

# Table of Contents

## PART I. PRIVACY

### CHAPTER 1. OVERVIEW OF PRIVACY LAW

- § 1:1 Introduction
- § 1:2 Privacy issues in the workplace—Preemployment inquiries
  - § 1:3 —Employee and applicant testing
  - § 1:4 —Employee background checks
  - § 1:5 —Employee monitoring
  - § 1:6 —Personnel and medical records
  - § 1:7 —Health Insurance Portability and Accountability Act
- § 1:8 Privacy issues related to the internet and e-commerce—Privacy policies
  - § 1:9 —Children’s Online Privacy Protection Act of 1998
  - § 1:10 —Cybersmearing
  - § 1:11 —Unsolicited commercial e-mail
- § 1:12 Federal privacy statutes—Wiretapping
  - § 1:13 —Computer Fraud and Abuse Act
  - § 1:14 —Gramm-Leach-Bliley Act
  - § 1:15 —Unsolicited telephone calls and facsimiles—Telephone Consumer Protection Act of 1991
  - § 1:16 —The Junk Fax Prevention Act of 2005
- § 1:17 State privacy law-related claims—State privacy laws
  - § 1:18 —Right of publicity
  - § 1:19 International privacy issues
- § 1:20 Workplace privacy torts: Termination and beyond
- § 1:21 The Consumer Privacy Bill of Rights

### CHAPTER 2. THE GRAMM-LEACH-BLILEY ACT

- § 2:1 Introduction
- § 2:2 Scope
  - § 2:3 —Regulated entities
    - § 2:4 —Financial institution
    - § 2:5 —Nonaffiliated third party
  - § 2:6 —Protected entities
    - § 2:7 —Consumer
    - § 2:8 —Customer
    - § 2:9 —Information

- § 2:10 —Exceptions
- § 2:11 —Redislosure and reuse
- § 2:12 Notice
- § 2:13 —Types
- § 2:14 —Content
- § 2:15 — —Privacy notice
- § 2:16 — —Opt-out notice
- § 2:17 —Form
- § 2:18 —Recipients
- § 2:19 — —Consumers
- § 2:20 — —Customers—Current
- § 2:21 — — —Former
- § 2:22 — —Joint transactions
- § 2:23 —Delivery
- § 2:24 —Timing
- § 2:25 — —Privacy—Consumers
- § 2:26 — — —Customers
- § 2:27 — —Opt out
- § 2:28 Opt-out procedures
- § 2:29 —Opportunity
- § 2:30 —Duration
- § 2:31 —Joint relationships
- § 2:32 —Exceptions
- § 2:33 Standards for safeguarding customer information
- § 2:34 State laws
- § 2:35 Pretexting
- § 2:36 Litigation Discovery
- § 2:37 Conclusion

Appendix 2-A. FTC Guidance on Privacy Rule

Appendix 2-B. FTC Safeguards Rule: What Your Business  
Needs to Know

## CHAPTER 3. STATE PRIVACY LAWS

- § 3:1 Introduction
- § 3:2 Selected summary of state privacy laws—State unfair  
and deceptive trade practices acts
- § 3:3 —State versions of federal privacy laws
- § 3:4 —Privacy acts
- § 3:5 —Identity theft statutes
- § 3:6 —Credit reporting statutes
- § 3:7 —State insurance record laws
- § 3:8 —Common-law privacy claims
- § 3:9 —State constitutions
- § 3:10 —Computer crime/internet laws
- § 3:11 —Trespass/trespass to chattels/other novel tort claims

## TABLE OF CONTENTS

|               |   |
|---------------|---|
| § 3:12        | —Disposal of consumer information contained in business records                                 |
| § 3:13        | —Telemarketing laws   |
| § 3:14        | —Drone regulation   |
| § 3:15        | —Miscellaneous state laws   |
| § 3:16        | Causes of actions addressing various violations of state privacy laws                           |
| § 3:17        | —Failure to disclose—Use of cookies and web bugs  |
| § 3:18        | — —Providing information to third parties/marketing firms                                       |
| § 3:19        | —Misrepresentation regarding the use of information   |
| § 3:20        | —Biometric data protection  |
| § 3:21        | —State law right-of-publicity claims  |
| § 3:22        | — —Does a corporation have a right of privacy?  |
| § 3:23        | —Common-law tort/invasion-of-privacy claims   |
| § 3:24        | Conclusion  |
| Appendix 3-A. | California Consumer Privacy Act of 2018   |
| Appendix 3-B. | FTC Policy Statement on Biometric Information and Section 5 of the Federal Trade Commission Act |

