

# Table of Contents

## PART A. DATA BREACH LITIGATION

### CHAPTER 1. STANDING

#### I. INTRODUCTION

- § 1:1 Overview of Article III standing
- § 1:2 Elements of Article III standing

#### II. EARLY DATA BREACH LITIGATION HOLDINGS ON STANDING

- § 1:3 Risk of future harm
- § 1:4 Post-*Clapper* risk of future harm
- § 1:5 Remedial and mitigation costs
- § 1:6 Delayed or inadequate notification

#### III. SPOKEO V. ROBINS

- § 1:7 Case holding

#### IV. POST-SPOKEO STANDING

- § 1:8 Data breach cases
- § 1:9 Increased risk of future harm and mitigation costs
- § 1:10 Other potential statutory claims
- § 1:11 —Violation of the Fair Credit Reporting Act
- § 1:12 —Violation of the Fair and Accurate Credit  
Transactions Act
- § 1:13 —Cases under Illinois Biometric Privacy Act where  
standing found
- § 1:14 —Cases under Illinois Biometric Information Privacy  
Act where no standing found

Appendix 1A. Federal Statutes Involving Privacy Rights

## **CHAPTER 2. REASONABLE SECURITY MEASURES**

### **I. INTRODUCTION**

- § 2:1 Reasonableness standard in cybersecurity litigation
- § 2:2 Legal framework for reasonableness
- § 2:3 —Federal statutes and regulations
- § 2:4 —State statutes and regulations
- § 2:5 —Guidance from federal agencies
- § 2:6 —Standardized controls
- § 2:7 Regulatory enforcement for failure to maintain reasonable security measures
- § 2:8 Judicial actions alleging failure to maintain reasonable security measures
- § 2:9 International actions assessing reasonable security measures
- § 2:10 Complying with the reasonable security measures standard
- § 2:11 —Designating a responsible individual
- § 2:12 —Conduct an initial and annual risk assessments
- § 2:13 —Implement appropriate controls
- § 2:14 —Exercise diligence and oversight of service providers
- § 2:15 —Train employees and prepare for incidents
- § 2:16 —Evaluate effectiveness
- § 2:17 —Include senior corporate management and/or the board of directors

## **CHAPTER 3. RETAIL DATA BREACHES**

### **I. INTRODUCTION**

- § 3:1 Retail data breaches
- § 3:2 Standing in retail data breach litigation
- § 3:3 Attorney-client privilege and work product issues
- § 3:4 Payment card industry data security standards
- § 3:5 —State statutes

### **II. COMMON LAW CLAIMS**

- § 3:6 Negligence and negligence per se
- § 3:7 —Economic loss rule
- § 3:8 —Causation
- § 3:9 —Reasonable security measures
- § 3:10 Breach of contract

## TABLE OF CONTENTS

- § 3:11 Unjust enrichment
- § 3:12 Invasion of privacy claims
- § 3:13 Payment Card Industry Data Security Standards (PCI DSS) and breach of contract claims by financial institutions
- § 3:14 —Derivative actions
- § 3:15 —Negligence
- § 3:16 Damages
- § 3:17 —Risk of future harm
- § 3:18 —Actual costs
- § 3:19 —Benefit of the bargain
- § 3:20 —Delayed or inadequate notification

### III. STATE STATUTORY CLAIMS

- § 3:21 State statutory claims in retail data breach litigation

### IV. CLASS ACTIONS

- § 3:22 Class certification issues
- § 3:23 Class action settlement issues

## CHAPTER 4. HEALTHCARE DATA BREACH LITIGATION

### I. INTRODUCTION

- § 4:1 Healthcare data breach litigation, in general
- § 4:2 Office of Civil Rights enforcement

### II. STANDING

- § 4:3 Standing
- § 4:4 —Fear of future identity theft
- § 4:5 —Benefit of the bargain theory

### III. STATE COMMON LAW CLAIMS

- § 4:6 Negligence and the duty to safeguard personally identifiable information and protected health information
- § 4:7 —Special relationship
- § 4:8 — —California
- § 4:9 — —Florida
- § 4:10 — —District of Columbia
- § 4:11 — —Illinois
- § 4:12 Negligence per se

