INFORMATION PRIVACY ENGINEERING AND PRIVACY BY DESIGN

Understanding Privacy Threats, Technology, and Regulations Based on Standards and Best Practices

WILLIAM STALLINGS

Information Privacy Engineering and Privacy by Design

Understanding Privacy Threats, Technology, and Regulations Based on Standards and Best Practices

Dr. William Stallings

Addison-Wesley

Visit us on the Web: informit.com/aw

Library of Congress Control Number: 2019952003

ISBN-13: 978-0-13-530215-6

ISBN-10: 0-13-530215-3

ScoutAutomatedPrintCode

Editor-in-Chief
Mark Taub

Product Line Manager
Brett Bartow

Development Editor
Christopher A. Cleveland

Managing Editor
Sandra Schroeder

Senior Project Editor
Lori Lyons

Copy Editor
Catherine D. Wilson

Production Manager
Gayathri Umashankaran/
codeMantra

Indexer
Tim Wright

Proofreader
Karen Davis

Technical Reviewers
Bruce DeBruhl

Stefan Schiffner

Editorial Assistant
Cindy Teeters

Cover Designer
Chuti Prasertsith

Compositor
codeMantra

Chapter 2

Information Privacy Concepts

Learning Objectives

After studying this chapter, you should be able to:

- Explain the difference between privacy by design and privacy engineering
- Understand how privacy-related activities fit into the system development life cycle
- Define *privacy control*
- Discuss the areas of overlap between security and privacy and the areas that are distinct to either security or privacy
- Explain the trade-off between privacy and utility
- Explain the distinction between privacy and usability

This chapter provides a roadmap for the remainder of the book, introducing the key information privacy concepts and indicating how they relate to one another. The chapter begins by defining key terms in the field of information privacy. Then, Sections 2.2 and 2.3 introduce the concepts of privacy by design and privacy engineering. Sections 2.4 through 2.6 deal with the relationship between privacy and security, the trade-off between privacy and utility, and the concept of usable privacy.

2.1 Key Privacy Terminology

The term ***privacy*** is used frequently in ordinary language as well as in philosophical, political, and legal discussions. However, there is no single definition or analysis or meaning of the term; a good survey of this topic is the privacy entry in the *Stanford Encyclopedia of Philosophy* [DECE18]. Two general characteristics of privacy are the right to be left alone—that is, free from being observed or disturbed—and the ability to control the information released about oneself.

This book is concerned with a concept of privacy referred to as ***information privacy***. ITU-T Recommendation X.800 (*Security Architecture for Open Systems Interconnection*) defines *privacy* as the right of individuals to control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed. A U.S. National Research Council report (*At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues*) [CLAR14] indicates that in the context of information, the term *privacy* usually refers to making ostensibly private information about an individual unavailable to parties that should not have that information. Privacy interests attach to the gathering, control, protection, and use of information about individuals.

Information privacy generally pertains to what is known as ***personally identifiable information*** (PII), as opposed to, say, video surveillance. PII is information that can be used to distinguish or trace an individual's identity. NIST SP 80-122 (*Guide to Protecting the Confidentiality of Personally Identifiable Information*) gives the following examples of information that might be considered PII:

- Name, such as full name, maiden name, mother's maiden name, or alias
- Personal identification number, such as Social Security number (SSN), passport number, driver's license number, taxpayer identification number, patient identification number, and financial account or credit card number
- Address information, such as street address or email address
- 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 to a small, well-defined group of people
- Telephone numbers, including mobile, business, and personal numbers
- Personal characteristics, including photographic images (especially of the face or other distinguishing characteristic), x-rays, fingerprints, or other biometric image or template data (e.g., retinal scan, voice signature, facial geometry)
- Information identifying personally owned property, such as vehicle registration number or title number and related information
- Information about an individual that is linked or linkable to one of the above (e.g., date of birth, place of birth, race, religion, weight, activities, geographic indicators, employment information, medical information, education information, financial information)

In dealing with the privacy of PII, two 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. ISO 29100 (*Information Technology—Security Techniques—Privacy Framework*) views PbD as the practice of considering privacy safeguarding measures at the time of the design of the system; that is, designers should consider privacy compliance during the design phase for systems processing PII rather than address compliance only at a subsequent stage.

Privacy engineering involves taking account of privacy during the entire life cycle of ICT (information and communications technology) systems, such that privacy is and remains an integral part of their function. NISTIR 8062 (*An Introduction to Privacy Engineering and Risk Management in Federal Systems*) defines privacy engineering as a specialty discipline of systems engineering focused on achieving freedom from conditions that can create problems for individuals with unacceptable consequences that arise from the system as it processes PII. 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. Such techniques decrease risks related to privacy harms and enable purposeful decisions about resource allocation and effective implementation of controls.

