

Table of Contents

CHAPTER 1. ELECTRONIC SECURITY RISKS AND THE NEED FOR PRIVACY

§ 1:1	Introduction
§ 1:2	Cyberattacks against government agencies
§ 1:3	Cyberattacks against businesses
§ 1:4	Cyberattacks against society in general
§ 1:5	—Cyberterrorism and infowarfare
§ 1:6	—Viruses and other “malware” pandemics
§ 1:7	—Identity theft
§ 1:8	Culprits/perpetrators
§ 1:9	—General make-up
§ 1:10	—Categories
§ 1:11	— —Hacker
§ 1:12	— —Cracker
§ 1:13	— —Hit-man
§ 1:14	— —Page-jacker
§ 1:15	— —Employee
§ 1:16	— —Ex-employee
§ 1:17	— —Phreaker
§ 1:18	— —Overview of state-sponsored cyberthreats
§ 1:19	— —State-sponsored threats from the People’s Republic of China (PRC)
§ 1:20	— —State-sponsored threats from Russia and other countries
§ 1:21	Methods and tools for gaining system access
§ 1:22	—Physical access
§ 1:23	—Technical access
§ 1:24	— —Probing
§ 1:25	— —Scanning
§ 1:26	— —Cracking codes, passwords and keys
§ 1:27	— —Sniffing
§ 1:28	— —Spoofing
§ 1:29	— —Wardriving
§ 1:30	— —ATM skimming
§ 1:31	—System compromise
§ 1:32	— —Packet sniffing
§ 1:33	— —Snooping and downloading
§ 1:34	— —Data tampering or manipulating
§ 1:35	Methods and tools for cyberattacks
§ 1:36	—Viruses
§ 1:37	— —Traditional
§ 1:38	— —Boot sector
§ 1:39	— —Partition sector
§ 1:40	— —Macro
§ 1:41	— —Polymorphic
§ 1:42	— —Stealth
§ 1:43	— —Multipartite
§ 1:44	—Trojan horse
§ 1:45	— —Logic bomb
§ 1:46	—Ransomware
§ 1:47	—Phishing

- § 1:48 —Hoaxes
- § 1:49 —Worms
- § 1:50 —Denial of service
- § 1:51 —Infrastructure attacks
- § 1:52 Examples of malware program code
- § 1:53 —Virus: Macro
- § 1:54 —Virus: Batch file
- § 1:55 —Trojan horse
- § 1:56 Legal ramifications of cyberattacks
- § 1:57 Privacy issues
- § 1:58 —Data gathering
- § 1:59 —Aggregating
- § 1:60 —Automated data interception systems
- § 1:61 — —NarusInsight
- § 1:62 — —Echelon
- § 1:63 — —Terrorism Information Awareness
- § 1:64 —E-911
- § 1:65 Conclusion

CHAPTER 2. SECURITY AND PRIVACY IN THE NETWORKED WORLD

- § 2:1 Introduction
- § 2:2 The increasing vulnerability of networks
- § 2:3 Overview of cyberattacks
- § 2:4 Overview of privacy issues
- § 2:5 Cyberattacks and privacy cost assessments
- § 2:6 Technological overview of networks
- § 2:7 —Brief history of NISs
- § 2:8 — —Birth of the Internet
- § 2:9 — —Emergence of the World Wide Web
- § 2:10 — —Future of the Internet and World Wide Web
- § 2:11 —Operation of networks
- § 2:12 — —Network topologies and relationships
- § 2:13 — —Network hardware, software, and protocols
- § 2:14 — —Classifications of networks
- § 2:15 New technologies subject to cyberattacks
- § 2:16 —Telephone and SMS malware and scams
- § 2:17 —Cellular telephone spam
- § 2:18 —Voice over Internet Protocol (VoIP)
- § 2:19 —Radio-frequency identification (RFID)
- § 2:20 —Cloud computing and storage
- § 2:21 —Geolocation
- § 2:22 —Smart grids
- § 2:23 —Vehicles
- § 2:24 —Medical Devices
- § 2:25 —Preinstalled Malware
- § 2:26 Next-generation online tracking tools
- § 2:27 Conclusion

CHAPTER 3. TECHNICAL SECURITY MEASURES

- § 3:1 Overview
- § 3:2 Data security generally
- § 3:3 Internal data security

TABLE OF CONTENTS

§ 3:4	—Network
§ 3:5	—System
§ 3:6	External data security
§ 3:7	—DMZ
§ 3:8	—NAT
§ 3:9	—Firewalls
§ 3:10	— —Concepts and usage
§ 3:11	— —Alternatives
§ 3:12	—Networked security traps
§ 3:13	— —Honeypots
§ 3:14	— —Wartrapping and wardriving
§ 3:15	— —Warchalking
§ 3:16	— —Strike-backs
§ 3:17	—System identity verification
§ 3:18	— —Digital certificates
§ 3:19	— —Hash Functions
§ 3:20	— —Kerberos
§ 3:21	—Personal identity verification methods
§ 3:22	— —Tokens and keys
§ 3:23	— —Biometric measures
§ 3:24	— — —Fingerprint
§ 3:25	— — —Signature
§ 3:26	— — —Voice
§ 3:27	— — —Retina
§ 3:28	— — —Facial
§ 3:29	— — —Palm
§ 3:30	Encryption
§ 3:31	—Disk
§ 3:32	—File
§ 3:33	—Message
§ 3:34	—Network
§ 3:35	Intrusion detection systems
§ 3:36	—Designs
§ 3:37	—Signature-based
§ 3:38	—Heuristic-based
§ 3:39	—Anomaly detection
§ 3:40	Industry security initiative: Internet protocol version six

CHAPTER 4. *[Reserved]*

CHAPTER 5. CORPORATE RISK MANAGEMENT

I. OVERVIEW OF RISK-MANAGEMENT PROCESS

§ 5:1	Risk management generally
§ 5:2	Components of risk-management process
§ 5:3	—Risk framing
§ 5:4	—Risk assessment
§ 5:5	—Risk response
§ 5:6	Components of risk management process—Risk response—Policy
§ 5:7	Components of risk-management process—Risk response—Controls
§ 5:8	—Risk monitoring and Audit

