

# U.S. Private-sector Privacy Certification

## Outline of the Body of Knowledge for the Certified Information Privacy Professional/United States (CIPP/US™)



### I. Introduction to the U.S. Privacy Environment

- A. Structure of U.S. Law
  - a. Branches of government
  - b. Sources of law
    - i. Constitutions
    - ii. Legislation
    - iii. Regulations and rules
    - iv. Case law
    - v. Common law
    - vi. Contract law
  - c. Legal definitions
    - i. Jurisdiction
    - ii. Person
    - iii. Preemption
    - iv. Private right of action
  - d. Regulatory authorities
    - i. Federal Trade Commission (FTC)
    - ii. Federal Communications Commission (FCC)
    - iii. Department of Commerce (DoC)
    - iv. Department of Health and Human Services (HHS)
    - v. Banking regulators
      - 1. Federal Reserve Board
      - 2. Comptroller of the Currency
    - vi. State attorneys general
    - vii. Self-regulatory programs and trust marks
  - e. Understanding laws
    - i. Scope and application
    - ii. Analyzing a law
    - iii. Determining jurisdiction
    - iv. Preemption

- B. Enforcement of U.S. Privacy and Security Laws
  - a. Criminal versus civil liability
  - b. General theories of legal liability
    - i. Contract
    - ii. Tort
    - iii. Civil enforcement
  - c. Negligence
  - d. Unfair and deceptive trade practices (UDTP)
  - e. Federal enforcement actions
  - f. State enforcement (Attorneys General (AGs), California Privacy Protection Agency (CPPA))
  - g. Cross-border enforcement issues (Global Privacy Enforcement Network (GPEN))
  - h. Self-regulatory enforcement (PCI, Trust Marks)
- C. Information Management from a U.S. Perspective
  - a. Data sharing and transfers
    - i. Data inventory
    - ii. Data classification
    - iii. Data flow mapping
  - b. Privacy program development
  - c. Managing User Preferences
  - d. Incident response programs
    - i. Cyber threats (e.g., ransomware)
  - e. Workforce Training
  - f. Accountability
  - g. Data and records retention and disposal (FACTA)
  - h. Online Privacy
  - i. Privacy notices
  - j. Vendor management
    - i. Vendor incidents
    - ii. Cloud issues
    - iii. Third-party data sharing
  - k. International data transfers
    - i. U.S. Safe Harbor, Privacy Shield, and the EU-U.S. Data Privacy Framework
    - ii. Binding Corporate Rules (BCRs)
    - iii. Standard Contractual Clauses (SCCs)
    - iv. Other approved transfer mechanisms
    - v. Schrems decisions, implications of
  - l. Other key considerations for U.S.-based global multinational companies
    - i. GDPR requirements
    - ii. APEC privacy framework
  - m. Resolving multinational compliance conflicts
    - i. EU data protection versus e-discovery

## II. Limits on Private-sector Collection and Use of Data

- A. Cross-sector FTC Privacy Protection
  - a. The Federal Trade Commission Act
  - b. FTC Privacy Enforcement Actions
  - c. FTC Security Enforcement Actions
  - d. The Children's Online Privacy Protection Act of 1998 (COPPA)
  - e. Future of federal enforcement (Data brokers, Big Data, IoT, AI, unregulated data)

B. Healthcare/Medical

- a. The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
  - i. HIPAA privacy rule
  - ii. HIPAA security rule
  - iii. Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates
- b. Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009
- c. The 21<sup>st</sup> Century Cures Act of 2016
- d. Confidentiality of Substance Use Disorder Patient Records Rule
  - i. 42 CFR Part 2

C. Financial

- a. The Fair Credit Reporting Act of 1970 (FCRA)
- b. The Fair and Accurate Credit Transactions Act of 2003 (FACTA)
- c. The Financial Services Modernization Act of 1999 ("Gramm-Leach-Bliley" or GLBA)
  - i. GLBA privacy rule
  - ii. GLBA safeguards rule
  - iii. Exemptions under state laws
- d. Red Flags Rule
- e. Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010
- f. Consumer Financial Protection Bureau
- g. Online Banking

D. Education

- a. Family Educational Rights and Privacy Act of 1974 (FERPA)
- b. Education technology

E. Telecommunications and Marketing

- a. Telemarketing sales rule (TSR) and the Telephone Consumer Protection Act of 1991 (TCPA)
  - i. The Do-Not-Call registry (DNC)
- b. Combating the Assault of Non-solicited Pornography and Marketing Act of 2003 (CAN-SPAM)
- c. The Junk Fax Prevention Act of 2005 (JFPA)
- d. The Wireless Domain Registry
- e. Telecommunications Act of 1996 and Customer Proprietary Network Information
- f. Cable Communications Policy Act of 1984
- g. Video Privacy Protection Act of 1988 (VPPA)
  - i. Video Privacy Protection Act Amendments Act of 2012 (H.R. 6671)
- h. Driver's Privacy Protection Act (DPPA)
- i. Digital advertising
- j. Data Ethics