The European Data Protection Supervisor (EDPS), an independent institution of the European Union, relates the two concepts by indicating that the principles of privacy by design must be translated into privacy engineering methodologies [EDPS18].

Figure 2.1 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 deal with determining what is needed and how to satisfy requirements. The lower part of the figure deals with implementation and operation of privacy features as part of the overall system.

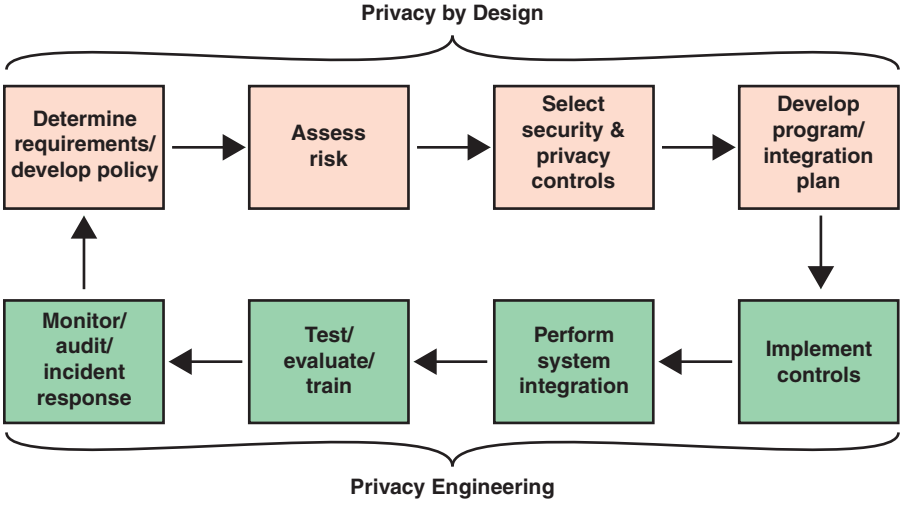


FIGURE 2.1 Information Privacy Development Life Cycle

Section 2.2 provides an overview of PbD, and Section 2.3 looks at privacy engineering.

2.2 Privacy by Design

PbD, as defined earlier, is concerned with ensuring that privacy features are designed into a system before implementation begins. PbD is a holistic concept that applies to information technology, business practices, processes, physical design, and networked infrastructure.

Privacy by Design Principles

A useful guide to the development of a PbD approach is the set of foundational principles for PbD first proposed by Ann Cavoukian, the information and privacy commissioner of Ontario [CAVO09]. 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 [ICDP10]. Figure 2.2 illustrates the foundational principles of PbD, which are further described in the list that follows:

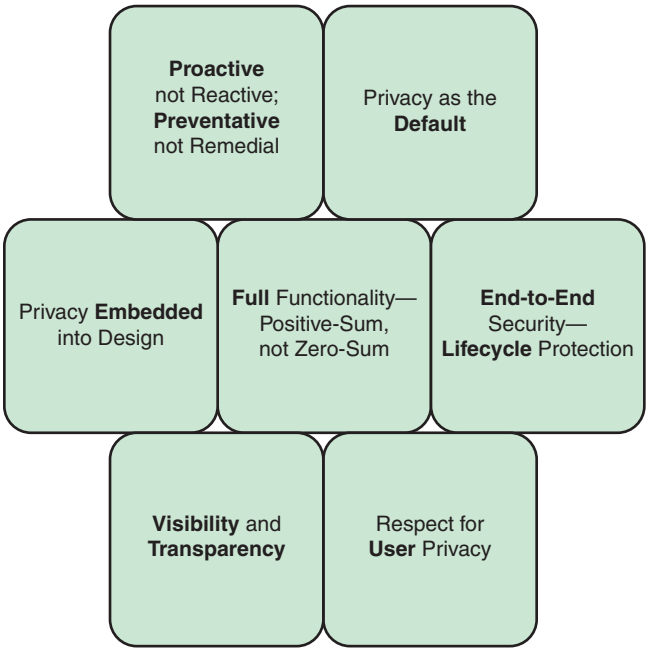


FIGURE 2.2 Foundational Principles of Privacy by Design

- **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. In addition, individuals need not take affirmative action to protect their PII.
- **Privacy embedded into 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:** An essential goal of PbD is that it not degrade either the system functionality that is required or the security measures that are part of the system. 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 in accountability for the data. The term ***security*** highlights that security processes and controls are used to provide not just security but privacy. The use of security measures ensures the confidentiality, integrity, and availability of PII throughout the life cycle. Examples of security measures include encryption, access controls, logging methods, and secure destruction.
- **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. Key aspects of this principle are the following:
  - **Accountability:** The organization should clearly document responsibility for all privacy-related policies and procedures.
  - **Openness:** The organization should provide information about the policies and practices related to managing PII, as well as the individuals and groups accountable for protecting PII within the organization. The concept of openness includes a clearly defined organizational privacy policy for internal distribution as well as a privacy notice available to outsiders, such as web users.
  - **Compliance:** The organization should have compliance and redress mechanisms.
- **Respect for user privacy:** The organization must view privacy as primarily being characterized by personal control and free choice. Key aspects of this principle are the following:
  - **Consent:** Except where otherwise mandated by law, each individual should be empowered with consent for the collection, use, or disclosure of PII.

- **Accuracy:** The organization is responsible for ensuring that any PII that it maintains is accurate and up-to-date.
- **Access:** Individuals should be able to access any PII maintained by an organization, be informed of its uses and disclosures, and be able to challenge its correctness.
- **Compliance:** The organization should have compliance and redress mechanisms.

These principles are fundamental tenets that guide a privacy program, which an organization must translate into specific practices. The remainder of this section looks at the major activities involved in planning and designing information privacy protection for an information system. In essence, the PbD principles are requirements for the way in which systems are designed and implemented. The descriptions throughout this book of the various aspects of information privacy reflect these requirements.

Requirements and Policy Development

Refer to Figure 2.1 and notice that the first stage of privacy by design deals with privacy planning and policy. An essential element of planning for information privacy is the definition of the privacy requirements. The specific requirements for privacy features and protections drive the planning, design, and implementation of these features and protections. Key sources of requirements include regulations, standards, and the organization's contractual commitments. Chapter 3, "Information Privacy Requirements and Guidelines," examines this topic in detail.

A key actor at this stage is the ***system owner***, which is the person or organization having responsibility for the development, procurement, integration, modification, operation, maintenance, and final disposition of an information system. The system owner needs to identify the standards and regulations that apply and develop an overall plan for privacy milestones during system development. It is also important to ensure that all key stakeholders have a common understanding, including privacy implications, considerations, and requirements. This planning activity enables developers to design privacy features into the project.

An expected output of this activity is a set of supporting documents that provide a record of the agreed planning decisions, including how these decisions conform to overall corporate privacy policy. Another key output is an initial set of privacy activities and decisions related to the overall development of the information system.

This stage is explored in more detail in Part V, "Information Privacy Management."

Privacy Risk Assessment

The ultimate 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. This objective is met by providing an estimate of the potential cost to the organization of privacy violations, coupled with an estimation of the likelihood of such breaches. Four elements are involved in the assessment:

- **Privacy-related asset:** Anything that has value to the organization and that therefore requires protection. With respect to privacy, the primary asset is PII of employees, customers, patients, business partners, and so on. This category also includes intangible assets such as reputation and goodwill.
- **Privacy threat:** A potential for violation of privacy, which exists when there is a circumstance, a capability, an action, or an event that could violate privacy and cause harm to an individual. That is, a threat is a possible danger that might exploit vulnerability. A related term is ***threat action***, which is a realization of a threat—that is, an occurrence in which a vulnerability is exploited as a result of either an accidental event or an intentional act.
- **Privacy vulnerability:** A flaw or weakness in a system's design, implementation, or operation and management that could be exploited by a threat action to violate the system's privacy policy and compromise PII.
- **Privacy controls:** The management, operational, and technical controls (i.e., countermeasures) prescribed for an information system to protect PII and ensure that the organization's privacy policy is enforced.

Using these four elements, a privacy risk assessment consists of these three steps:

1. Determine the harm, or impact, to individuals and the organization of a privacy violation. For each privacy-related asset, determine the possible threats to that asset. Then determine the impact to individuals if their privacy rights are violated and the impact to the organization, in terms of cost or lost value, if a threat action occurs.
2. Determine the likelihood of a privacy incident, where a ***privacy incident*** is defined as an occurrence that actually or potentially violates the privacy of PII or that constitutes a violation or an imminent threat of violation of privacy policies, privacy procedures, or acceptable use policies. For each asset, three factors determine the likelihood: the relevant threats to the asset, the vulnerability of the asset to each threat, and the privacy controls currently in place that reduce the likelihood that each threat will cause harm.
3. Determine the level of risk as the combination of the cost if the privacy incident occurs and the likelihood that that incident occurs.

An organization should use the level of risk to determine a budget allocation for security controls. The combination of privacy risk assessment and privacy control selection is referred to as a *privacy impact assessment* (PIA). Chapter 11, "Risk Management and Privacy Impact Assessment," discusses PIAs in detail.

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. This section discusses both.