- § 4:13 —California
- § 4:14 —Connecticut
- § 4:15 —Florida
- § 4:16 —Ohio
- § 4:17 Invasion of privacy
- § 4:18 —Publicity
- § 4:19 Breach of confidentiality
- § 4:20 Conversion
- § 4:21 Fraud
- § 4:22 —Misrepresentations in privacy policies
- § 4:23 Breach of express contracts
- § 4:24 Breach of implied contracts
- § 4:25 Breach of duty of good faith and fair dealing
- § 4:26 Unjust enrichment
- § 4:27 Common law damages
- § 4:28 —Identity theft
- § 4:29 —Emotional distress
- § 4:30 —Benefit of the bargain
- § 4:31 —Inherent value of protected health information
- § 4:32 Equitable relief under common law

#### **IV. STATE STATUTORY CLAIMS**

- § 4:33 State unfair competition laws
- § 4:34 State privacy protection acts
- § 4:35 —Georgia
- § 4:36 —New Jersey
- § 4:37 — —Disclosure Requirements
- § 4:38 —North Carolina
- § 4:39 — —Disclosure requirements
- § 4:40 —California Confidentiality of Medical Information Act
- § 4:41 — —Actual viewing of access
- § 4:42 — —Statutory damages
- § 4:43 —California Consumer Rights Act
- § 4:44 Breach notification statutes

#### **V. FEDERAL STATUTORY CLAIMS**

- § 4:45 Health Insurance Portability and Accountability Act of 1996
- § 4:46 —Violation as basis for tortious interference
- § 4:47 —Standard used in negligence claims
- § 4:48 —Pre-emption
- § 4:49 ERISA pre-emption
- § 4:50 Stored Communications Act



TABLE OF CONTENTS

**CHAPTER 5. BREACHES INVOLVING  
FINANCIAL INSTITUTIONS AND  
FINANCIAL SERVICES COMPANIES**

**I. INTRODUCTION**

- § 5:1 Financial breaches, generally
- § 5:2 Standing

**II. FEDERAL STATUTORY CLAIMS**

- § 5:3 Stored Communications Act
- § 5:4 —Scienter
- § 5:5 Fair Credit Reporting Act
- § 5:6 —Biographical data is not a consumer report
- § 5:7 Gramm Leach Bliley Act
- § 5:8 Federal securities laws

**III. STATE COMMON LAW CLAIMS**

- § 5:9 Breach of contract
- § 5:10 —Implied contracts
- § 5:11 Unjust enrichment
- § 5:12 Negligence
- § 5:13 —Duty to safeguard personal information
- § 5:14 —Causation
- § 5:15 —Independent intervening cause
- § 5:16 —Damages
- § 5:17 Negligence per se
- § 5:18 Economic loss rule
- § 5:19 Breach of confidence
- § 5:20 Bailment

**IV. STATE STATUTORY CLAIMS**

- § 5:21 Violations of state breach notification statutes
- § 5:22 Duty to disclose in consumer protection claims
- § 5:23 California Unfair Competition Law
- § 5:24 California Consumer Legal Remedies Act
- § 5:25 Unfair and Deceptive Acts and Practices in the states
- § 5:26 —Georgia
- § 5:27 —Florida
- § 5:28 —New York
- § 5:29 —Texas
- § 5:30 —Washington
- § 5:31 —Extraterritoriality

§ 5:32 Cryptocurrency breaches

## **CHAPTER 6. ERISA BREACHES**

- § 6:1 Introduction
- § 6:2 Overview of ERISA
- § 6:3 Definition of ERISA fiduciary
- § 6:4 ERISA fiduciary duties and responsibilities
- § 6:5 ERISA fiduciary retirement plan cybersecurity responsibilities
- § 6:6 Fiduciary duty to protect and manage participant data
- § 6:7 Participant data as plan asset
- § 6:8 Participant data not a plan asset
- § 6:9 Fiduciary duty to manage third party service providers
- § 6:10 ERISA fiduciary breach claims
- § 6:11 —Third-party plan administrator and custodian liability
- § 6:12 —Plan sponsor liability
- § 6:13 —Record keeper liability
- § 6:14 ERISA denial of benefits claims
- § 6:15 State law claims of fraud and deceptive practices against third-party record-keeper and ERISA preemption
- § 6:16 Legislative guidance on retirement plan cybersecurity
- § 6:17 Regulatory guidance on retirement plan cybersecurity
- § 6:18 Retirement plan cybersecurity regulatory investigations
- § 6:19 Regulatory initiatives regarding retirement plan cybersecurity

