 40:13 Security freeze laws
- § 40:14 Red flag regulations under FACT Act
- § 40:15 Electronic health records
- § 40:16 Social Security numbers
- § 40:17 Credit card receipt issues
- § 40:18 Spyware, phishing, and pharming
- § 40:19 Cloud computing
- § 40:20 Transfers in M&A, bankruptcy, and retroactive changes to privacy policies
- § 40:21 Internet concerns
- § 40:22 Public display of information
- § 40:23 Behavioral advertising
- § 40:24 Genetic privacy
- § 40:25 Payment card industry standards
- § 40:26 Biometrics
- § 40:27 RFID/GPS
- § 40:28 International issues
- § 40:29 SOX
- § 40:30 Responding to government requests
- § 40:31 Application of consumer reporting agency laws

- § 40:32 Employment applications
- § 40:33 Industry specific concerns—Energy companies
- § 40:34 —Financial institutions
- § 40:35 —Hospitals and medical providers
- § 40:36 —Government employers
- § 40:37 —Social networking sites
- § 40:38 —The airline industry
- § 40:39 —Retail issues
- § 40:40 —Telecom
- § 40:41 —Insurance companies
- § 40:42 —Publishers
- § 40:43 —Cable and video companies
- § 40:44 Understanding and managing cyber risk—  
Introduction
- § 40:45 —COSO 2017 Framework
- § 40:46 —NIST
- § 40:47 —SANS Top 20
- § 40:48 —Understanding cyber risk and risk tolerance
- § 40:49 —Understanding cyber
- § 40:50 —The costs of cyber
- § 40:51 —What are the ramifications of cyber incidents?
- § 40:52 —Risk assessments, assessing risk, and risk  
tolerance
- § 40:53 —Assessing risk/understanding enterprise cyber risk
- § 40:54 —What is your cyber risk tolerance?
- § 40:55 —Determining risk tolerance:
- § 40:56 —What are the relevant legal obligations for the  
Board?
- § 40:57 —Where should cyber sit at the Board?
- § 40:58 —What key questions should the Board be asking?
- § 40:59 —What key questions should management be asking?
- § 40:60 —What key questions should the General Counsel be  
asking?
- § 40:61 —Key incident response questions to consider
- § 40:62 —What should the Board do?
- § 40:63 —What should management do?

## **CHAPTER 41. APPLICATION OF NON- PRIVACY AND SECURITY-BASED LAWS TO CYBERSECURITY, PRIVACY, AND OTHER DATA ISSUES—SEC AND DELAWARE OBLIGATIONS**

### **I. OVERVIEW**

- § 41:1 Introduction

## TABLE OF CONTENTS

§ 41:2 An overview

## II. UNDERSTANDING SEC AND DELAWARE OBLIGATIONS

- § 41:3 Why do for-profit companies exist?
- § 41:4 SEC obligations summarized
- § 41:5 Delaware law summarized—Why does Delaware law matter?
- § 41:6 —The internal affairs doctrine
- § 41:7 —Operations versus oversight
- § 41:8 —The duty of care and the duty of loyalty
- § 41:9 Key take-aways regarding SEC and Delaware law

## III. GOVERNANCE

- § 41:10 Overview
- § 41:11 Differing governance obligations
- § 41:12 Corporate governance
- § 41:13 Nested governance
- § 41:14 The materiality fallacy—An over-emphasis on legal risk
- § 41:15 Putting technology, data, and AI risk in context
- § 41:16 Combining Delaware corporate principles and technology, data, and AI risk
- § 41:17 Examples of resiliency and legal compliance impacts
- § 41:18 Creating technology, data, and AI risk governance
- § 41:19 Redefining requests
- § 41:20 Conclusions and take-aways

## CHAPTER 42. EUROPEAN UNION ARTIFICIAL INTELLIGENCE ACT

- § 42:1 Introduction
- § 42:2 Subject matter
- § 42:3 Scope
- § 42:4 Amendments to Annex I
- § 42:5 Prohibited AI practices
- § 42:6 High-risk AI practices—Classification of AI systems as high-risk—Classification rules for high-risk AI systems
- § 42:7 —Amendments to Annex III
- § 42:8 —Requirements for high-risk AI systems—Compliance with the requirements
- § 42:9 —Risk management system
- § 42:10 —Data and data governance