Privacy Controls

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
- Changing the consequences of a privacy event

Two especially valuable sources of information on privacy controls can be used as guidance in control selection. NIST SP 800-53 (*Security and Privacy Controls for Information Systems and Organizations*) is an invaluable and extraordinarily detailed discussion of controls and should be consulted in the development of any risk treatment plan. This 500-page document provides plenty of guidance on the overall development of a treatment plan and includes an extensive catalog of security controls and privacy controls. ISO 29151 (*Code of Practice for Personally Identifiable Information Protection*) offers guidance on a broad range of privacy controls that are commonly applied in many different organizations that deal with protection of PII.

Part IV, "Privacy Enhancing Technologies," provides a detailed examination of technical privacy controls that can be implemented as part of an IT system or subsystem. Part V includes a discussion of administrative and managerial controls.

Security Controls

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. As discussed in Section 2.4, there is an overlap in the areas of concern of information security and information privacy. Security controls, when selected and implemented for information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII, address both security and privacy concerns. For example, access control mechanisms can be used to limit the access to PII stored in a database.

Nonetheless, individual privacy cannot be achieved solely through securing personally identifiable information. Hence, both security and privacy controls are needed.

As discussed previously, SP 800-53 is an excellent source of security controls. ISO 27002 (*Code of Practice for Information Security Controls*) is another good source. Part III, "Technical Security Controls for Privacy" covers this topic.

The Selection Process

Selecting and documenting security and privacy controls should be synchronized with the risk assessment activity. Typically, a baseline set of controls is selected and then adjusted, with additional controls based on a refinement of the risk assessment. The refinement considers any possible secondary risks that result from the baseline controls and how they affect the risk assessment.

Privacy Program and Integration Plan

The principal objective of PbD is to ensure that information privacy considerations are considered at every stage of system development and that privacy protection measures are designed into the system during the system design and development process rather than retrofitted. An essential element in achieving this objective is a documented and approved privacy program. Elements of such a program should include:

- Identifying key privacy roles that will be active throughout the system design and implementation
- Identifying standards and regulations that apply
- Developing an overall plan for privacy milestones during system development
- Ensuring that all key stakeholders have a common understanding, including privacy implications, considerations, and requirements
- Describing the requirements for integrating privacy controls within the system and the process for coordinating privacy engineering activities with overall system development

Part of the privacy program document, or provided as a separate document, is a privacy plan that deals with the implementation of privacy features and their integration with the rest of the system. This is a formal document that provides an overview of the privacy requirements for the information system and describes the privacy controls that are in place or planned for meeting those requirements. Key components of the plan are a privacy categorization, which gives the acceptable level of risk for each distinct element of the system, and a description of each privacy control and its implementation plan.

This stage should also produce a detailed architecture that incorporates privacy features and controls into the system design. Expected outputs include:

- A schematic of privacy integration that provides details on where, within the system, privacy is implemented and, if applicable, where privacy mechanisms are shared by multiple services or applications
- A list of shared services and resulting shared risk
- Identification of common controls used by the system

Chapter 10, "Information Privacy Governance and Management," discusses privacy programs and plans.

2.3 Privacy Engineering

Figure 2.1 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

Although Figure 2.1 shows privacy engineering as being distinct from, and following on, PbD, the term ***privacy engineering*** is often used to encompass privacy-related activities throughout the system development life cycle. An example of this is shown in Figure 2.3, adapted from NISTIR 8062.