II. ANALYSIS OF RISK-MANAGEMENT PROCESS COMPONENTS

A. ANALYSIS OF RISK FRAMING COMPONENT

§ 5:9 Risk framing in general

B. ANALYSIS OF RISK-ASSESSMENT COMPONENT

- § 5:10 Risk assessment of information systems generally
- § 5:11 Information systems security risk
- § 5:12 —Vulnerabilities
- § 5:13 — —Non-technical vulnerabilities
- § 5:14 — —Technical vulnerabilities
- § 5:15 —Threats
- § 5:16 — —Attack phase 1: Reconnaissance
- § 5:17 — —Attack phase 2: Scanning
- § 5:18 — —Attack phase 3: Exploiting systems
- § 5:19 — — —Gaining unauthorized access
- § 5:20 — — —Conducting application-level attacks
- § 5:21 — — —Conducting denial-of-service attacks
- § 5:22 — —Attack phase 4: Maintaining access
- § 5:23 — —Attack phase 5: Covering tracks
- § 5:24 —Losses
- § 5:25 Evaluating enterprise information system security risk
- § 5:26 —Quantitative evaluation
- § 5:27 —Qualitative evaluation
- § 5:28 — —Stage 1: Asset valuation
- § 5:29 — —Stage 2: Risk evaluation
- § 5:30 — —Stage 3: Risk management

C. ANALYSIS OF RISK RESPONSE COMPONENT

- § 5:31 Risk Response generally
- § 5:32 Risk response-policies and controls generally
- § 5:33 Risk response-Information security policy generally
- § 5:34 Developing policy documents
- § 5:35 —IT policy types
- § 5:36 —Pertinent laws and regulations
- § 5:37 —Best practice documents and resources
- § 5:38 Risk response-controls
- § 5:39 Control types, generally
- § 5:40 Technical controls
- § 5:41 Administrative controls
- § 5:42 Applying administrative and technical controls
- § 5:43 Corporate personnel security controls
- § 5:44 —Pre-employment screenings
- § 5:45 —Background investigation
- § 5:46 —Drug screening
- § 5:47 —Self-certification
- § 5:48 Corporate IT security controls
- § 5:49 —Identification and authentication
- § 5:50 — —Information systems access
- § 5:51 — —Password format and management
- § 5:52 — —Computer account management
- § 5:53 — —Remote access

TABLE OF CONTENTS

- § 5:54 —Computer system security
- § 5:55 —Network security
- § 5:56 —Application security
- § 5:57 —Corporate information classification controls
- § 5:58 Physical security controls
- § 5:59 —Public area controls
- § 5:60 —Sensitive area controls
- § 5:61 —Confidential area controls

D. ANALYSIS OF MONITORING AND AUDIT COMPONENT

- § 5:62 Monitoring, audit and regulatory supervision generally
- § 5:63 Internal audits
- § 5:64 External audits

III. SECURITY SERVICES AND MECHANISMS

- § 5:65 Information system security incident response
- § 5:66 —Information systems
- § 5:67 —Incidents and incident response
- § 5:68 — —Incident taxonomy
- § 5:69 — —Incident response methodology
- § 5:70 — — —Phase 1: Prepare
- § 5:71 — — —Phase 2: Identify
- § 5:72 — — —Phase 3: Contain
- § 5:73 — — —Phase 4: Eradicate
- § 5:74 — — —Phase 5: Recover
- § 5:75 — — —Phase 6: Follow-up
- § 5:76 — —Incident/Incident Response Flow
- § 5:77 Open Systems Interconnection (OSI) reference model

IV. THE MODERN RISK LANDSCAPE

- § 5:78 The risk management cycle
- § 5:79 Major sources of risk
- § 5:80 Mobile Devices & the Bring-Your-Own-Device (“BYOD”) workplace
- § 5:81 Cloud computing
- § 5:82 Social media
- § 5:83 The “Internet of Things”
- § 5:84 The Work from Home (“WFH”) workplace
- § 5:85 Artificial Intelligence (“AI”)

CHAPTER 6. DATA SECURITY STATUTES

- § 6:1 Introduction
- § 6:2 The Uniting and Strengthening America by Providing Appropriate Tools Required To Intercept and Obstruct Terrorism Act of 2001 (USA Patriot Act)
- § 6:3 Computer Fraud and Abuse Act of 1986
- § 6:4 —Prohibited acts
- § 6:5 — —Unauthorized access: National security
- § 6:6 — —Confidential information and communications
- § 6:7 — —Government computers
- § 6:8 — —Fraud
- § 6:9 — —Damage to computers
- § 6:10 — —Password trafficking
- § 6:11 — —Threats of extortion

- § 6:12 —Attempted acts
- § 6:13 —Criminal penalties
- § 6:14 — —Violations involving national security
- § 6:15 — —Violations involving confidential information, government computers, password trafficking and access resulting in damage
- § 6:16 — —Violations involving fraud and threats of extortion
- § 6:17 — —Violations involving damages as a result of violations of § 1030(a)(5)
- § 6:18 — —Violations involving knowing or reckless conduct causing serious bodily injury
- § 6:19 — —Violations involving knowing or reckless conduct causing death
- § 6:20 —Authority of Secret Service and Federal Bureau of Investigation
- § 6:21 —Key definitions
- § 6:22 —Government law enforcement activity not affected
- § 6:23 —Private right of action and statute of limitations
- § 6:24 —Mens rea requirement
- § 6:25 —Harvesting of e-mail addresses and spamming
- § 6:26 —Mere access may not be “thing of value”
- § 6:27 —Use by employers against disloyal employees
- § 6:28 —What constitutes “loss”
- § 6:29 Federal wiretap statutes
- § 6:30 —Unlawful interception of wire, oral or electronic communication
- § 6:31 Electronic Communications Privacy Act
- § 6:32 —Title I: Overview of Wiretap Act, General Protection from Interception
- § 6:33 —Title I: When Interception Is Allowed
- § 6:34 —Title I: Redress for Violations of the Wiretap Act
- § 6:35 —Title II: Overview of the SCA
- § 6:36 —Title II: SCA Defenses and Proscriptions
- § 6:37 —Title II: Overview of the CLOUD Act
- § 6:38 —Title III: Overview of Pen Registers and Trap and Trace Devices
- § 6:39 —Title III: Key Definitions
- § 6:40 —Title III: When Installation is Allowed
- § 6:41 —Title III: Violations
- § 6:42 —Title III: Time Period
- § 6:43 —Title III: Geographical Limits
- § 6:44 —Title III: Assistance in Installation
- § 6:45 —Title III: Reporting
- § 6:46 Foreign Intelligence Surveillance Act
- § 6:47 Homeland Security Act of 2002
- § 6:48 Federal Wire Fraud Statute
- § 6:49 —Application
- § 6:50 —Penalties
- § 6:51 No Electronic Theft Act of 1997
- § 6:52 National Stolen Property Act
- § 6:53 —Application
- § 6:54 —Penalties
- § 6:55 Economic Espionage Act
- § 6:56 —Application
- § 6:57 —Penalties
- § 6:58 The Defend Trade Secrets Act—Application
- § 6:59 —Remedies
- § 6:60 The IoT Cybersecurity Improvement Act of 2020
- § 6:61 The K-12 Cybersecurity Act of 2021
- § 6:62 Strengthening American Cybersecurity Act of 2022
- § 6:63 The State and Local Government Cybersecurity Act of 2021