## INFORMATION SECURITY AND PRIVACY

- § 42:11 — —Technical documentation
- § 42:12 — —Record-keeping
- § 42:13 — —Transparency and provision of information to users
- § 42:14 — —Human oversight
- § 42:15 — —Accuracy, robustness and cybersecurity
- § 42:16 —Obligations of providers and users of high-risk AI systems and other parties—Obligations of providers
- § 42:17 — —Quality management system
- § 42:18 — —Obligation to draw up technical documentation
- § 42:19 — —Conformity assessment
- § 42:20 — —Automatically generated logs
- § 42:21 — —Corrective actions
- § 42:22 — —Duty of information
- § 42:23 — —Cooperation with competent authorities
- § 42:24 — —Obligations of product manufacturers
- § 42:25 — —Authorised representatives
- § 42:26 — —Obligations of importers
- § 42:27 — —Obligations of distributors
- § 42:28 — —Obligations of distributors, importers, users or any other third-party
- § 42:29 — —Obligations of users of high-risk AI systems
- § 42:30 —Notifying authorities and notified bodies—Notifying authorities
- § 42:31 — —Application of a conformity assessment body for notification
- § 42:32 — —Notification procedure
- § 42:33 Requirements for high-risk AI systems—Notifying authorities and notified bodies—Notified bodies
- § 42:34 High-risk AI practices—Notifying authorities and notified bodies—Subsidiaries of and subcontracting by notified bodies
- § 42:35 — —Identification numbers and lists of notified bodies designated under this regulation
- § 42:36 — —Changes to notifications
- § 42:37 — —Challenge to the competence of notified bodies
- § 42:38 — —Coordination of notified bodies
- § 42:39 — —Conformity assessment bodies of third countries
- § 42:40 —Standards, conformity assessment, certificates, registration—Harmonised standards
- § 42:41 — —Common specifications
- § 42:42 — —Presumption of conformity with certain requirements
- § 42:43 — —Conformity assessment
- § 42:44 — —Certificates



## TABLE OF CONTENTS

§ 42:45	— —Appeal against decisions of notified bodies
§ 42:46	— —Information obligations of notified bodies
§ 42:47	— —Derogation from conformity assessment procedure
§ 42:48	— —EU declaration of conformity
§ 42:49	— —CE marking of conformity
§ 42:50	— —Document retention
§ 42:51	— —Registration
§ 42:52	Transparency obligations for certain AI systems
§ 42:53	Measures in favor of innovation—AI regulatory sandboxes
§ 42:54	—Further processing of personal data for developing certain AI systems in the public interest in the AI regulatory sandbox
§ 42:55	—Measures for small-scale providers and users
§ 42:56	Governance—European Artificial Intelligence Board—Establishment of the European Artificial Intelligence Board
§ 42:57	— —Structure of the Board
§ 42:58	— —Tasks of the Board
§ 42:59	—National competent authorities—Designation of national competent authorities
§ 42:60	EU database for stand-alone high-risk AI systems
§ 42:61	Post-market monitoring, information sharing, market surveillance—Post-market monitoring—Post-market monitoring by providers and post-market monitoring plan for high-risk AI systems
§ 42:62	— —Sharing of information on incidents and malfunctioning—Reporting of serious incidents and of malfunctioning
§ 42:63	—Enforcement—Market surveillance and control of AI systems in the Union market
§ 42:64	— —Access to data and documentation
§ 42:65	— —Procedure for dealing with AI systems presenting a risk at national level
§ 42:66	— —Union safeguard procedure
§ 42:67	— —Compliant AI systems which present a risk
§ 42:68	— —Formal non-compliance
§ 42:69	Codes of conduct
§ 42:70	Confidentiality and penalties—Confidentiality
§ 42:71	—Penalties
§ 42:72	—Administrative fines on Union institutions, agencies and bodies
§ 42:73	Delegation of power and committee procedure—Exercise of the delegation
§ 42:74	—Committee procedure

## INFORMATION SECURITY AND PRIVACY

- § 42:75 Amendments
- § 42:76 Evaluation and review
- § 42:77 Entry into force and application

### **Table of Laws and Rules**

### **Table of Cases**

### **Index**