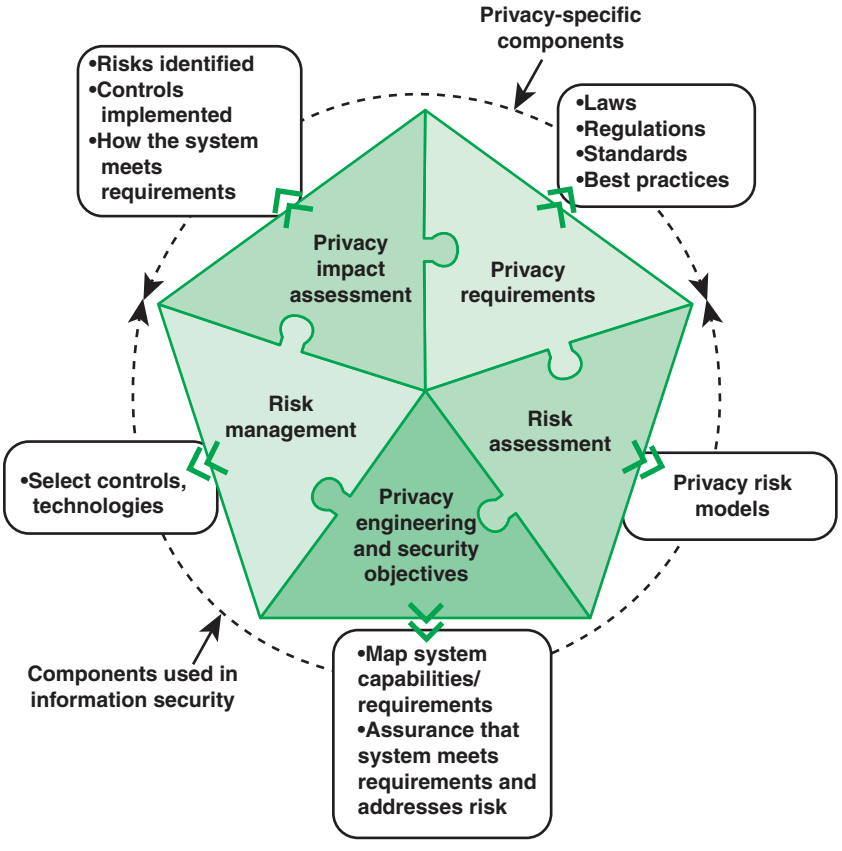


FIGURE 2.3 Components of Privacy Engineering

As illustrated in Figure 2.3, the NIST document lists five components of privacy engineering—two that are specific to the privacy engineering process and three that are components typically used in information security management. The components are:

- **Security risk assessment:** A security risk is an expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result. Security risk assessment is a process that systematically (a) identifies valuable system resources and threats to those resources, (b) quantifies loss exposures (i.e., loss potential) based on estimated frequencies and costs of occurrence. Thus, risk assessment follows two parallel paths. First, for each threat to a resource, the value of the resource is assessed and the potential impact, or cost, if the threat to that resource becomes a successful threat action. Second, based on the strength of a threat, the probability of the threat becoming an actual threat action, and the vulnerability of the resource, a likelihood of a successful threat action is determined. Finally, the potential impact of the threat and the likelihood of its success are factors in determining the risk.
- **Risk management:** NIST SP 800-37 (*Risk Management Framework for Information Systems and Organizations*) states that 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. It also includes enterprise-level activities to help better prepare organizations to execute the RMF at the system level. Risk management is an iterative process, as illustrated in Figure 2.4, based on one in ITU-T X.1055 (*Risk management and risk profile guidelines for telecommunication organizations*), consisting of four steps:

  1. Assess risk based on assets, threats, vulnerabilities, and existing controls. From these inputs determine impact and likelihood and then the level of risk. This is the risk assessment component described in the preceding bullet.
  2. Identify potential security controls to reduce risk, prioritize their use, and select controls for implementation.
  3. Allocate resources, roles, and responsibilities and implement controls.
  4. Monitor and evaluate risk treatment effectiveness.

  In the context of privacy engineering, the emphasis is on privacy risk and the implementation of privacy controls. Chapter 11 discusses risk management.

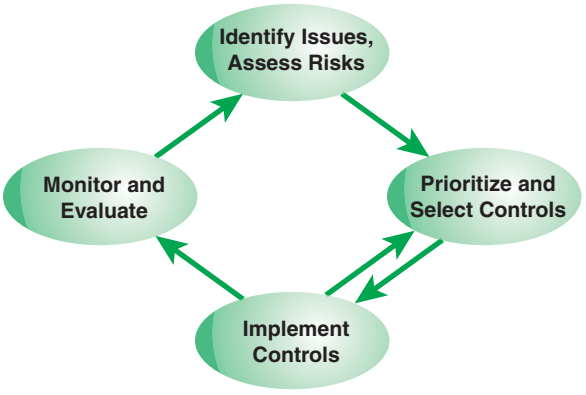


FIGURE 2.4 Risk Management Cycle

- **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 a variety of sources including laws, regulations, standards, and stakeholder expectations. Chapter 3 examines privacy requirements.
- **Privacy impact assessment:** The NIST Computer Security Glossary (https://csrc.nist.gov/glossary) defines a PIA as an analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (ii) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks. In essence, PIA consists of privacy risk assessment followed by a selection of privacy and security controls to reduce the risk. Chapter 11 examines the PIA.
- **Privacy engineering and security objectives:** Information security risk assessment focuses on meeting the common security objectives, including confidentiality, integrity, and availability (Figure 1.1). Similarly, privacy engineering objectives focus on the types of capabilities the system needs in order to demonstrate implementation of an organization's privacy policies and system privacy requirements. NISTIR 8062 proposes three privacy objectives, illustrated in Figure 2.5. Chapter 3 expands on this topic.