TABLE OF CONTENTS

- § 6:64 The Protecting American Intellectual Property Act of 2022
- § 6:65 The Protecting Americans' Data from Foreign Adversaries Act of 2024
- § 6:66 State computer security statutes
- § 6:67 State computer security regulations

CHAPTER 7. DATA PRIVACY STATUTES

I. POLITICAL CLIMATE MANDATES INCREASING PRIVACY REGULATION

- § 7:1 Concern about the lack of electronic security and privacy
- § 7:2 The FTC and privacy
- § 7:3 FTC enforcement actions
- § 7:4 FCC and privacy
- § 7:5 FCC enforcement
- § 7:6 Technological initiatives
- § 7:7 Transformation of business methods poses increased risk for privacy loss
- § 7:8 Protecting social security numbers
- § 7:9 State privacy laws
- § 7:10 California
- § 7:11 State security breach notification measures
- § 7:12 Enforcement actions and litigation
- § 7:13 Federal and state anti-spamming legislation
- § 7:14 Federal and state legislation—Unauthorized dissemination of personal information by e-commerce merchants
- § 7:15 —Electronic privacy at work

II. MAJOR LEGISLATIVE AREAS

- § 7:16 Generally
- § 7:17 Biometric Information Privacy

A. ONLINE PRIVACY

- § 7:18 Section 5 of the Federal Trade Commission Act
- § 7:19 The FTC's Internet-specific privacy proposals
- § 7:20 The FTC's Red Flag Rules
- § 7:21 Phishing and spyware

B. FINANCIAL PRIVACY

- § 7:22 Generally
- § 7:23 The Gramm-Leach-Bliley Act
- § 7:24 —Scope
- § 7:25 —Requirements

C. HEALTHCARE PRIVACY

- § 7:26 Generally
- § 7:27 Protected health information
- § 7:28 Parameters for the use and disclosure of health information
- § 7:29 Patients' rights under HIPAA
- § 7:30 Standards for full compliance
- § 7:31 Penalties
- § 7:32 The HITECH Act

D. CHILDREN'S PRIVACY

- § 7:33 Introduction

- § 7:34 Coverage
- § 7:35 Major provisions
- § 7:36 Notice requirements under COPPA
- § 7:37 Verifiable parental consent
- § 7:38 Exceptions to parental consent requirement
- § 7:39 Enforcement and compliance
- § 7:40 Safe harbor provision under COPPA

E. STUDENT'S PRIVACY

- § 7:41 In general
- § 7:42 The Family Educational Rights and Privacy Act
- § 7:43 State educational privacy

F. PRIVACY FOR PERSONAL INFORMATION IN PUBLIC RECORDS

- § 7:44 Introduction
- § 7:45 The Freedom of Information Act
- § 7:46 The Privacy Act of 1994
- § 7:47 Other legislation
- § 7:48 Conclusion

G. UNIFORM COMMERCIAL CODE ARTICLE 4A

- § 7:49 Generally
- § 7:50 A wholesale wire transfer
- § 7:51 Scope of Article 4A
- § 7:52 Security procedures

H. ELECTRONIC COMMUNICATIONS PRIVACY ACT OF 1986

- § 7:53 Introduction
- § 7:54 Major provisions of ECPA
- § 7:55 Exceptions under ECPA
- § 7:56 Penalties under ECPA

III. INTERACTION BETWEEN FEDERAL AND STATE STATUTES

- § 7:57 Generally
- § 7:58 Preemption
- § 7:59 State enforcement powers

IV. DATA PRIVACY LEGISLATION

- § 7:60 State spyware laws
- § 7:61 Privacy policies on governmental Web sites
- § 7:62 State data breach notification initiatives
- § 7:63 State Anti-Spam Laws
- § 7:64 State Comprehensive Consumer Privacy Laws
- § 7:65 Federal privacy legislation

CHAPTER 8. CIVIL LITIGATION: SECURITY

- § 8:1 Introduction
- § 8:2 Jurisdiction
- § 8:3 Determining Anonymous or Pseudonymous Parties for Personal Jurisdiction
- § 8:4 Standing

