Privacy Technology Certification

Outline of the Body of Knowledge (BOK) for the Certified Information Privacy Technologist (CIPT)

I. Foundational Principles

A. Privacy Risk Models and Frameworks
   a. Nissenbaum’s Contextual Integrity
   b. Calo’s Harms Dimensions
   c. Legal Compliance
   d. FIPPs
   e. NIST/NICE frameworks
   f. FAIR (Factors Analysis in Information Risk)

B. Privacy by Design Foundational Principles
   a. Full Life Cycle Protection
   b. Embedded into Design
   c. Full Functionality
   d. Visibility and Transparency
   e. Proactive not Reactive
   f. Privacy by Default
   g. Respect for Users

C. Value Sensitive Design
   a. How Design Affects Users
   b. 14 Methods
   c. Strategies for Skillful practice

D. The Data Life Cycle
   a. Collection
   b. Use
   c. Disclosure
   d. Retention
   e. Destruction

II. The Role of IT in Privacy

A. Fundamentals of privacy-related IT
   a. Organization privacy notice
b. Organization internal privacy policies

c. Organization security policies, including data classification policies and schema, data retention and data deletion

d. Other commitments made by the organization (contracts, agreements)

e. Common IT Frameworks (COBIT, ITIL, etc.)

f. Data inventories
g. Enterprise architecture and data flows, including cross-border transfers

h. Privacy impact assessments (PIAs)

B. Information Security

a. Transactions which collect confidential data for use in later processing activities

b. Breach/disclosure incident investigations and responses—security and privacy perspectives

c. Security and privacy in the systems development life cycle (SDLC) process

d. Privacy and security regulations with specific IT requirements

C. The privacy responsibilities of the IT professional

a. Providing feedback on policies

b. Providing feedback on contractual and regulatory requirements

c. Understanding how Information Technology and Information Security support information governance in an organization

III. Privacy Threats and Violations

A. During Data Collection

a. Asking people to reveal personal information

b. Surveillance

B. During Use

a. Insecurity

b. Identification

c. Aggregation

d. Secondary Use

e. Exclusion

C. During Dissemination

a. Disclosure

b. Distortion

c. Exposure

d. Breach of Confidentiality

e. Increased accessibility

f. Blackmail

g. Appropriation

D. Intrusion, Decisional Interference and Self Representation

a. Behavioral advertising

b. Cyberbullying

c. Social engineering

E. Software Security
IV. Technical Measures and Privacy Enhancing Technologies

A. Data Oriented Strategies

a. Separate
   i. Distribute
   ii. Isolate

b. Minimize
   i. Exclude
   ii. Select
   iii. Strip
   iv. Destroy

c. Abstract
   i. Group
   ii. Summarize
   iii. Perturb

d. Hide
   i. Restrict
   ii. Mix
   iii. Obfuscate
   iv. Dissociate

B. Techniques

a. Aggregation
   i. Frequency and magnitude data
   ii. Noise addition through differential privacy
   iii. Differential identifiability

b. De-identification
   i. Anonymize
   ii. Pseudonymize
   iii. Labels that point to individuals
   iv. Strong and weak identifiers
   v. Degrees of Identifiability
   vi. k-anonymity, l-diversity, t-closeness
   vii. Tokenization

c. Encryption
   i. Algorithms and Keys
   ii. Symmetric and Asymmetric
   iii. Crypto design and implementation considerations
   iv. Application or field encryption
   v. Quantum encryption
   vi. Public Key Infrastructure
   vii. Homomorphic
   viii. Polymorphic
   ix. Mix networks
   x. Secure multi-party computation
xi. Private information retrieval
d. Identity and access management
   i. Limitations of access management as a privacy tool
   ii. Principle of least-privilege required
   iii. Role-based access control (RBAC)
   iv. User-based access controls
   v. Context of authority
   vi. Cross-enterprise authentication and authorization models
   vii. Federated identity
   viii. Bring your own device (BYOD) concerns

e. Authentication
   i. Single/multi factor authentication
   ii. Something you know (usernames, passwords)
   iii. Something you are (biometrics, facial recognition, location)
   iv. Something you have (tokens, keys)

C. Process Oriented Strategies
   a. Informing the Individual
      i. Supply
      ii. Notify
      iii. Explain
   b. User Control
      i. Consent
      ii. Choose
      iii. Update
      iv. Retract
   c. Policy and Process Enforcement
      i. Create
      ii. Maintain
      iii. Uphold
   d. Demonstrate Compliance
      i. Log
      ii. Audit
      iii. Report

V. Privacy Engineering
   A. The Privacy Engineering role in the organization
   B. Privacy Engineering Objectives
      a. Predictability
      b. Manageability
      c. Disassociability
   C. Privacy Design Patterns
      a. Design patterns to emulate
      b. Dark patterns to avoid
   D. Privacy Risks in Software
      a. Risks
      b. Countermeasures
VI. Privacy by Design Methodology

A. The Privacy by Design Process
   a. Goal Setting
   b. Documenting Requirements
   c. Understanding quality attributes
   d. Identify information needs
   e. High level design
   f. Low level design and implementation
   g. Impose controls
      1. Architect
      2. Secure
      3. Supervise
      4. Balance
   h. Testing and validation

B. Ongoing Vigilance
   a. Code reviews
   b. Code audits
   c. Runtime behavior monitoring
   d. Software evolution

VII. Technology Challenges for Privacy

A. Automated decision making
   a. Machine learning
   b. Deep learning
   c. Artificial Intelligence (AI)
   d. Context aware computing

B. Tracking and Surveillance
   a. Internet monitoring
   b. Web tracking
   c. Location tracking
   d. Audio and Video Surveillance
   e. Drones

C. Anthropomorphism
   a. Speech recognition
   b. Natural language understanding
   c. Natural language generation
   d. Chat bots
   e. Robots

D. Ubiquitous computing
   a. Internet of Things (IoT)
   b. Vehicular automation
   c. Wearable devices

E. Mobile Social Computing
   a. Geo-tagging
b. Geo-social patterns