## CHAPTER 4. INTERNATIONAL PRIVACY ISSUES

|               |  |
|---------------|--|
| § 4:1         | Introduction   |
| § 4:2         | European community directive on data protection  |
| § 4:3         | EU-U.S. Privacy Shield Framework   |
| § 4:4         | Canadian actions   |
| § 4:5         | Data breach notification   |
| § 4:6         | Records retention requirements—What records must be retained?  |
| § 4:7         | —What are the requirements?  |
| § 4:8         | —Verification  |
| § 4:9         | International privacy resources  |
| Appendix 4-A. | Directive 95/46/EC   |
| Appendix 4-B. | Commission decision of 8 May 2008 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Jersey |
| Appendix 4-C. | Digital Agenda: How New EU Rules Improve Privacy Protection for Internet Users (Memo/11/320)   |
| Appendix 4-D. | Letter from U.S. Department of Commerce, International Trade Administration, on the Schrems II Decision (September 2020)   |

- Appendix 4-E. EU-US Data Privacy Framework Updates
- Appendix 4-F. The GDPR, New Opportunities, New Obligations—What Every Business Needs to Know about the EU’s General Data Protection Regulation (European Commission, Directorate-General for Justice and Consumers, Publications Office of the European Union 2019, <https://data.europa.eu/doi/10.2838/820044>)
- Appendix 4-G. Seven Steps for Businesses to Get Ready for the General Data Protection Regulation (European Commission)

## CHAPTER 5. RECORD-KEEPING ASPECTS OF PRIVACY LAWS

- § 5:1 Introduction
- § 5:2 Children’s Online Privacy Protection Act
- § 5:3 —Provisions of the Children’s Online Privacy Protection Act
- § 5:4 —Record-keeping issues
- § 5:5 Gramm-Leach-Bliley Act
- § 5:6 Health Insurance Portability and Accountability Act of 1996
- § 5:7 Company privacy policies—Generally
- § 5:8 —Training
- § 5:9 —Audits
- § 5:10 Privacy and corporate e-discovery
- § 5:11 Conclusion
- § 5:12 The Internet of Things Cybersecurity Improvement Act of 2020
- Appendix 5-A. FTC Policy Statements on COPPA

## CHAPTER 6. THE RIGHT OF PUBLICITY

- § 6:1 Introduction
- § 6:2 Historical development of the right of publicity
- § 6:3 Types of right of publicity claims
- § 6:4 —State statutory and common-law right of publicity claims
- § 6:5 — —The persona
- § 6:6 — —Use without permission
- § 6:7 — —Commercial purpose
- § 6:8 — —Releases
- § 6:9 —Right of publicity claims under the Lanham Act
- § 6:10 Preemption
- § 6:11 Types of damages awarded
- § 6:12 Right of publicity defenses and preemption issues—The First Amendment defense

## TABLE OF CONTENTS

- § 6:13 —Copyright law preemption as a bar to a right of publicity claim
- § 6:14 —The copyright law’s first sale doctrine as a defense
- § 6:15 Right of publicity issues on the Internet and the growth of new technology—The Internet
- § 6:16 —Computer-generated imagery
- § 6:17 Checklist for licensing a name and likeness