### III. Government and Court Access to Private-sector Information

A. Law Enforcement and Privacy

- a. Access to financial data
  - i. Right to Financial Privacy Act of 1978
  - ii. Bank Secrecy Act of 1970 (BSA)
- b. Access to communications
  - i. Wiretaps
  - ii. Electronic Communications Privacy Act (ECPA)
    - 1. E-mails
    - 2. Stored records

- 3. Pen registers
- c. The Communications Assistance to Law Enforcement Act (CALEA)
- B. National Security and Privacy
  - a. Foreign Intelligence Surveillance Act of 1978 (FISA)
    - i. Wiretaps
    - ii. E-mails and stored records
    - iii. National security letters
    - iv. Amendments Act: Section 702 (2008)
  - b. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA-Patriot Act)
  - c. The USA Freedom Act of 2015
  - d. The Cybersecurity Information Sharing Act of 2015 (CISA)
- C. Civil Litigation and Privacy
  - a. Compelled disclosure of media information
    - i. Privacy Protection Act of 1980
  - b. Electronic discovery

#### iv. Workplace Privacy

- A. Introduction to Workplace Privacy
  - a. Workplace privacy concepts
    - i. Human resources management
  - b. U.S. agencies regulating workplace privacy issues
    - i. Federal Trade Commission (FTC)
    - ii. Department of Labor
    - iii. Equal Employment Opportunity Commission (EEOC)
    - iv. National Labor Relations Board (NLRB)
    - v. Occupational Safety and Health Act (OSHA)
    - vi. Securities and Exchange Commission (SEC)
  - c. U.S. Anti-discrimination laws
    - i. Civil Rights Act of 1964
    - ii. Americans with Disabilities Act (ADA)
    - iii. Genetic Information Nondiscrimination Act (GINA)
- B. Privacy before, during and after employment
  - a. Automated employment decision tools and potential for bias
  - b. Employee background screening
    - i. Requirements under FCRA
    - ii. Methods
      - 1. Personality and psychological evaluations
      - 2. Polygraph testing
      - 3. Drug and alcohol testing
      - 4. Social media
  - c. Employee monitoring
    - i. Technologies
      - 1. Computer usage (including social media)
      - 2. Biometrics
      - 3. Location-based services (LBS)
      - 4. Wellness Programs
      - 5. Mobile computing

- 6. E-mail and postal mail
- 7. Photography
- 8. Telephony
- 9. Video
- ii. Requirements under the Electronic Communications Privacy Act of 1986 (ECPA)
- iii. Unionized worker issues concerning monitoring in the U.S. workplace
- d. Investigation of employee misconduct
  - i. Data handling in misconduct investigations
  - ii. Use of third parties in investigations
  - iii. Documenting performance problems
  - iv. Balancing rights of multiple individuals in a single situation
- e. Termination of the employment relationship
  - i. Transition management
  - ii. Records retention
  - iii. References

## V. State Privacy Laws

- A. Federal vs. state authority
  - a. California Privacy Protection Agency (CPPA)
- B. Data Privacy and Security Laws
  - a. SSN
  - b. Data destruction
  - c. Security procedures
  - d. Cookie and online tracking regulations
  - e. Facial recognition use restrictions
  - f. Biometric information privacy regulations
    - i. Illinois Biometric Information Privacy Act (BIPA) (2008)
  - g. Recent developments
    - i. California Consumer Privacy Act (CCPA) (2018)
    - ii. California Privacy Rights Act (CPRA) (2020)
    - iii. Virginia Consumer Data Protection Act (VCDPA) (2021)
    - iv. Colorado Privacy Act (CPA) (2021)
    - v. Nevada Privacy Law & Amendment (SB260) (2019/2021)
    - vi. Connecticut Data Privacy Act (CTDPA) (2022)
    - vii. Utah Consumer Privacy Act (UCPA) (2022)
    - viii. California Age-Appropriate Design Code Act (A.B. 2273) (2022)
    - ix. Other significant state acts and laws
- C. Data Breach Notification Laws
  - a. Elements of state data breach notification laws
    - i. Definitions of relevant terms (personal information, security breach)
    - ii. Conditions for notification (who, when, how)
    - iii. Subject rights (credit monitoring, private right of action)
  - b. Key differences among states today
  - c. Recent developments
    - i. Illinois HB 1260
    - ii. Massachusetts HB 4806
    - iii. Other significant state amendments