TABLE OF CONTENTS

§ 8:5	Computer Fraud and Abuse Act
§ 8:6	—Elements
§ 8:7	Civil litigation under the Computer Fraud and Abuse Act—Survey of caselaw—Access
§ 8:8	— —Transmission
§ 8:9	— —“Damages” and “loss”
§ 8:10	Civil litigation under the Computer Fraud and Abuse Act—Good faith security research
§ 8:11	Civil Litigation Under the Stored Communications Act
§ 8:12	Civil litigation under the Computer Fraud and Abuse Act—Record keeping
§ 8:13	Trespass to personal property/chattels
§ 8:14	—Elements
§ 8:15	—Damages
§ 8:16	—Defenses
§ 8:17	—Survey of caselaw
§ 8:18	Conversion
§ 8:19	—Elements
§ 8:20	—Damages
§ 8:21	—Survey of caselaw
§ 8:22	Fraud/misrepresentation
§ 8:23	—Elements
§ 8:24	—Damages
§ 8:25	—Defenses
§ 8:26	Breach of contract
§ 8:27	—Elements
§ 8:28	Breach of Implied Contract
§ 8:29	Breach of contract—Damages
§ 8:30	—Defenses
§ 8:31	Negligence
§ 8:32	—Elements
§ 8:33	—Damages
§ 8:34	—Defenses
§ 8:35	—Third-party liability
§ 8:36	—Internet service providers
§ 8:37	The FTC: Developing a framework for assessing the standard of care in negligence
§ 8:38	Computer malpractice
§ 8:39	Misappropriation of trade secrets
§ 8:40	—Elements
§ 8:41	—Damages
§ 8:42	—Defenses
§ 8:43	—Remedies
§ 8:44	Copyright infringement
§ 8:45	—Remedies
§ 8:46	Digital Millennium Copyright Act
§ 8:47	—Section 1201(a)(1)
§ 8:48	—Section 1201(a)(2)
§ 8:49	—Section 1201(b)
§ 8:50	—Exemptions
§ 8:51	—Remedies
§ 8:52	—Survey of caselaw
§ 8:53	— —Fair-use
§ 8:54	Challenges to spyware and adware
§ 8:55	United States Securities and Exchange Commission Enforcement
§ 8:56	Shareholder Derivative Lawsuits Spawning from Cyber Attacks

CHAPTER 9. PRIVACY LITIGATION

I. OVERVIEW

- § 9:1 Introduction
- § 9:2 Sources of liability for electronic privacy violations generally

II. PRIMARY SOURCES OF LIABILITY FOR ELECTRONIC PRIVACY VIOLATIONS

A. COMPUTER FRAUD AND ABUSE ACT

- § 9:3 Federal Computer Fraud and Abuse Act generally
- § 9:4 Elements of a CFAA claim
- § 9:5 Prohibited acts relevant to electronic privacy litigation
- § 9:6 —Intrusion into financial records [§ 1030(a)(2)(A)]
- § 9:7 —Hacking and other unauthorized access
- § 9:8 —Fraud [§ 1030(a)(4)]
- § 9:9 —Password Sharing [§ 1030(a)(4)]
- § 9:10 —Data Scraping[§§ 1030(a)(2), (4)]
- § 9:11 —Unauthorized infection [§ 1030(a)(5)(A)]
- § 9:12 —Intentional or reckless unauthorized access [§ 1030(a)(5)(B) to (C)]
- § 9:13 —Trafficking in access information [§ 1030(a)(6)(A)]
- § 9:14 —Threat intended to extort [§ 1030(a)(7)]
- § 9:15 Proper parties to CFAA claim—Including disloyal employees
- § 9:16 —Supreme Court resolves split in authority as to whether the CFAA applies to an employee who was granted authorized access to an employer's electronic information systems but breaches his duty of loyalty when using that access
- § 9:17 Proper court for CFAA claim
- § 9:18 Statute of limitations for CFAA claim
- § 9:19 Remedies available under CFAA
- § 9:20 Pleading requirements under the CFAA
- § 9:21 Secondary Liability under the CFAA

B. STORED COMMUNICATIONS ACT—TITLE II OF THE ECPA

- § 9:22 Federal Stored Communications Act generally
- § 9:23 Elements of Stored Communications Act claim
- § 9:24 Prohibited acts relevant to electronic privacy litigation—Unlawful access to a facility through which an electronic communications service is provided [18 U.S.C.A. § 2701]
- § 9:25 —Voluntary Disclosure of customer communications or records of stored communications [18 U.S.C.A. § 2702]
- § 9:26 Knowing or intentional state of mind required under Stored Communications Act
- § 9:27 Proper parties to Stored Communications Act claim
- § 9:28 Proper court for Stored Communications Act claim
- § 9:29 Statute of limitations for Stored Communications Act claim
- § 9:30 Remedies available under Stored Communications Act
- § 9:31 Defenses to Stored Communications Act claim—Exceptions to prohibitions of §§ 2701(a) and 2702(a)
- § 9:32 —Authorized government request
- § 9:33 —Good faith belief that conduct permitted by § 2511(3)
- § 9:34 Special electronic privacy issues under Stored Communications Act—Interception/monitoring of employee e-mail or e-mail generated in non-employment context
- § 9:35 —Subpoenas and Search Warrants as to emails, social-media postings and messages
- § 9:36 —Cookies, device identifiers and location data

§ 9:37 —Cross-border data requests and the CLOUD Act

C. FEDERAL WIRETAP ACT—TITLE I OF THE ECPA

- § 9:38 Federal Wiretap Act generally
- § 9:39 Elements of Federal Wiretap Act claim
- § 9:40 Prohibited acts relevant to electronic privacy litigation
- § 9:41 —Unlawful interception of electronic communications by any person [18 U.S.C.A. § 2511(1)(a)]
- § 9:42 —Unlawful disclosure or use of intercepted electronic communications by any person [18 U.S.C.A. § 2511(1)(a), (c) and (d)]
- § 9:43 —Unlawful disclosure of electronic communications in transit by electronic communication service provider [18 U.S.C.A. § 2511(3)]
- § 9:44 —Exceptions to violations [18 U.S.C.A. § 2511(2)]
- § 9:45 Proper parties to a Federal Wiretap Act claim
- § 9:46 Proper court for a Federal Wiretap Act claim
- § 9:47 Statute of limitations for a Federal Wiretap Act claim
- § 9:48 Remedies available under Federal Wiretap Act
- § 9:49 Defenses to Federal Wiretap Act claim—Authorized government request
- § 9:50 —Good faith belief that conduct permitted under § 2511(3)
- § 9:51 —Absence of Intent
- § 9:52 Special electronic privacy issues under Federal Wiretap Act
- § 9:53 State analogs to Federal Wiretap Act and Stored Communications Act—General
- § 9:54 —Employee e-mail and social media activity