## **CHAPTER 7. ELECTRONIC TRANSACTIONS AND PRIVACY STANDARDS UNDER HIPAA**

- § 7:1 Introduction
- § 7:2 Administrative simplification
- § 7:3 Electronic transaction standards
- § 7:4 Medical privacy rules
- § 7:5 —Overview
- § 7:6 —Specific privacy requirements
- § 7:7 —Key concepts and definitions
- § 7:8 —Patients’ rights to control their health information
- § 7:9 —Consent and authorization
- § 7:10 —Definition of “minimum necessary”
- § 7:11 —Business associates
- § 7:12 —Parents and minors
- § 7:13 —Marketing
- § 7:14 —Preemption of state privacy laws
- § 7:15 —Enforcement
- § 7:16 —Subsequent revisions
- § 7:17 Compliance
- § 7:18 Immunity
- § 7:19 Conclusion
- Appendix 7-A. Sample Business Associate Agreement Provisions
- Appendix 7-B. Permitted Uses and Disclosures: Healthcare Operations
- Appendix 7-C. Permitted Uses and Disclosures: Exchange for Treatment
- Appendix 7-D. Department of Health and Human Services Guidance on HIPAA & Cloud Computing
- Appendix 7-E. HIPAA Basics for Providers: Privacy, Security, and Breach Notification Rules (U.S. Department of Health & Human Services—February 2023)
- Appendix 7-F. Guide to Privacy and Security of Electronic Health Information (U.S. Department of Health & Human Services—April 2015)

Appendix 7-G. Collecting, Using, or Sharing Consumer Health Information? Look to HIPAA, the FTC Act, and the Health Breach Notification Rule (Federal Trade Commission—August 2024)

## **PART II. SAMPLE POLICIES AND CHECKLISTS**

### **CHAPTER 8. MASTER PRIVACY CHECKLIST**

- § 8:1 Privacy issues in the workplace
- § 8:2 Privacy issues related to the internet and e-commerce
- § 8:3 Federal privacy statutes
- § 8:4 State privacy law issues
- § 8:5 International privacy issues

Appendix 8-A. FTC Data Breach Response and model letter

### **CHAPTER 9. PRIVACY POLICIES**

- § 9:1 Introduction
- § 9:2 Due diligence issues involved in drafting a privacy policy
- § 9:3 Drafting the policy
- § 9:4 —FTC fair information collection principles
- § 9:5 —The importance of a “readable” policy
- § 9:6 —The use of absolutes/contrary statements
- § 9:7 —Relationships with third parties/affiliates and online profiling
- § 9:8 —Available tools/models for drafting a policy
- § 9:9 —State privacy policy legislation
- § 9:10 —The use of click-through agreements for opt-in/opt-out purposes
- § 9:11 —Third-party oversight seals on web sites
- § 9:12 Amending a policy
- § 9:13 Software tools to assist consumers in understanding a site’s privacy policy
- § 9:14 Corporate software tools for privacy policies
- § 9:15 Company enforcement of privacy policies—  
Enforcement/legal action—Misrepresentation or nondisclosure regarding information collection practices
- § 9:16 — —Selling personally identifiable information (a database) in a bankruptcy in violation of privacy policy
- § 9:17 — —Unintentional release of personally identifiable information

## TABLE OF CONTENTS

- § 9:18 — —Claims regarding the security of information
- § 9:19 — —Private litigation
- § 9:20 —General suggestions concerning compliance/auditing issues
- § 9:21 —Checklist for developing/auditing a privacy policy
- § 9:22 Conclusion
- Appendix 9-A. Discussion and Sampling of Privacy Policy Clauses
- Appendix 9-B. Remington Colleges Privacy Policy

## **PART III. EMPLOYMENT**

### **CHAPTER 10. PRIVACY ISSUES IN PREEMPLOYMENT INQUIRIES**

- § 10:1 Introduction
- § 10:2 Sources of privacy protection—Constitutions
- § 10:3 —State laws—Right to privacy statutes
- § 10:4 — —Marital status statutes
- § 10:5 —Common-law invasion of privacy
- § 10:6 Federal statutes—Pregnancy
- § 10:7 —Americans with Disabilities Act
- § 10:8 — —Inquiries related to ability to perform job functions and accommodations
- § 10:9 — —Inquiries about attendance
- § 10:10 — —Drug and alcohol usage
- § 10:11 —ADA Amendments Act
- § 10:12 —Americans with Disabilities Act—Unlawful inquiries tied to a disability
- § 10:13 —Other federal antidiscrimination statutes
- § 10:14 Employment references
- § 10:15 Conclusion
- Appendix 10-A. Washington Administrative Code
- Appendix 10-B. ADA Amendments Act of 2008 (PL 110-325, 2008 S 3406) (effective January 1, 2009)
- Appendix 10-C. EEOC's Answers to Frequently Asked Questions to Rulemaking Under the ADA Amendments Act