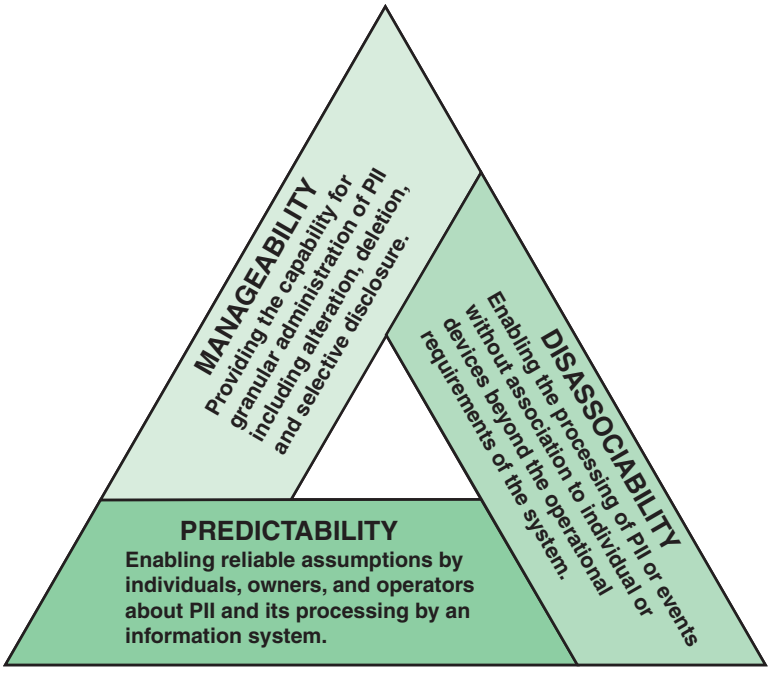


FIGURE 2.5 Privacy Engineering Objectives

The remainder of this section provides an overview of the major stages of privacy engineering (refer to Figure 2.1). Chapter 10 addresses the management and operational aspects of these stages.

Privacy Implementation

During the privacy implementation stage, developers configure and enable system privacy features. Implementation includes alignment and integration of privacy controls with system functional features. As part of implementation, an organization should perform developmental testing of the technical and privacy features/functions to ensure that they perform as intended prior to launching the integration phase.

System Integration

System integration activity occurs at the point of deployment of the system for operation. Privacy control settings are enabled, and other privacy features need to be integrated at this point. The output of this activity is a verified list of operational privacy controls integrated into the completed system documentation.

Privacy Testing and Evaluation

Privacy testing includes the following types of testing:

- **Functional testing:** Advertised privacy mechanisms of an information system are tested under operational conditions to determine whether a given function works according to its requirements.
- **Penetration testing:** Evaluators mimic real-world attacks in an attempt to identify ways to circumvent the privacy features of an application, a system, or a network.
- **User testing:** The software or system is tested in the "real world" by the intended audience. Also called *end user testing*.

This stage should result in formal management certification and accreditation of the system with its privacy features. ***Certification*** involves a comprehensive assessment of the management, operational, and technical privacy controls in an information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. ***Accreditation*** is the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of privacy controls.

Privacy Auditing and Incident Response

In the privacy auditing and incident response stage, systems and products are in place and operating, enhancements and/or modifications to the system are developed and tested, and hardware and/or software is added or replaced. During this stage, the organization should continuously monitor performance of the system to ensure that it is consistent with pre-established privacy requirements and that needed system modifications are incorporated.

Two key activities during this stage are as follows:

- **Auditing:** Auditing involves independent examination of records and activities to ensure compliance with established controls, policy, and operational procedures and to recommend any indicated changes in controls, policies, or procedures.
- **Incident response:** An IT security incident is an adverse event in a computer system or network caused by the failure of a security mechanism or an attempted or threatened breach of such mechanisms. Incident response involves the mitigation of violations of security policies and recommended practices.

Chapter 13, "Event Monitoring, Auditing, and Incident Response," discusses auditing and incident response.

2.4 Privacy and Security

The two concepts of privacy and information security are closely related. On the one hand, the scale and interconnectedness of personal information collected and stored in information systems has increased dramatically, motivated by law enforcement, national security, and economic incentives. Economic incentives perhaps have been the main driving force. In a global information economy, it is likely that the most economically valuable electronic asset is aggregations of information on individuals [JUDY14]. On the other hand, individuals have become increasingly aware of the extent to which government agencies, businesses, and even Internet users have access to their personal information and private details about their lives and activities.