## **CHAPTER 7. TERRORISTIC BREACHES**

### **I. INTRODUCTION**

- § 7:1 Terroristic breaches, in general

### **II. PLEADING ISSUES**

- § 7:2 Introduction
- § 7:3 Identifying the perpetrator
- § 7:4 —John Doe complaints
- § 7:5 Foreign Sovereign Immunities Act jurisdictional challenges
- § 7:6 Personal jurisdiction

### **III. FEDERAL CLAIMS**

- § 7:7 Computer Fraud and Abuse Act

## TABLE OF CONTENTS

- § 7:8 —Exceeds authorization
- § 7:9 —Vicarious liability
- § 7:10 Anti-cybersquatting Consumer Protection Act
- § 7:11 —Vicarious liability

## IV. STATE CLAIMS

- § 7:12 Defamation
- § 7:13 —Vicarious liability
- § 7:14 Tortious interference
- § 7:15 —Vicarious liability
- § 7:16 Civil conspiracy
- § 7:17 Zoombombing

## V. THIRD PARTY LAWSUITS

- § 7:18 Data breach litigation
- § 7:19 —Standing
- Appendix 7A. State Cyber Harassment, Cyberstalking, and Cyberbullying Laws

# CHAPTER 8. BREACHES OF EMAIL AND NON-SENSITIVE PERSONAL INFORMATION

## I. INTRODUCTION

- § 8:1 Data breaches involving non-sensitive personal information, in general
- § 8:2 Evolving recognition of emails and passwords as sensitive
- § 8:3 Standing in data breach cases
- § 8:4 —Fear of identity theft
- § 8:5 —Loss of time as actual harm
- § 8:6 —Loss of value of personal data
- § 8:7 —Delay in reporting as actual harm
- § 8:8 —Benefit of the bargain
- § 8:9 —Is the fear of identity theft fairly traceable to breach?

## II. STATE COMMON LAW CLAIMS

- § 8:10 Negligence and the duty to safeguard data
- § 8:11 —Negligence per se in Georgia
- § 8:12 Causation where there have been multiple breaches
- § 8:13 Negligence and the economic loss doctrine
- § 8:14 —Special relationship between users and online service providers

- § 8:15 Deceit by concealment in California
- § 8:16 —Reliance where plaintiffs fail to discontinue use of a service
- § 8:17 —Damages
- § 8:18 Unjust enrichment
- § 8:19 —Existence of express contract
- § 8:20 Breach of contract and limitation of liability provisions
- § 8:21 Punitive damages

### **III. STATE CONSUMER PROTECTION CLAIMS**

- § 8:22 State consumer fraud and unfair or deceptive trade practices acts
- § 8:23 California Unfair Competition Law
- § 8:24 —Misrepresentations concerning data security
- § 8:25 —Fraudulent omissions relating to data security
- § 8:26 —Restitution damages
- § 8:27 California False Advertising Law
- § 8:28 California Legal Remedies Act
- § 8:29 —Continued use after learning of breach
- § 8:30 —Software as good or service
- § 8:31 Florida Deceptive and Unfair Trade Practices Act
- § 8:32 Maryland Consumer Protection Act Claims
- § 8:33 Michigan Consumer Protection Act
- § 8:34 —Reliance
- § 8:35 Missouri Merchandising Practices Act
- § 8:36 New Hampshire Consumer Protection Act
- § 8:37 New York General Business Law
- § 8:38 New York Deceptive Practices Act
- § 8:39 Texas Deceptive Trade Practices Act

### **IV. STATE DATA BREACH NOTIFICATION LAWS**

- § 8:40 State data breach notification laws, in general
- § 8:41 California breach notification statute requires actual damages arising from the delay in reporting
- § 8:42 Punitive damages under the California breach notification statute
- § 8:43 Maryland Personal Information Privacy Act Claims