D. CAN-SPAM ACT

- § 9:55 Federal CAN-SPAM Act generally
- § 9:56 Pre-emption of many state spam laws
- § 9:57 Who can sue under the CAN-SPAM Act
- § 9:58 Predicates for all CAN-SPAM Act violations
- § 9:59 Prohibited acts—“Protections for users of commercial electronic mail”; “Requirements for transmission of messages” [15 U.S.C.A. § 7704(a)(1) to (5)]
- § 9:60 —15 U.S.C.A. § 7704(a) claims; “Pattern or practice” requirement
- § 9:61 —“Aggravated violations” [15 U.S.C.A. § 7704(b)]
- § 9:62 —15 U.S.C.A. § 7704(d)(1) “violation” (unlabeled “sexually oriented material”); criminal offenses under 18 U.S.C.A. § 1037; and co-extensive crimes based on other acts
- § 9:63 —FTC enforcement of 15 U.S.C.A. § 7705(a) violation (“false or misleading transmission information”)
- § 9:64 Exceptions/defenses—Transactional or relationship messages
- § 9:65 —Prior affirmative consent
- § 9:66 —Subsequent affirmative consent
- § 9:67 —Fraudulent content to be pled with particularity
- § 9:68 Proper Parties to a CAN-SPAM Act claim—Potential Private Plaintiffs—Restricted Universe
- § 9:69 —Potential Defendants—Including Secondary Liability
- § 9:70 Proper court for a CAN-SPAM Act civil claim
- § 9:71 Available remedies for a CAN-SPAM civil claim
- § 9:72 State analogs to the CAN-SPAM Act

E. TELEPHONE CONSUMER PROTECTION ACT (“TCPA”)

- § 9:73 Generally
- § 9:74 Constitutionality
- § 9:75 Prohibited Acts—Calls Made “using any automatic telephone dialing system or an artificial or prerecorded voice” to cellular telephones and certain other protected telephone lines [47 U.S.C. § 227(b)(1)(A)]

- § 9:76 —Calls made to residential telephone lines using an artificial or prerecorded voice [47 U.S.C. § 227(b)(1)(B)]
- § 9:77 —Unsolicited Fax Advertisements [47 U.S.C. § 227(b)(1)(C)]
- § 9:78 Exceptions/Defenses—Prior Express Consent
- § 9:79 Private Right of Action/Standing/Damages
- § 9:80 Proper Forum For TCPA Lawsuits/Subject Matter Jurisdiction
- § 9:81 Potential Defendants
- § 9:82 Class Actions
- § 9:83 Preemption

F. CHILDREN’S ONLINE PRIVACY PROTECTION ACT—15 U.S.C. §§ 6501–6508

- § 9:84 Children’s Online Privacy Protection Act Generally
- § 9:85 Elements of COPPA Claim
- § 9:86 Prohibited Acts—In general
- § 9:87 —Failure to Obtain Parental Consent Prior to Collection or Distribution of Children’s Information
- § 9:88 —Failure to Use Reasonable Procedures to Protect Information
- § 9:89 Proper Parties
- § 9:90 Proper Court
- § 9:91 Remedies under COPPA

G. VIDEO PRIVACY PROTECTION ACT—18 U.S.C. §§ 2710 *ET SEQ.*

- § 9:92 Video Privacy Protection Act generally
- § 9:93 Elements of VPPA Claim
- § 9:94 Prohibited Acts—Disclosure of personally identifiable information by a video tape service provider [18 U.S.C.A. § 2710(b)(2)]
- § 9:95 —Improperly obtained personally identifiable information rendered inadmissible as evidence in any U.S. judicial, regulatory, legislative or administrative proceeding [18 U.S.C.A. § 2710(d)]
- § 9:96 —Failure to timely destroy personally identifiable information [18 U.S.C.A. § 2710(e)]
- § 9:97 Proper Parties [18 U.S.C.A. § 2710(c)(1)]
- § 9:98 Proper Court [18 U.S.C.A. § 2710(c)(1)]
- § 9:99 Statute of Limitations under the VPPA [18 U.S.C.A. § 2710(c)(3)]
- § 9:100 Remedies under the VPPA [18 U.S.C.A. § 2710(c)(2)]
- § 9:101 Defenses—Standing—No Injury-in-Fact
- § 9:102 —No Disclosure for Intra-Company Transfer
- § 9:103 —Disclosure not made Knowingly or Willingly
- § 9:104 —Use in ordinary course of business—Request processing
- § 9:105 —Retention for ongoing marketing purposes

H. SECURITY-BREACH NOTIFICATION STATUTES AND RELATED SOURCES

- § 9:106 State Notice-Of-Breach Laws
- § 9:107 Other Federal and State Laws Regarding Data Breaches
- § 9:108 The Duty of Care in Data Breach Cases
- § 9:109 Standing in Data Breach Cases
- § 9:110 Causation in Data Breach Cases

I. BREACH OF CONTRACT

- § 9:111 Breach of contract generally
- § 9:112 Elements of breach-of-contract claim
- § 9:113 Defenses to breach-of-contract claim
- § 9:114 Proper parties to breach-of-contract claim

TABLE OF CONTENTS

- § 9:115 Proper court for breach-of-contract claim
- § 9:116 Statutes of limitations for breach-of-contract claim
- § 9:117 Remedies for breach of contract
- § 9:118 Special electronic privacy issues: Enforceability of privacy policies or terms-of-use statements
- § 9:119 Special electronic privacy issues: enforceability of privacy policies or terms-of-use statements—Mutual assent
- § 9:120 —Consideration
- § 9:121 —Liability for prohibited transfer of customer data
- § 9:122 —Employer policies on employee e-mail, computer and internet use

J. INVASION OF PRIVACY

- § 9:123 Invasion of privacy generally
- § 9:124 Constitutional claims for invasion of privacy generally
- § 9:125 Elements of a constitutional invasion-of-privacy claim
- § 9:126 Common law invasion of privacy generally
- § 9:127 Elements of claim for intrusion into plaintiff's solitude or private affairs
- § 9:128 Elements of claim for public disclosure of private facts
- § 9:129 Defenses to invasion-of-privacy claims
- § 9:130 Proper parties to invasion-of-privacy claim
- § 9:131 Proper court for invasion-of-privacy claim
- § 9:132 Statute of limitations for invasion-of-privacy claim
- § 9:133 Remedies available for invasion of privacy
- § 9:134 Special electronic privacy issues: Employer monitoring of employee e-mails, internet usage and social media activity

