Information Privacy Concepts

- Information privacy generally pertains to what is known as **personally identifiable information** (PII).
- **PII** is information that can be used to distinguish or trace an individual's identity, such as:
    - Information about birth, race, religion, weight, activities, geographic indicators, employment information, medical information, education information, and financial information;
    - Personal characteristics, including photographic images, x-rays, fingerprints, or biometric image; and
    - Asset information, such as Internet Protocol (IP) or media access control (MAC) address or other host-specific persistent static identifier that consistently links to a particular person or a small, well-defined group of people.

Privacy by Design

- In dealing with the privacy of PII, two (2) new concepts have emerged: privacy by design (PbD) and privacy engineering.
- The goal of privacy by design is to take privacy requirements into account throughout the system development process, from the conception of a new IT system through detailed system design, implementation, and operation.
    - **Privacy requirements**: These are system requirements that have privacy relevance. System privacy requirements define the protection capabilities provided by the system, the performance and behavioral characteristics exhibited by the system, and the evidence used to determine that the system privacy requirements have been satisfied. Privacy requirements are derived from various sources, including laws, regulations, standards, and stakeholder expectations.
- *Figure* 1 provides an overview of the major activities and tasks involved in integrating information privacy protection into any information system developed by an organization. The upper part of the figure encompasses design activities that determine what is needed and how to satisfy requirements. The lower part of the figure deals with the implementation and operation of privacy features as part of the overall system.

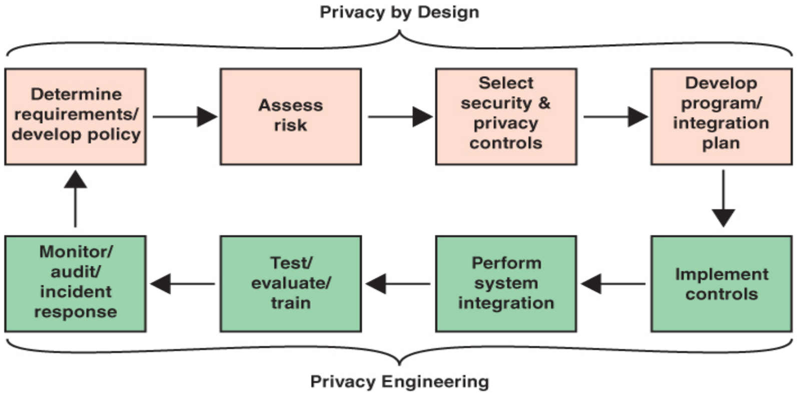
Privacy by Design
Determine requirements/ develop policy
Assess risk
Select security & privacy controls
Develop program/ integration plan
Implement controls
Perform system integration
Test/ evaluate/ train
Monitor/ audit/ incident response
Privacy Engineering

Figure 1. Information Privacy Development Life Cycle

Privacy by Design Principles

- A useful guide to developing a PbD approach is the set of foundational principles for PbD first proposed by Ann Cavoukian, as shown in *Figure* 2. These principles were later widely adopted as a resolution by other prominent policymakers at the 32nd Annual International Conference of Data Protection and Privacy Commissioners meeting.

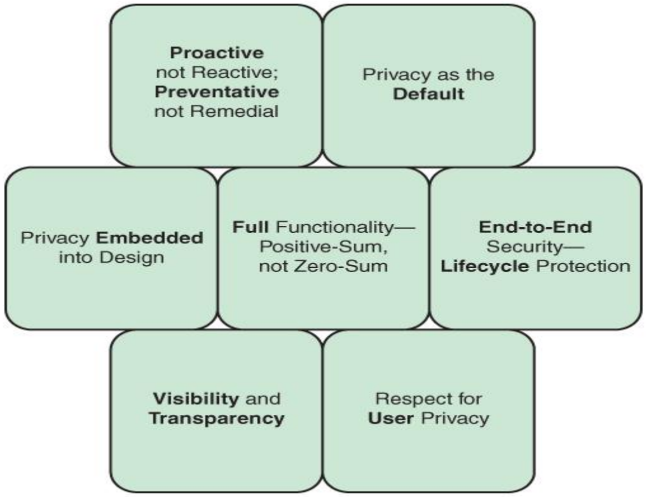
Proactive not Reactive; Preventative not Remedial
Privacy as the Default
Privacy Embedded into Design
Full Functionality— Positive-Sum, not Zero-Sum
End-to-End Security— Lifecycle Protection
Visibility and Transparency
Respect for User Privacy