## **CHAPTER 9. CALIFORNIA CONSUMER PRIVACY ACT**

### **I. INTRODUCTION TO THE CALIFORNIA CONSUMER PRIVACY ACT**

- § 9:1 California Consumer Privacy Act, in general

## TABLE OF CONTENTS

- § 9:2 The legislative history of the California Consumer Privacy Act

## **II. OVERVIEW OF THE CALIFORNIA CONSUMER PRIVACY ACT'S PROVISIONS**

- § 9:3 Threshold for applicability
- § 9:4 Definition of personal information
- § 9:5 Consumer rights and business obligations under the California Consumer Privacy Act
- § 9:6 Attorney General enforcement
- § 9:7 Private right of action

## **III. CAUSES OF ACTION**

- § 9:8 Data breach litigation
- § 9:9 Litigation alleging unauthorized sharing
- § 9:10 Hybrid claims involving California's Unfair Competition Law
- § 9:11 No retroactive application
- § 9:12 Personal jurisdiction and venue
- § 9:13 Standing
- § 9:14 Curing the violation
- § 9:15 Reasonableness of security measures
- § 9:16 Enforceability of arbitration clauses

## **VI. FUTURE ISSUES**

- § 9:17 The California Privacy Rights Act

## **CHAPTER 10. HACKABILITY CLAIMS**

### **I. INTRODUCTION**

- § 10:1 Overview of hackability claims

### **II. CAUSES OF ACTION**

- § 10:2 Tort claims
- § 10:3 Contract and quasi-contractual claims
- § 10:4 State consumer protection claims

### **III. DEFENSES**

- § 10:5 Article III standing defenses
- § 10:6 Diminution in value and overpayment
- § 10:7 The risk of future hacking

§ 10:8 Benefit of the bargain

## **CHAPTER 11. EMPLOYEE BREACHES**

### **I. INTRODUCTION**

§ 11:1 Employee theft of company proprietary, confidential or trade secret information

### **II. DEFENSE OF TRADE SECRETS ACT**

- § 11:2 Defense of Trade Secrets Act, in general
- § 11:3 Interstate commerce requirement and effective date
- § 11:4 Inevitable disclosure doctrine
- § 11:5 Identifying the proper plaintiff in pleading
- § 11:6 Definition of trade secret
- § 11:7 “Reasonable Measures to Keep Such Information Secret”
- § 11:8 Misappropriation of the trade secret
- § 11:9 Unlawful acquisition as a form of misappropriation
- § 11:10 Unlawful use or disclosure
- § 11:11 —Improper means to acquire knowledge
- § 11:12 —Acquired from, or derived through, a person under a duty to maintain secrecy
- § 11:13 Defenses
- § 11:14 —Insufficient particularity
- § 11:15 —Plaintiff did not employ reasonable measures
- § 11:16 Remedies

### **III. THE COMPUTER FRAUD AND ABUSE ACT**

- § 11:17 Computer Fraud and Abuse Act, in general
- § 11:18 Definition of “loss” under the CFAA
- § 11:19 Statute of limitations
- § 11:20 Types of claims
- § 11:21 Actual access
- § 11:22 “Without authorization”
- § 11:23 Meaning of “exceeds authorized access”
- § 11:24 Mens rea
- § 11:25 Conspiracy liability for third-parties including subsequent employers
- § 11:26 Damages

TABLE OF CONTENTS

## **CHAPTER 12. SECURITIES & DERIVATIVE LITIGATION**

### **I. INTRODUCTION**

- § 12:1 Data breach securities and derivative litigation
- § 12:2 SEC guidance on disclosing data breaches

### **II. SECURITIES LITIGATION**

- § 12:3 Federal jurisdiction over securities cases
- § 12:4 Class certification
- § 12:5 Heightened pleading standards
- § 12:6 Identifying false statements
- § 12:7 Forward looking statements
- § 12:8 Examples of knowingly false statements
- § 12:9 Pleading scienter
- § 12:10 Loss causation

### **III. DERIVATIVE LITIGATION**

- § 12:11 Board's duties as to cybersecurity
- § 12:12 Jurisdiction over derivative litigation
- § 12:13 Delaware pleading standard
- § 12:14 Stating a claim for demand futility