### **CHAPTER 11. PRIVACY ASPECTS OF EMPLOYEE AND APPLICANT TESTING**

- § 11:1 Introduction
- § 11:2 Preemployment personality and psychological testing
- § 11:3 —Types of personality and psychological tests
- § 11:4 —Ensuring lawful testing practices

- § 11:5 Polygraph tests
- § 11:6 —Prohibitions on lie detector use
- § 11:7 —Notice requirements
- § 11:8 —Enforcement
- § 11:9 —Exemptions
- § 11:10 — —Governmental employers
- § 11:11 — —National defense and security
- § 11:12 — —Ongoing investigations
- § 11:13 — —Security services
- § 11:14 — —Employers in the controlled substances industry
- § 11:15 —Restrictions on the use of exemptions
- § 11:16 —The examiner
- § 11:17 —Disclosure of information
- § 11:18 —Operation of state law
- § 11:19 —Effect on other legal claims
- § 11:20 Substance abuse testing
- § 11:21 —Types of testing
- § 11:22 —State constitutional privacy rights
- § 11:23 —State statutes and common-law principles—State and local statutes
- § 11:24 — —Common-law principles
- § 11:25 — — —Defamation
- § 11:26 — — —Invasion of privacy
- § 11:27 Genetic testing
- § 11:28 —Genetic monitoring and screening
- § 11:29 —Confidentiality
- § 11:30 —Health and safety
- § 11:31 —Wellness programs
- § 11:32 —Common-law privacy issues—Invasion of privacy
- § 11:33 — —Defamation
- § 11:34 —other statutory privacy protections
- § 11:35 Health checks in pandemic situations
- § 11:36 Conclusion

Appendix 11-A. Sample Policy on Genetic Information

Appendix 11-B. Sample Policy for Wellness Program

## CHAPTER 12. PRIVACY IMPLICATIONS OF USING CREDIT REPORTS FOR EMPLOYMENT PURPOSES

- § 12:1 Introduction
- § 12:2 Key terms
- § 12:3 —“Person”
- § 12:4 —“Consumer”
- § 12:5 —“Consumer report”
- § 12:6 —“Investigative consumer report”



## TABLE OF CONTENTS

- § 12:7 Employer use of consumer reports
- § 12:8 —Written disclosure and consent
- § 12:9 —Certification to the consumer reporting agency
- § 12:10 —Requirements when adverse action taken
- § 12:11 —Disposal of information
- § 12:12 Employer use of investigative consumer reports
- § 12:13 The Fair and Accurate Credit Transactions Act of 2003
- § 12:14 Penalties for violations
- Appendix 12-A. CFPB Model Summaries of FCRA Rights and Notice of User Responsibilities

## **CHAPTER 13. USING CRIMINAL, BANKRUPTCY, AND OTHER RECORDS IN EMPLOYMENT BACKGROUND CHECKS**

- § 13:1 Criminal records—State laws
- § 13:2 —Negligent hiring
- § 13:3 Bankruptcy
- § 13:4 Miscellaneous records—Driving records
- § 13:5 —Academic records
- § 13:6 —Arrests
- § 13:7 Conclusion

## **CHAPTER 14. EMPLOYEE MONITORING**

- § 14:1 Introduction
- § 14:2 E-mail monitoring and social media
- § 14:3 E-mail monitoring—The Electronic Communications Privacy Act
- § 14:4 — —The business-use exception
- § 14:5 — —The employee consent exception
- § 14:6 —Other sources of privacy protection
- § 14:7 Computer monitoring and searches
- § 14:8 Monitoring “snail mail”
- § 14:9 Telephone monitoring
- § 14:10 Video surveillance monitoring
- § 14:11 Breastfeeding
- § 14:12 State law
- § 14:13 Conclusion

## **CHAPTER 15. PRIVACY ASPECTS OF PERSONNEL AND EMPLOYEE MEDICAL RECORDS**

- § 15:1 Introduction
- § 15:2 Personnel records generally
- § 15:3 —Disclosure to third parties

- § 15:4 — —Blacklisting
- § 15:5 —Disclosure to unions
- § 15:6 —Other potential liability
- § 15:7 — —Defamation
- § 15:8 — —Interference with prospective economic advantage
- § 15:9 — —Public disclosure of private facts
- § 15:10 Employee medical records—State laws
- § 15:11 —Federal laws
- § 15:12 —Efforts to enhance individuals’ access to health information
- § 15:13 Conclusion
- Appendix 15-A. Select State Laws Concerning Employee Medical Records and Personnel Records
- Appendix 15-B. EEOC Fact Sheet on Obtaining and Using Employee Medical Information as Part of Emergency Evacuation Procedures