K. STATES' DATA PROTECTION STATUTORY CLAIMS

- § 9:135 California Consumer Privacy Act (CCPA) of 2018 (eff. 1/1/20)
- § 9:136 Other states' privacy legislation

III. OTHER POTENTIAL SOURCES OF PRIVACY CLAIMS

A. STATE UNFAIR COMPETITION STATUTES/"LITTLE FTC" ACTS

- § 9:137 State unfair competition statutes/"Little FTC" acts generally
- § 9:138 Defenses to state unfair competition statutes
- § 9:139 Remedies available under state unfair competition statutes

B. FAIR CREDIT REPORTING ACT

- § 9:140 Fair Credit Reporting Act generally
- § 9:141 Elements of FCRA claim
- § 9:142 Prohibited acts relevant to electronic privacy—Failure to give notice and obtain consent to procure consumer report [15 U.S.C.A. § 1681b(b)(2)]
- § 9:143 —Failure to notify applicant of adverse employment decision based on consumer report/failure to provide requested copy of report [15 U.S.C.A. § 1681b]
- § 9:144 —Potential liability for requesting report on opposing party [§§ 1681a(d), 1681b, 1681b(3)(E)]
- § 9:145 Proper parties to FCRA claim
- § 9:146 Proper court for FCRA claim; possible preemption of state law claims
- § 9:147 Statute of limitations for FCRA claim
- § 9:148 Remedies available under FCRA—Consumer remedies for willful noncompliance [15 U.S.C.A. § 1681n]
- § 9:149 —Consumer remedies for negligent noncompliance

- § 9:150 —Attorney’s fees for bad faith litigation tactics
- § 9:151 Special electronic privacy issues—Broadening definition of “consumer report”
- § 9:152 —FCRA Issues in Data Breaches
- § 9:153 FACTA Civil Claims—Failure to truncate credit card and/or debit card numbers
- § 9:154 “Baby FACTAs”—Analogous state law issues, such as retailers’ collection of zip codes and e-mail addresses
- § 9:155 FACTA Civil Claims—Lack of compliance with FTC Disposal Rule as to consumer credit reports and/or information derived from consumer credit reports

C. 21ST-CENTURY-TECHNOLOGY-RELATED THEORIES

- § 9:156 Mobile-apps-related theories
- § 9:157 Social-media-related theories

IV. KEY GENERAL DEFENSES TO ELECTRONIC PRIVACY CLAIMS

A. COMMON LAW DEFENSES

- § 9:158 Consent/waiver/no expectation of privacy

B. STATUTORY DEFENSE IN FEDERAL AND STATE SUITS—IMMUNITY UNDER COMMUNICATIONS DECENTY ACT (CDA)

- § 9:159 Defense under Communications Decency Act of 1996
- § 9:160 —Defending party must be provider or user of interactive computer service
- § 9:161 —Defending party must not be information content provider of information giving rise to cause of action
- § 9:162 —Publisher liability for third-party content
- § 9:163 —Distributor liability for third-party content
- § 9:164 —Limits of defense

C. CONSTITUTIONAL DEFENSES

- § 9:165 Article III standing
- § 9:166 First Amendment and state free speech protections

D. GOVERNMENT-DEFENDANT DEFENSES

- § 9:167 NSA Anti-Terrorism—The state secrets privilege and “sovereign immunity;” defenses

V. PRIVACY LITIGATION PROCEDURAL NUANCES

- § 9:168 Privacy litigation procedural nuances generally
- § 9:169 Subject matter jurisdiction and preemption
- § 9:170 Personal Jurisdiction
- § 9:171 Standing
- § 9:172 Transfer motions
- § 9:173 Civil enforcement proceedings brought by, and settlements with, federal and state government agencies, including the FTC
- § 9:174 Motions to dismiss
- § 9:175 Motions for summary judgment
- § 9:176 Motions for preliminary injunction
- § 9:177 Discovery generally
- § 9:178 Identified plaintiff seeking disclosure of identity of anonymous defendant—Various contexts
- § 9:179 —Peer-to-Peer (P2P) file-sharing context
- § 9:180 Identified plaintiff seeking disclosure of identity of anonymous non-party witness(es)
- § 9:181 Anonymous plaintiff suing and seeking disclosure of anonymous defendant or seeking to avoid disclosure of own identity

§ 9:182 Class actions: Certification, standing, waivers, and settlement

CHAPTER 10. CORPORATE SECURITY AND PRIVACY DUTIES, POLICIES AND FORMS

I. INTERNAL SECURITY AND PRIVACY

- § 10:1 Internal security and privacy generally
- § 10:2 Duty of confidentiality for internal corporate information and trade secrets
- § 10:3 Duty to shareholders
- § 10:4 —SEC disclosures
- § 10:5 — —Management’s discussion and analysis
- § 10:6 — —Risk factors
- § 10:7 — —Description of business
- § 10:8 Fiduciary duty of due care
- § 10:9 Duty to customers to enable unhindered use of system
- § 10:10 —Security from viruses, Trojan horses, and other malware
- § 10:11 Duties owed by ISPs, OSPs, and ASPs
- § 10:12 Data risk and cloud computing
- § 10:13 Corporate policies—Forms

II. CONFIDENTIAL AND PRIVATE THIRD-PARTY INFORMATION

- § 10:14 Responsibility for data security—Contractual issues
- § 10:15 Fiduciary and other common-law obligations to protect information belonging to others
- § 10:16 Confidentiality agreements and issues therein
- § 10:17 Encrypted channels for maintenance and transfer of customer information
- § 10:18 —Internally
- § 10:19 Maintenance and transfer of customer information—By third-party commerce partners
- § 10:20 Privacy policy—In general
- § 10:21 —Notice/awareness
- § 10:22 Privacy policy regarding internal use of third-party information—Choice/consent:
consumers’ ability to opt out
- § 10:23 —Access/participation: consumers’ ability to access/change their information
- § 10:24 —Integrity/security: information on how data will be kept confidential
- § 10:25 —Enforcement: explanation to consumers of internal enforcement policies
- § 10:26 —Sending and receipt of unsolicited email
- § 10:27 —Liability for disclosing private information