## **CHAPTER 13. CYBERINSURANCE**

### **I. COVERAGE FOR DATA BREACHES UNDER TRADITIONAL INSURANCE POLICIES**

- § 13:1 Coverage for cybersecurity events under commercial general liability policies
- § 13:2 —Property damage provision
- § 13:3 — —Whether the loss constitutes property
- § 13:4 — —Coverage limited to insured's loss
- § 13:5 —Personal and advertising liability provisions
- § 13:6 —“Publications” under personal and advertising liability provisions
- § 13:7 —Third-party actions
- § 13:8 Coverage for cybersecurity events under director and officer policies
- § 13:9 Coverage for cybersecurity events under crime and fidelity policies
- § 13:10 —More than general fraud
- § 13:11 —Directness

## **II. COVERAGE FOR DATA BREACHES UNDER DEDICATED CYBER POLICIES**

- § 13:12 Coverage for cybersecurity events under dedicated cyber policies and exclusions

## **PART B. DATA PRIVACY LITIGATION**

### **CHAPTER 14. VIDEO PRIVACY LITIGATION**

#### **I. VIDEO PRIVACY**

- § 14:1 Video privacy, in general

#### **II. FEDERAL CLAIMS UNDER THE VIDEO PRIVACY PROTECTION ACT OF 1988**

- § 14:2 Introduction  
§ 14:3 Legislative history  
§ 14:4 Pleading requirements  
§ 14:5 No private right of action for failure to destroy consumer information  
§ 14:6 Who is a videotape service provider?  
§ 14:7 Who is a “consumer” under the VPPA?  
§ 14:8 What is “personally identifiable information”?  
§ 14:9 What is a “knowing” disclosure?  
§ 14:10 Is the disclosure within or outside the “ordinary course of business”?  
§ 14:11 The consent exception to nondisclosure  
§ 14:12 Disclosure in civil proceedings based upon “compelling need”  
§ 14:13 Standing  
§ 14:14 Statute of limitations  
§ 14:15 Proper defendants  
§ 14:16 Civil remedies

#### **III. STATE VIDEO RENTAL PRIVACY STATUTES**

- § 14:17 Introduction  
§ 14:18 Michigan  
§ 14:19 —Application to magazine publishers  
§ 14:20 —Limitation on civil damages  
§ 14:21 Rhode Island



TABLE OF CONTENTS

§ 14:22 Satellite and cable providers

**CHAPTER 15. DRIVER’S PRIVACY  
PROTECTION ACT LITIGATION**

- § 15:1 Drivers Privacy Protection Act, in general
- § 15:2 Statutory history of the DPPA
- § 15:3 Permissible use
- § 15:4 —Enumerated exceptions
- § 15:5 —Resale or redisclosure
- § 15:6 —Duty of reasonable care for resellers and redisclosure
- § 15:7 —Mixed use cases
- § 15:8 —Not affirmative defense
- § 15:9 Improper uses: Legal solicitation, tagging and marketing
- § 15:10 Qualified immunity
- § 15:11 Constitutional challenges for “anti-commandeering”
- § 15:12 Constitutional challenges under the Tenth Amendment and Eleventh Amendment
- § 15:13 Civil cause of action
- § 15:14 Standing
- § 15:15 Remedies

**CHAPTER 16. BIOMETRICS PRIVACY  
LITIGATION**

**I. INTRODUCTION**

- § 16:1 Biometrics, in general

**II. ILLINOIS BIOMETRIC INFORMATION PRIVACY  
ACT**

- § 16:2 Illinois Biometric Information Privacy Act, in general
- § 16:3 “Biometric Identifier”
- § 16:4 —Health care exception
- § 16:5 —Photographs
- § 16:6 —Scans
- § 16:7 — —Facebook, Google, and TikTok settlements
- § 16:8 —Anonymity
- § 16:9 Requirements
- § 16:10 —Retention and destruction under Section 15(a)
- § 16:11 —Informed consent prior to collection under Section 15(b)
- § 16:12 —Restriction on trade under Section 15(c)

- § 16:13 —Informed consent and release to disclosure under  
Section 15(d)
- § 16:14 —Protection of data under Section 15(e)
- § 16:15 —Profiting from biometric information
- § 16:16 Private right of action
- § 16:17 Claim accrual
- § 16:18 Defenses
- § 16:19 —Statute of limitations
- § 16:20 —Standing
- § 16:21 — —Illinois
- § 16:22 — —Article III
- § 16:23 —Extra-territoriality
- § 16:24 —Preemption
- § 16:25 —First Amendment and publicly available  
information
- § 16:26 Third-party biometric technology vendors