## **PART IV. CYBERSPACE AND ELECTRONIC COMMUNICATION PRIVACY**

### **CHAPTER 16. COMPUTER FRAUD AND ABUSE ACT**

- § 16:1 Overview
- § 16:2 General civil and criminal cases
- § 16:3 Authorized access
- § 16:4 Individual privacy cases
- § 16:5 —*In re Intuit* privacy litigation
- § 16:6 —*In re DoubleClick* privacy litigation
- § 16:7 —*Register.com v. Verio*
- § 16:8 —*Theofel v. Farey-Jones*, No. 02-15742 (9th Cir. Aug. 28, 2003) (overbroad subpoena)
- § 16:9 —*Role Models Am., Inc. v. Jones & Nova S.E. Univ., Inc.* No. 03-1857 (D. Ma. Feb. 25, 2004)
- § 16:10 Employer/employee confidentiality agreements and computer fraud by employees
- § 16:11 Conclusion

### **CHAPTER 17. THE CHILDREN’S ONLINE PRIVACY PROTECTION ACT OF 1998**

- § 17:1 Introduction
- § 17:2 Scope of the Children’s Online Privacy Protection Act of 1998

## TABLE OF CONTENTS

- § 17:3 Complying with the Children’s Online Privacy Protection Act of 1998—Privacy notice
- § 17:4 —Parental consent
- § 17:5 —Security measures
- § 17:6 —Safe harbor provision
- § 17:7 Enforcement
- § 17:8 Records retention
- Appendix 17-A. Children’s Online Privacy Protection Rule 16 C.F.R. Part 312
- Appendix 17-B. FTC Six Step Checklist for COPPA Compliance

## **CHAPTER 18. THE VIDEO PRIVACY PROTECTION ACT OF 1988**

- § 18:1 The Video Privacy Protection Act of 1988
- Appendix 18-A. Video Privacy Protection Act of 1988

## **CHAPTER 19. CABLE COMMUNICATIONS POLICY ACT OF 1984**

- § 19:1 Cable Communications Policy Act of 1984
- Appendix 19-A. Cable Communications Policy Act of 1984

## **CHAPTER 20. STATE DATA SECURITY LAWS**

- § 20:1 Introduction
- § 20:2 Destruction of records provisions
- § 20:3 Security measures required
- § 20:4 Notification requirements
- § 20:5 Recommended practices
- § 20:6 —Protection and prevention
- § 20:7 —Preparation for notification
- § 20:8 —Notification
- § 20:9 Data breach litigation
- § 20:10 —Standing
- § 20:11 —Discovery
- § 20:12 —Insurance
- § 20:13 —Medical records

## **CHAPTER 21. CYBERSMEARING**

- § 21:1 Introduction
- § 21:2 Legal theories to combat cybersmearing—Defamation
- § 21:3 — —Elements of a libel action
- § 21:4 — —Immunity under the Communications Decency Act

- § 21:5 — — — Internet service providers
- § 21:6 — — — Web site operators
- § 21:7 — — — Repostings
- § 21:8 — — Anonymous posters
- § 21:9 — — — Parties to the action
- § 21:10 — — — Nonparties to an action
- § 21:11 — — Anti-SLAPP statutes
- § 21:12 — — Web hosting policies
- § 21:13 — — Jurisdictional issues on the internet
- § 21:14 — Trademark actions
- § 21:15 — — Trademark infringement
- § 21:16 — — — Use in commerce and likelihood of confusion
- § 21:17 — — — Exceptions
- § 21:18 — — — Metatags
- § 21:19 — — Dilution
- § 21:20 — — — Requirements of the Federal Trademark  
Dilution Act
- § 21:21 — — — Exceptions
- § 21:22 — — Cybersquatting
- § 21:23 — — — Anticybersquatting Consumer Protection Act
- § 21:24 — — — Uniform dispute resolution policy
- § 21:25 — State laws and tort theories of unfair competition
- § 21:26 — — Trade secret misappropriation
- § 21:27 — — Breach of fiduciary duty
- § 21:28 — — Unfair and deceptive trade practices
- § 21:29 — — Product disparagement
- § 21:30 — — Interference with business relations
- § 21:31 — Securities fraud
- § 21:32 Jurisdictional problems—Cybersmearing
- § 21:33 Conclusion