Figure 2. Foundational Principles of Privacy by Design

- **Proactive, not reactive; preventive, not remedial:** PbD is an approach that anticipates privacy issues and seeks to prevent problems before they arise. In this approach, designers must assess the potential vulnerabilities in a system and the types of threats that may occur and then select technical and managerial controls to protect the system.
- **Privacy as the default:** This principle requires an organization to ensure that it only processes the data that is necessary to achieve its specific purpose and that PII is protected during collection, storage, use, and transmission.
- **Privacy embedded into the design:** Privacy protections should be core, organic functions, not added on after a design is complete. Privacy should be integral both to the design and architecture of IT systems and to business practices.
- **Full functionality: positive-sum, not zero-sum:** Designers should seek solutions that avoid requiring a trade-off between privacy and system functionality or between privacy and security.
- **End-to-end security—life cycle protection:** This principle encompasses two concepts. The terms end-to-end and life cycle refer to the protection of PII from the time of collection through retention and destruction. During this life cycle, there should be no gaps in the protection of the data or accountability for the data. The term security highlights that security processes and controls are used to provide not just security but privacy.
- **Visibility and transparency:** PbD seeks to assure users and other stakeholders that privacy-related business practices and technical controls are operating according to state commitments and objectives.
- **Respect for user privacy:** The organization must view privacy as primarily being characterized by personal control and free choice.

Privacy Risk Assessment

- The objective of a privacy risk assessment is to enable organization executives to determine an appropriate budget for privacy and, within that budget, implement the privacy controls that optimize the level of protection.

Privacy and Security Control Selection

- The privacy protection of PII involves the use of both controls that are specific to privacy and the use of controls developed for information security requirements.
- **Security controls** are safeguards or countermeasures prescribed for an information system or an organization that are designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements
- individual privacy cannot be achieved solely through securing personally identifiable information. Hence, both security and privacy controls are needed.
- **Privacy controls** are the technical, physical, and administrative (or management) measures employed within an organization to satisfy privacy requirements. Privacy controls might result in:
  - Removing the threat source;
  - Changing the likelihood that the threat can exploit a vulnerability by reducing or eliminating the vulnerability or by changing the amount of PII collected or the way it is processed; and
  - Changing the consequences of a privacy event.

Privacy Engineering

- Privacy engineering involves taking account of privacy during the entire life cycle of ICT (information and communications technology) systems
- Privacy engineering focuses on implementing techniques that decrease privacy risks and enables organizations to make purposeful decisions about resource allocation and effective implementation of controls in information systems
- Figure 1 indicates that privacy engineering encompasses the implementation, deployment, and ongoing operation and management of privacy features and controls in systems
- Privacy engineering involves both technical capabilities and management processes. The primary goals of privacy engineering are to:
  - Incorporate functionality and management practices to satisfy privacy requirements
  - Prevent compromise of PII
  - Mitigate the impact of breach of personal data.

- Privacy engineering is often used to encompass privacy-related activities throughout the system development life cycle. An example of this is shown in Figure 3.

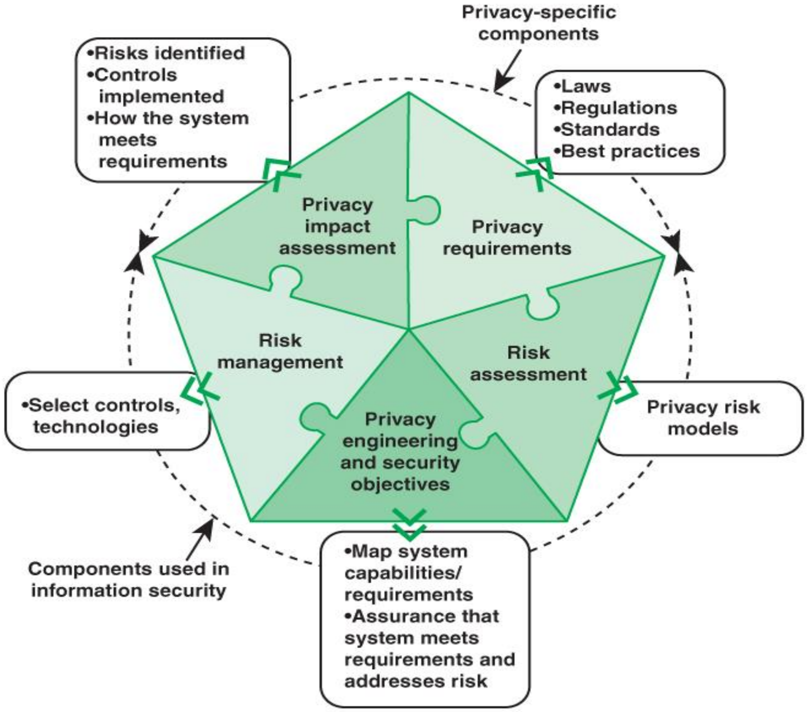
Privacy-specific components
•Risks identified
•Controls implemented
•How the system meets requirements
•Laws
•Regulations
•Standards
•Best practices
Privacy impact assessment
Privacy requirements
Risk management
Risk assessment
Privacy engineering and security objectives
•Select controls, technologies
Privacy risk models
•Map system capabilities/ requirements
•Assurance that system meets requirements and addresses risk
Components used in information security

Figure 3. Components of Privacy Engineering

- **Security risk assessment** is an expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.
- **Risk management** includes a disciplined, structured, and flexible process for organizational asset valuation; security and privacy control selection, implementation, and assessment; system and control authorizations; and continuous monitoring. Risk management is an iterative process, as illustrated in Figure 4, which consists of four steps:
  - Assess risk based on assets, threats, vulnerabilities, and existing controls. From these inputs, determine impact and likelihood and then the level of risk.
  - Identify potential security controls to reduce risk, prioritize their use, and select controls for implementation.
  - Allocate resources, roles, and responsibilities and implement controls.
  - Monitor and evaluate risk treatment effectiveness.