### **III. BIOMETRICS LAWS IN OTHER STATES**

- § 16:27 Generally
- § 16:28 Biometrics laws in Texas
- § 16:29 Biometrics laws in Washington: Biometric provisions  
of the Privacy Act
- § 16:30 Biometrics laws in Washington: My Health My Data  
Act
- § 16:31 Biometrics laws in Baltimore, Maryland
- § 16:32 Biometrics laws in New York City
- § 16:33 Biometrics laws in Portland, Oregon

## **CHAPTER 17. ONLINE TRACKING LITIGATION**

### **I. INTRODUCTION**

- § 17:1 Online tracking litigation, generally
- § 17:2 What are cookies?
- § 17:3 Browser fingerprinting technology

### **II. FEDERAL CLAIMS**

- § 17:4 Stored Communications Act
- § 17:5 —Standing
- § 17:6 —Meaning of “facility”
- § 17:7 —Meaning of “electronic storage”
- § 17:8 The Wiretap Act
- § 17:9 —Civil remedies

## TABLE OF CONTENTS

- § 17:10 —Standing
- § 17:11 —Meaning of “contents”
- § 17:12 —“Party” exception
- § 17:13 —Meaning of “intercept”
- § 17:14 —“Ordinary course of business”
- § 17:15 The Computer Fraud and Abuse Act
- § 17:16 —“Damages” Requirement
- § 17:17 Video Privacy Protection Act
- § 17:18 —Meaning of “personal identifiable information”
- § 17:19 —Meaning of “video tape service provider”
- § 17:20 —Meaning of “subscriber”
- § 17:21 —Meaning of “knowing disclosure”
- § 17:22 Children’s Online Privacy Protection Act
- § 17:23 —Claims against ad networks and developers; actual knowledge
- § 17:24 —Claims Against Ad Networks and Developers; reliance on schools as intermediaries

## III. CALIFORNIA STATUTORY CLAIMS

### A. CALIFORNIA INVASION OF PRIVACY ACT

- § 17:25 Similarity to Wiretap Act
- § 17:26 Meaning of “consent”
- § 17:27 Aiding and abetting liability for third party interception
- § 17:28 Eavesdropping liability for access to emails

### B. CALIFORNIA UNFAIR COMPETITION LAW

- § 17:29 Unlawful prong
- § 17:30 Unfair conduct prong
- § 17:31 Misrepresentation prong
- § 17:32 Standing under the UCL

### C. OTHER CALIFORNIA LAWS

- § 17:33 California Comprehensive Data Access and Fraud Act
- § 17:34 California Consumer Legal Remedies Act

## IV. NEW YORK STATUTORY CLAIMS

- § 17:35 New York General Business Law § 349

## V. PENNSYLVANIA WIRETAPPING AND ELECTRONIC SURVEILLANCE CONTROL ACT

- § 17:36 Party exception

- § 17:37 Locus of interception
- § 17:38 Consent

## VI. CALIFORNIA COMMON LAW CLAIMS

- § 17:39 Trespass to chattels
- § 17:40 —Unjust enrichment theory of damages
- § 17:41 —Impact of *Facebook Internet Tracking Litigation*
- § 17:42 Intrusion upon seclusion
- § 17:43 —What kind of data creates a reasonable expectation of privacy?
- § 17:44 — —IP addresses
- § 17:45 — —URLs
- § 17:46 —Highly offensive intrusion
- § 17:47 —Surreptitious tracking
- § 17:48 —Geolocation claims
- § 17:49 Invasion of privacy in violation of California Constitution

## PART C. DIGITAL RIGHTS CLAIMS

### CHAPTER 18. ANTITRUST LITIGATION

- § 18:1 Increasing scrutiny of technology companies
- § 18:2 Antitrust, generally
- § 18:3 Sherman Act Section 1
- § 18:4 —Government enforcement for ecommerce activities
- § 18:5 —Antitrust litigation related to payment cards
- § 18:6 — —Conspiracy
- § 18:7 — —Tying arrangements
- § 18:8 — —Vertical restraints
- § 18:9 Sherman Act Section 2
- § 18:10 —Government enforcement of technology companies and social media platforms
- § 18:11 — —Facebook
- § 18:12 — —Google
- § 18:13 —Private litigation against Apple
- § 18:14 —Private litigation against Google