III. DAMAGE CAUSED TO THIRD-PARTY SYSTEMS

- § 10:28 Damage caused to third-party systems generally
- § 10:29 Security from spreading viruses, Trojan horses, and other malware
- § 10:30 Security from employee/contractor intentional abuse of third-party systems
- § 10:31 Third-party policies and forms generally
- § 10:32 Click-wrap agreements—Website visitors/customers
- § 10:33 Information-sharing agreements
- § 10:34 Online/offline privacy and security policy: checkbox short form
- § 10:35 Sample privacy policy: form
- § 10:36 Disclosure of effect of sale of business: short form version 1
- § 10:37 Disclosure of effect of sale of business: short form version 2
- § 10:38 Choice/opt-out disclosure: short form
- § 10:39 Security disclosure: Sample
- § 10:40 Hosting agreement: security provisions

- § 10:41 Notice of security breach: form
- § 10:42 Notice of security breach: short form
- § 10:43 HITECH sample data breach notification letter to individual
- § 10:44 HITECH sample data breach notification to the media
- § 10:45 Notification for Public Companies
- § 10:46 Miscellaneous federal notification laws
- § 10:47 Computer use policy: long form for MIS department personnel
- § 10:48 Computer use policy: short form version 1
- § 10:49 Computer use policy: short form version 2
- § 10:50 IT policy acknowledgment: short form for all personnel
- § 10:51 Blogging and Social Media Policy

IV. DEVELOPING BEST PRACTICES AND LEGAL INFORMATION SECURITY STRATEGY

- § 10:52 Information security policies
- § 10:53 Creation of legal information security strategy
- § 10:54 —Legal threat modeling
- § 10:55 — —Data-intensive business
- § 10:56 — —Extent of internal information sharing; policy of least information privilege
- § 10:57 — —Extent of external information sharing and external legal dependencies
- § 10:58 — —History of strict data handling norms and good information security practices
- § 10:59 — —Reactive vs. proactive legal culture
- § 10:60 —Selling the legal benefits of good security practices to businesspeople
- § 10:61 —Drafting a corporate data security policy document
- § 10:62 Adherence and evolution
- § 10:63 —Success of incident response to most recent security incident
- § 10:64 —Success of last audit and efficacy of current data management systems
- § 10:65 —Impact of legal developments related to data security and privacy
- § 10:66 —Likely future uses for collected data and adequacy of current privacy policies
- § 10:67 —Adequacy of existing contracts regarding data security and potential for liability
- § 10:68 Legal information security threat modeling checklist

CHAPTER 11. EUROPEAN UNION DATA PROTECTION

I. OVERVIEW

- § 11:1 European Union Data Protection Directive 95/46/EC and the General Data Protection Regulation
- § 11:2 General Data Protection Regulation 2016/679
- § 11:3 GDPR—Scope and main provisions
- § 11:4 —Remedies, liability and sanctions
- § 11:5 —Transfer of personal data outside EU
- § 11:6 — —Standard contractual clauses
- § 11:7 —Transfers of Personal Data to the United States
- § 11:8 Rules on data protection for email marketing
- § 11:9 The Data Retention Directive 2006/24/EC: Rules on retention of communications data

II. WORLD TREATIES AND COOPERATIVE INITIATIVES

- § 11:10 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data
- § 11:11 —Privacy principles
- § 11:12 Council of Europe Convention 108
- § 11:13 —Data protection guidelines
- § 11:14 UN Guidelines for the Regulation of Computerized Personal Data Files

III. INFORMATION SECURITY ISSUES

- § 11:15 OECD guidelines for the security of information systems and networks: toward a culture of security
- § 11:16 OECD recommendation on Digital Security Risk Management for Economic and Social Prosperity-Principles
- § 11:17 Common criteria for information technology security evaluation
- § 11:18 —Overview
- § 11:19 —Structure
- § 11:20 —Key constructs
- § 11:21 —General security context
- § 11:22 Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security
- § 11:23 —Substantive issues
- § 11:24 —Dispute resolution
- § 11:25 European Union regulatory instruments for network and information security
- § 11:26 —Network and information security
- § 11:27 —Attacks against information systems
- § 11:28 Council of Europe Convention on Cyber-Crime
- § 11:29 —Terms
- § 11:30 —Substantive criminal law
- § 11:31 — —Criminal offenses
- § 11:32 — —Ancillary liability and sanctions
- § 11:33 —Procedural law issues
- § 11:34 —International cooperation
- § 11:35 —Other provisions
- § 11:36 Major Decisions in EU Member States relating to the GDPR (2018–2021)
- § 11:37 Major decisions in EU member states relating to the EU data protection directive 95/46/EC (1998–2012)

CHAPTER 12. HEALTH CARE PRIVACY AND THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996

- § 12:1 Introduction
- § 12:2 HIPAA privacy regulations generally
- § 12:3 Entities covered under HIPAA privacy regulations
- § 12:4 —Health plans
- § 12:5 —Health care clearinghouses
- § 12:6 —Covered health care providers
- § 12:7 Information covered under HIPAA privacy regulations
- § 12:8 —De-identified information
- § 12:9 — —Limited data set
- § 12:10 Uses and disclosures of protected health information under HIPAA privacy regulations
- § 12:11 —Treatment
- § 12:12 —Payment
- § 12:13 —Health care operations
- § 12:14 — —Uses and disclosures for treatment, payment and health care operations of a third party
- § 12:15 —Required by law
- § 12:16 —Other exceptions to authorization requirement
- § 12:17 — —Public health activities
- § 12:18 — —Abuse, neglect or domestic violence
- § 12:19 — —Health oversight activities
- § 12:20 — —Judicial and administrative proceedings
- § 12:21 — —Law enforcement purposes