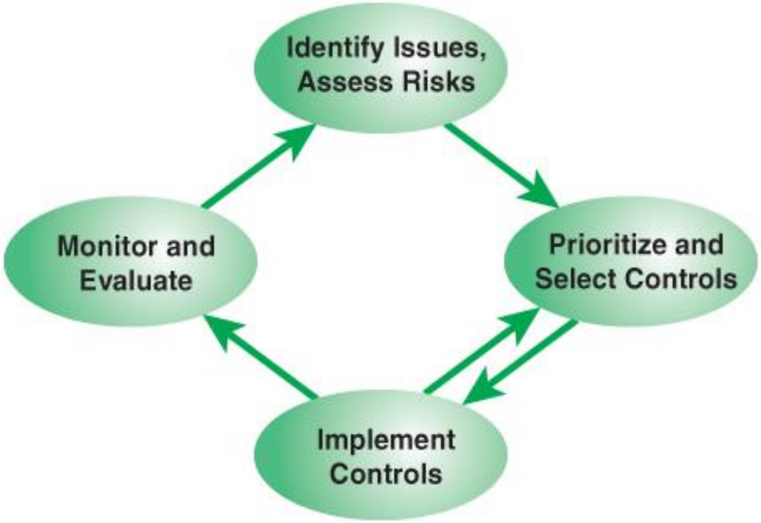

Figure 4. Risk Management Cycle

- **Privacy requirements** are system requirements that have privacy relevance. System privacy requirements define the protection capabilities provided by the system, the performance and behavioral characteristics exhibited by the system, and the evidence used to determine that the system privacy requirements have been satisfied. Privacy requirements are derived from various sources, including laws, regulations, standards, and stakeholder expectations.
- **Privacy impact assessment (PIA)** is an analysis of how information is handled: to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; to determine the risks and effects of collecting,

maintaining, and to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks. In essence, PIA consists of a privacy risk assessment followed by a selection of privacy and security controls to reduce the risk.

- **Privacy engineering and security objectives** focus on the types of capabilities the system needs to demonstrate the implementation of an organization's privacy policies and system privacy requirements.

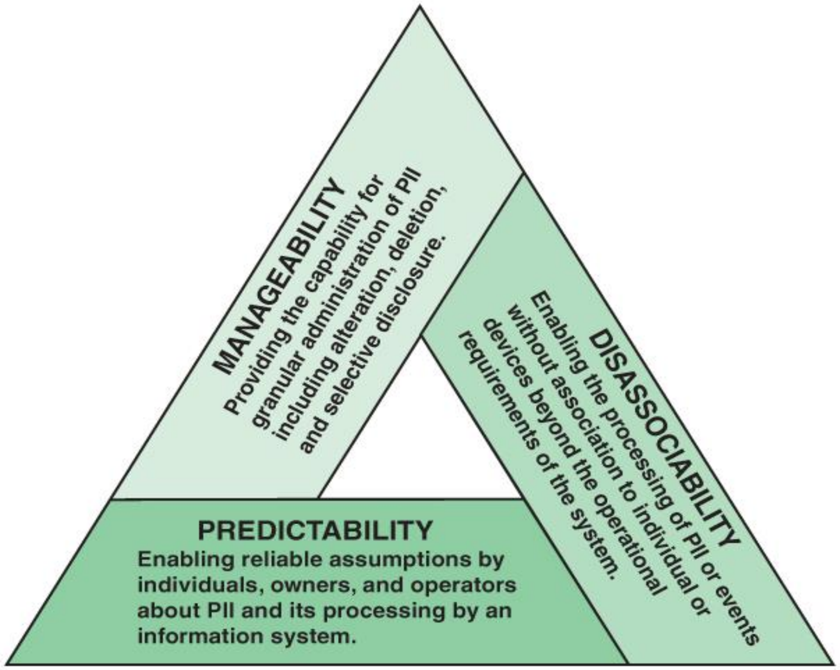
MANAGEABILITY
Providing the capability for granular administration of PII including alteration, deletion, and selective disclosure.
DISASSOCIABILITY
Enabling the processing of PII or events without association to individual or devices beyond the operational requirements of the system.
PREDICTABILITY
Enabling reliable assumptions by individuals, owners, and operators about PII and its processing by an information system.

Figure 5. Privacy Engineering Objectives

References:

Kumar, G., Saini, DK., Huy Cuong, NH. (2020). *Cyber defense mechanisms: Security, privacy, and challenges.* CRC Press.

Stallings, W. (2019). *Information privacy engineering and privacy by design: Understanding privacy threats, technologies, and regulations.* Assison-Wesley Professional.

Torra, V. (2018). *Data privacy: foundations, new developments, and the big data challenge.* Springer International Publishing.