### CHAPTER 19. WEBSITE ACCESSIBILITY

#### I. WEBSITE ACCESSIBILITY

- § 19:1 Website accessibility, in general

#### II. RELEVANT STATUTES AND REGULATIONS

- § 19:2 Americans with Disabilities Act of 1990

## TABLE OF CONTENTS

§ 19:3	—Public accommodations under Title III
§ 19:4	—DOJ regulations implementing Title III
§ 19:5	— —Accessibility of website information
§ 19:6	—DOJ regulations implementing Title II and Title III—Inactive regulations
§ 19:7	—DOJ proposed regulations implementing Title II
§ 19:8	—Web content accessibility guidelines
§ 19:9	— —DOJ implementation and enforcement
§ 19:10	—Circuit split on applicability of Title III
§ 19:11	— —Nexus requirement
§ 19:12	— —“No nexus” requirement
§ 19:13	Website accessibility requirements under the California Consumer Privacy Act of 2018

## III. CLAIMS

§ 19:14	Causes of action for violations of Title III of the ADA in website accessibility cases
§ 19:15	—Pendent Section 504 claims
§ 19:16	—Pendent civil rights claims

## IV. DEFENSES

§ 19:17	Defenses
§ 19:18	—Statutory
§ 19:19	—Remediation and mootness
§ 19:20	—Standing
§ 19:21	—Third-party host and information content provider
§ 19:22	—Due Process
§ 19:23	—Nexus to physical location
§ 19:24	Damages

## V. LITIGATION

§ 19:25	Website accessibility litigation, in general
§ 19:26	—Eleventh Circuit
§ 19:27	—Ninth Circuit
§ 19:28	—Second Circuit
§ 19:29	Impacted industries
§ 19:30	Litigation and regulatory risk trends

## CHAPTER 20. WEB SCRAPING

### I. INTRODUCTION

§ 20:1	What is web scraping?
--------	-----------------------

- § 20:2 The practice of scraping
- § 20:3 Who scrapes, and what do they scrape?
- § 20:4 Ongoing tactics to prevent or regulate scraping, and the responses by scrapers

## II. CAUSES OF ACTION

- § 20:5 Computer Fraud and Abuse Act
- § 20:6 —Legislative history
- § 20:7 —Circuit split over meaning of “exceeds authorized access”
- § 20:8 — —Supreme Court review
- § 20:9 —Current trends
- § 20:10 Trespass to chattels
- § 20:11 —Unauthorized interference
- § 20:12 —Damages
- § 20:13 Web scraping and copyright
- § 20:14 —Meaning of “copying”
- § 20:15 —Meaning of “improper appropriation”
- § 20:16 —Burden of proof
- § 20:17 —Limitations for factual works and unoriginal arrangements
- § 20:18 —Fair use
- § 20:19 —Remedies
- § 20:20 Anti-circumvention protections of the Digital Millennium Copyright Act
- § 20:21 —Elements of a 1201(a)(1) claim
- § 20:22 —Elements of a 1201(a)(2) claim
- § 20:23 —Elements of a 1201(b)(1) claim
- § 20:24 —Affirmative defenses
- § 20:25 Web scraping as trade secret misappropriation
- § 20:26 —Elements
- § 20:27 —Definition of “misappropriation”
- § 20:28 —Use of bots
- § 20:29 Breach of contract
- § 20:30 —Clickwrap agreements
- § 20:31 —Browsewrap agreements
- § 20:32 Intentional/tortious interference with contractual relations
- § 20:33 —Elements
- § 20:34 State anti-hacking statutes
- § 20:35 —California
- § 20:36 — —Criminal penalties
- § 20:37 —New York
- § 20:38 Web scraping and free speech

## TABLE OF CONTENTS

- § 20:39 —Time, place and manner restrictions
- § 20:40 —Illinois Biometric Information Privacy Act