- § 12:22 — —Decedents
- § 12:23 — —Cadaveric organ, eye or tissue donation
- § 12:24 — —Research
- § 12:25 — —Threat to health or safety
- § 12:26 — —Specialized government functions
- § 12:27 — —Workers' compensation
- § 12:28 —Opportunity to agree or object
- § 12:29 —Incidental uses and disclosures
- § 12:30 —Authorization requirement
- § 12:31 Individual rights under HIPAA privacy regulations
- § 12:32 —Right to access and copy information in designated record set
- § 12:33 —Right to request amendment or correction
- § 12:34 —Right to accounting of disclosures
- § 12:35 —Right to request restriction
- § 12:36 —Right to specify how confidential information is communicated
- § 12:37 Notice requirement under HIPAA privacy regulations (notice of privacy practices)
- § 12:38 Notice requirement under HIPAA privacy regulations—Required elements
- § 12:39 —Revisions to notice of privacy practices
- § 12:40 —Dissemination of notice and written acknowledgment of receipt
- § 12:41 Minimum necessary standard under HIPAA privacy regulations
- § 12:42 Administrative obligations under HIPAA privacy regulations
- § 12:43 —Privacy officer
- § 12:44 —Training
- § 12:45 —Security
- § 12:46 — —Electronic protected health information
- § 12:47 — —Flexible and scalable
- § 12:48 — —Security requirements
- § 12:49 — — —Administrative safeguards
- § 12:50 — — —Physical safeguards
- § 12:51 — — —Technical safeguards
- § 12:52 —Complaints
- § 12:53 —Mitigation
- § 12:54 —Breach notification analysis under the HITECH Act
- § 12:55 —Breach notification obligations under the HITECH Act
- § 12:56 —Sanctions
- § 12:57 —Policies and procedures
- § 12:58 Business associates under HIPAA privacy regulations
- § 12:59 Organizational rules under HIPAA privacy regulations: Hybrid entities
- § 12:60 Organizational rules under HIPAA privacy regulations: Affiliated covered entities
- § 12:61 Organizational rules under HIPAA privacy regulations: Organized health care arrangements
- § 12:62 Special requirements for group health plans under HIPAA privacy regulations
- § 12:63 Research under the HIPAA privacy regulations
- § 12:64 Marketing under HIPAA privacy regulations
- § 12:65 Fundraising under HIPAA privacy regulations
- § 12:66 Enforcement of HIPAA privacy regulations
- § 12:67 State privacy laws
- § 12:68 —Regulation by user
- § 12:69 —Privilege
- § 12:70 —Condition-specific confidentiality laws
- § 12:71 —Comprehensive state privacy laws
- § 12:72 —Breach notification under state privacy laws
- § 12:73 State law claims based on HIPAA violations

TABLE OF CONTENTS

- § 12:74 Other federal privacy laws
- § 12:75 —Genetic Information Nondiscrimination Act
- § 12:76 —Gramm-Leach-Bliley Act
- § 12:77 —Substance abuse regulations
- § 12:78 —Privacy Act of 1974
- § 12:79 Federal Agency Enforcement
- § 12:80 Conclusion
- § 12:81 Group health plan obligations under HIPAA privacy regulations
- § 12:82 Significant definitions under HIPAA privacy regulations
- § 12:83 Administrative safeguards
- § 12:84 Physical safeguards
- § 12:85 Technical safeguards

CHAPTER 13. BANKING, FINANCIAL, AND INSURANCE INDUSTRIES

- § 13:1 Introduction
- § 13:2 Gramm-Leach-Bliley Act
- § 13:3 —Financial institutions
- § 13:4 —Nonpublic personal information
- § 13:5 —Affiliates
- § 13:6 —Consumers
- § 13:7 —Customers
- § 13:8 —Affiliated financial institutions
- § 13:9 —Contents of privacy policy notice
- § 13:10 —Method of delivery of privacy policy notice
- § 13:11 —Timing of initial privacy policy notice
- § 13:12 —Annual privacy policy notices
- § 13:13 —Exceptions to notice and opt-out
- § 13:14 — —Service processors
- § 13:15 — —Joint agreements
- § 13:16 — —Necessary to effect, administer, or enforce a transaction
- § 13:17 — —Consent of consumer
- § 13:18 — —Special relationships
- § 13:19 — —Other exceptions
- § 13:20 — —Reuse and redisclosure
- § 13:21 —Disclosure of account numbers
- § 13:22 —Enforcement
- § 13:23 Fair Credit Reporting Act
- § 13:24 —Scope
- § 13:25 —Investigative consumer reports
- § 13:26 —Business credit transactions
- § 13:27 —Consumer reporting agency
- § 13:28 —Prescreening
- § 13:29 —Obsolete information
- § 13:30 —Limits on investigative consumer reports
- § 13:31 —Medical information
- § 13:32 —Assuring that consumer reports are provided for permissible purposes
- § 13:33 —Accuracy
- § 13:34 —Disclosures to consumers
- § 13:35 —Resolution of credit reporting disputes
- § 13:36 —Nature of adverse action
- § 13:37 —Adverse action based on third-party information
- § 13:38 —The Fair and Accurate Credit Transactions Act of 2003

- § 13:39 —Affiliate sharing
- § 13:40 —Risk-based pricing
- § 13:41 —Identity theft prevention
- § 13:42 —Civil liability for willful noncompliance
- § 13:43 State financial privacy laws
- § 13:44 —Constitutional guarantees of privacy
- § 13:45 —Statutory approaches to financial privacy
- § 13:46 —Common law rights to financial privacy
- § 13:47 Electronic Funds Transfer Act: Initial disclosures
- § 13:48 Health Insurance Portability and Accountability Act: Applicability to financial institutions
- § 13:49 Children’s Online Privacy Protection Act: Applicability to financial institutions
- § 13:50 Other federal privacy statutes: Electronic Communications Privacy Act
- § 13:51 Regulatory guidelines: Agency guidelines on safety and soundness
- § 13:52 Trends in cybersecurity and data protection litigation
- § 13:53 The future of breach notification laws: federal legislation
- § 13:54 The future of data security legislation: state legislation

CHAPTER 14. PERSONAL DATA PROTECTION LAWS AROUND THE WORLD

- § 14:1 Introduction
- § 14:2 Common themes among personal data protection laws
- § 14:3 Personal data protection laws around the world

Table of Laws and Rules

Table of Cases

Index