Areas of Overlap Between Security and Privacy

Although security and privacy are related, they are not equivalent. Figure 2.6, from NISTIR 8062, shows a non-proportional representation of the relationship between the privacy and security domains. While some privacy concerns arise from unauthorized activity, privacy concerns also can arise from authorized processing of information about individuals. Recognizing the boundaries and overlap between privacy and security is key to determining when existing security risk models and security-focused guidance may be applied to address privacy concerns—and where there are gaps that need to be filled in order to achieve an engineering approach to privacy. For instance, existing information security guidance does not address the consequences of a poor consent mechanism for use of PII, the purpose of transparency, what PII is being collected, correction of PII, or which changes in use of PII are permitted if authorized personnel are conducting the activity. Given these material distinctions in the disciplines, it should be clear that agencies will not be able to effectively manage privacy solely on the basis of managing security.

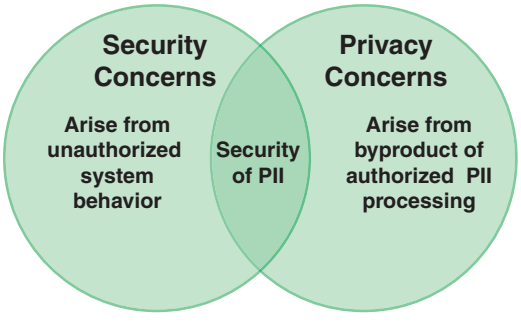


FIGURE 2.6 Overlap Between Information Security and Privacy

Figure 2.7, from the technical paper *Privacy Fundamentals: What an Information Security Officer Needs to Know* [BAKI05], further illustrates the overlap and distinctions between security and privacy by listing key objectives. Some objectives—such as availability, system and data protection

from threats, and physical protection—are primarily information security objectives. Objectives dealing specifically with the management and use of PII are primarily or exclusively privacy objectives. The technical paper just mentioned identifies five objectives that are relevant to both privacy and security [BAKI05]. Table 2.1 indicates the difference in emphasis for each objective for privacy and security.

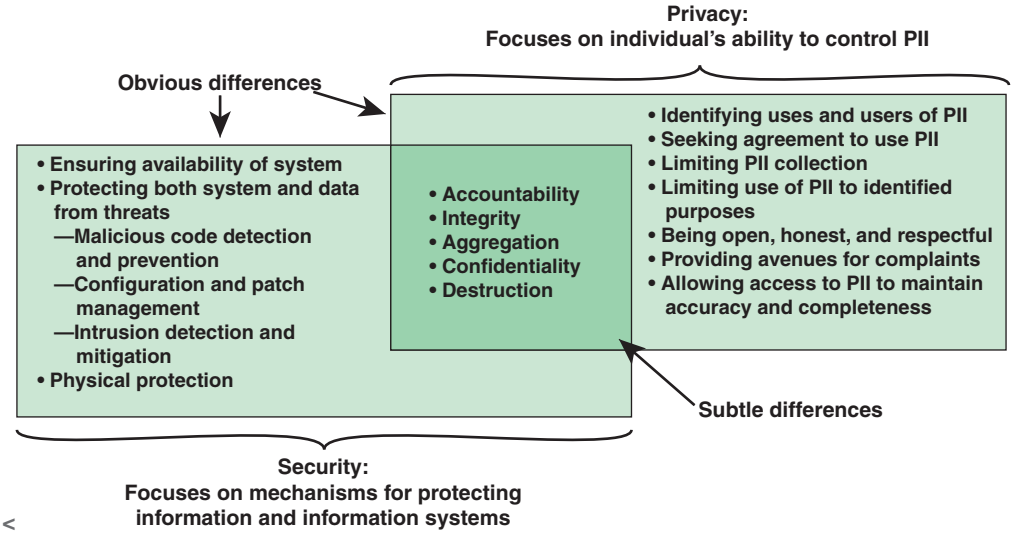


FIGURE 2.7 Privacy and Security Objectives

TABLE 2.1 Overlapping Security and Privacy Objectives

	Security	Privacy
Accountability	Focuses on tracking an individual's actions and manipulation of information	Focuses on tracking the trail of PII disclosure
Integrity	Protects against the corruption of data by authorized or unauthorized individuals	Seeks to ensure that inaccurate PII is not used to make an inappropriate decision about a person
Aggregation	Focuses on determining the sensitivity of derived and aggregated data so that appropriate access guidance can be defined	Dictates that aggregation or derivation of new PII should not be allowed if the new information is neither authorized by law nor necessary to fulfill a stated purpose
Confidentiality	Focuses on processes and mechanisms (e.g., authenticators) that prevent unauthorized access	Focuses on ensuring that PII is only disclosed for a purpose consistent with the reason it was collected
Destruction	Focuses on ensuring that the information cannot be recovered once deleted	Addresses the need for the complete elimination of collected information once it has served its purpose