## **PART D. REGULATORY ENFORCEMENT**

### **CHAPTER 21. FEDERAL TRADE COMMISSION**

- § 21:1 Introduction
- § 21:2 Structure of the Federal Trade Commission
- § 21:3 FTC authority regarding unfair or deceptive practices
- § 21:4 —Deceptive acts or practices
- § 21:5 —Unfair acts or practices
- § 21:6 —Rulemaking
- § 21:7 —Enforcement
- § 21:8 —Consent orders
- § 21:9 —Enforcement procedures
- § 21:10 —Enforcement remedies
- § 21:11 FTC data security enforcement history
- § 21:12 FTC enforcement regarding data breaches
- § 21:13 —Data minimization
- § 21:14 —Secure development and deployment
- § 21:15 —Risk assessments
- § 21:16 —Employees
- § 21:17 —Third party oversight
- § 21:18 —Technical security measures
- § 21:19 —Encryption
- § 21:20 —Secure disposal
- § 21:21 —Escalating security issues
- § 21:22 FTC enforcement challenges
- § 21:23 —Wyndham Worldwide Corporation
- § 21:24 —LabMD
- § 21:25 Other FTC data security authority
- § 21:26 —Gramm-Leach-Bliley Act
- § 21:27 —Fair Credit Reporting Act
- § 21:28 —Health Breach Notification Rule
- § 21:29 Efforts to expand FTC authority
- § 21:30 Civil penalty authority
- § 21:31 Administrative Procedure Act rulemaking
- § 21:32 Nonprofits and common carriers

## **CHAPTER 22. GENERAL DATA PROTECTION REGULATION (“GDPR”)**

### **I. OVERVIEW**

- § 22:1 Introduction to the General Data Protection Regulation
- § 22:2 Collective action lawsuits
- § 22:3 —Notable EU collective actions under the GDPR

### **II. FINES AND ORDERS ISSUED BY EU SUPERVISORY AUTHORITIES**

- § 22:4 EU regulatory enforcement powers
- § 22:5 —Notable fines
- § 22:6 —Article 5 (Principles of processing)
- § 22:7 —Article 6 (Lawfulness of processing)
- § 22:8 —Article 7 (Conditions for consent)
- § 22:9 —Article 9 (Processing of special categories of personal data)
- § 22:10 —Article 12 (Transparency)
- § 22:11 —Article 13 (Privacy Notices where personal data are collected from the data subject)
- § 22:12 —Article 14 (Privacy notice where personal data have not been obtained from the data subject)
- § 22:13 —Article 15 (Right of access)
- § 22:14 —Article 17 (Right to erasure)
- § 22:15 —Article 21 (Right to object)
- § 22:16 —Article 25 (Data protection by design)
- § 22:17 —Article 28 (Processor)
- § 22:18 —Article 32 (Security of processing)
- § 22:19 —Article 33 (Personal Breach Notification)
- § 22:20 —Article 35 (Data protection impact assessment)
- § 22:21 —Article 37 (Designation of a data protection officer)
- § 22:22 —Article 58 (Supervisory authority powers)

### **III. ENFORCEABILITY OF GDPR SUPERVISORY AUTHORITY ORDERS IN U.S. COURTS**

- § 22:23 U.S. legal framework
- § 22:24 Enforceability of EU supervisory authority rulings in U.S. courts through injunctive relief
- § 22:25 Enforceability of EU administrative fines in U.S. courts through judgments for taxes, fines and penalties



TABLE OF CONTENTS

**IV. ENFORCEABILITY OF JUDGMENTS BY DATA  
SUBJECTS IN U.S. COURTS**

- § 22:26 Civil claims in U.S. courts seeking recognition of  
GDPR judgments
- § 22:27 —Personal jurisdiction
- § 22:28 — —Whose law applies?
- § 22:29 — —Jurisdiction based on Article 3 of the GDPR.
- § 22:30 — —Jurisdiction based on agency theory
- § 22:31 —Repugnancy to federal or state public policy
- § 22:32 —Subject matter jurisdiction
- § 22:33 —Article III standing
- § 22:34 — —Individual actions
- § 22:35 — —Representative body claims
- § 22:36 FTC remedies for violation of the GDPR
- § 22:37 Data subject rights under the EU-U.S. Framework

**Table of Laws and Rules**

**Table of Cases**

**Index**