## CHAPTER 22. SPYWARE

- § 22:1 Introduction
- § 22:2 State spyware legislation
- § 22:3 Federal legislation
- § 22:4 Litigation/enforcement—FTC actions
- § 22:5 — Litigation
- § 22:6 — State actions
- § 22:7 — European Union

Appendix 22-A. California Spwyare Law—Consumer  
Protection against Computer Spyware Act

## CHAPTER 23. UNSOLICITED COMMERCIAL E-MAIL

- § 23:1 Introduction

## TABLE OF CONTENTS

- § 23:2 CAN-SPAM Act—General requirements
- § 23:3 —Preemption of state laws
- § 23:4 —UCE and wireless subscribers
- § 23:5 —Enforcement/penalties
- § 23:6 State spam laws
- § 23:7 Litigation/enforcement
- § 23:8 —Trespass to chattel, constitutional claims, and other theories
- § 23:9 —Litigation involving internet service providers
- § 23:10 —State enforcement
- § 23:11 Best practices for online marketers sending unsolicited commercial e-mail
- § 23:12 Counseling suggestions
- § 23:13 Conclusion

## CHAPTER 24. UNSOLICITED FACSIMILES

- § 24:1 Overview
- § 24:2 Exception—Established business relationship (EBR)
- § 24:3 —Directories
- § 24:4 Exceptions—Established business relationship (EBR)—Trade association memberships
- § 24:5 The Junk Fax Prevention Act of 2005—EBR exception
- § 24:6 —Determining what qualifies as an advertisement
- § 24:7 —Opt-out notice requirement
- § 24:8 Fax broadcasters
- § 24:9 —Vicarious liability
- § 24:10 Fax servers
- § 24:11 Penalties for violations of the TCPA fax provisions
- § 24:12 Insurance coverage for TCPA fax provision violations
- § 24:13 2013 FCC Amendments
- § 24:14 Conclusion

## CHAPTER 25. UNSOLICITED TELEPHONE CALLS

- § 25:1 Introduction to the Telephone Consumer Protection Act of 1991
- § 25:2 2003 FCC rules implementing the TCPA—The national do-not-call list
- § 25:3 —Company do-not-call lists
- § 25:4 —Tax-exempt nonprofit organization exemption
- § 25:5 —Automated telephone dialing equipment
- § 25:6 — —Predictive dialers
- § 25:7 —Abandoned calls
- § 25:8 —Caller identification
- § 25:9 2005 FCC rules implementing the TCPA—The EBR exemption

- § 25:10 —Company-specific do-not-call lists
- § 25:11 Penalties for violations of the TCPA
- § 25:12 Standing
- § 25:13 State do-not-call lists
- § 25:14 Emergency purposes exemption
- § 25:15 Conclusion

## **CHAPTER 26. WIRETAPPING**

- § 26:1 Introduction
- § 26:2 What constitutes a communication?
- § 26:3 What constitutes an interception?
- § 26:4 Exceptions to the prohibition on interception or disclosure
- § 26:5 Procedures for law enforcement officers to use an intercepting device
- § 26:6 Improper disclosure of an authorized wiretap
- § 26:7 Disclosure of an illegally intercepted communication by the media
- § 26:8 Prohibition of intercepting devices
- § 26:9 Exclusionary rule
- § 26:10 Remedies for interception
- § 26:11 State wiretap laws
- § 26:12 Workplace surveillance

## **CHAPTER 27. STORED COMMUNICATIONS ACT**

- § 27:1 Introduction
- § 27:2 Unlawful access to stored communications
- § 27:3 Voluntary disclosure of customer communications or records
- § 27:4 Required disclosure of customer communications or records
- § 27:5 —Backup preservation
- § 27:6 Civil actions
- § 27:7 Counterintelligence access to telephone toll and transactional records
- § 27:8 Website/browser activity

## **APPENDIX**

Appendix A. Selected Web Sites

**Table of Laws and Rules**

**Table of Cases**

**Index**