Trade-Offs Between Security and Privacy

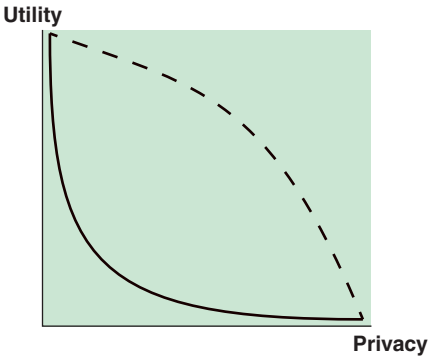
To some extent, information security measures can protect privacy. For example, an intruder seeking ostensibly private information (e.g., personal emails or photographs, financial or medical records, phone calling records) may be stymied by good cybersecurity measures. In addition, security measures can protect the integrity of PII and support the availability of PII. But the National Research Council paper *At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues* points out that certain measures taken to enhance cybersecurity can also violate privacy [CLAR14]. For example, some firewalls use technical measures to block Internet traffic containing malware before it reaches its destination. To identify malware-containing traffic, the content of all in-bound network traffic must be inspected. But some regard inspection of traffic by any party other than its intended recipient as a violation of privacy because most traffic will in fact be malware free. Under many circumstances, inspection of traffic in this manner is also a violation of law.

2.5 Privacy Versus Utility

An important consideration in the provision of privacy features in an information system or database is the potential conflict between the privacy of PII and the potential utility of collections of PII to third parties. In this context, the term ***utility*** can be defined as a quantifiable benefit to multiple legitimate information consumers [SANK11]. How specifically to quantify the utility of information depends on the nature of the information and the application context.

Utility and privacy are often competing requirements. Any access of data that contains or is derived from PII has the potential to leak information that the source of the PII wishes to keep private. On the other hand, increasing the privacy restrictions on information increases the restrictions on the flow of potentially useful information. For example, databases of individual data records can facilitate beneficial research in areas such as public health, medicine, criminal justice, and economics. Several strategies can be used to protect privacy, such as making available only aggregations of data or removing key identifiers and/or altering values of sensitive attributes before releasing the data. It should be clear that the more aggressive the measures to protect privacy, the less utility the information will have for researchers.

Figure 2.8 illustrates the trade-off between utility and privacy. With no special measures taken, there is a clear loss of privacy with increased utility and vice versa. One of the objectives of privacy by design and privacy engineering is to provide technical and managerial safeguards to privacy while enabling a high degree of utility. The upper line in the figure indicates this.



Solid line: little or no use of PbD and privacy engineering techniques
Dashed line: cost-effective use of PbD and privacy engineering techniques

FIGURE 2.8 Utility–Privacy Trade-Off

2.6 Usable Privacy

Like utility, usability is an important constraint in PbD and privacy engineering. ISO 9241-11 (*Ergonomic Requirements for Office Work with Visual Display Terminals (VDTs)—Part 11: Guidance on Usability*) defines ***usability*** as "the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use." The key terms in this definition are:

- **Effectiveness:** Accuracy and completeness with which users achieve specified goals. This is typically based on error rates.
- **Efficiency:** Resources expended in relation to the accuracy and completeness with which users achieve goals. This is typically based on the time required to complete a task or subtask, taking into account accuracy goals.
- **Satisfaction:** Freedom from discomfort and positive attitudes toward the use of the product. This is a subjective parameter and can be judged using questionnaires.
- **Context of use:** Users, tasks, equipment (hardware, software, and materials), and the physical and social environments in which a product is used.
- **User:** A person who interacts with the product.
- **Goal:** The intended outcome.
- **Task:** An activity (physical or cognitive) required to achieve a goal.
- **Product:** Part of the equipment (hardware, software, and materials) for which usability is to be specified or evaluated.

Users of Privacy Services and Functions

The National Research Council publication *Toward Better Usability, Security, and Privacy of Information Technology* points out that usability in the context of privacy can refer to three different classes of users [NRC10]:

- **End users of IT systems:** End users of IT systems are individuals who wish to have as much control as possible over the privacy of their PII. Examples of privacy services for end users are those that allow individuals to opt in or opt out of certain uses of their PII, enable them to determine the accuracy of their PII stored in databases, and file complaints about PII violations. Frequently, end users find these services difficult to understand and use.
- **Administrators of IT systems:** Administrators need to configure IT systems to enable or disable specific privacy features for individuals or groups of individuals whose PII is stored in the system. Administrators often contend with systems that are difficult to understand and configure.
- **System developers:** Developers need usable tools that make it easy to avoid or detect design and coding errors that affect privacy.

Usability and Utility

Usability and utility are distinct concepts. *Usability* refers to the ease of use of privacy features. *Utility* refers to the functionality available for databases containing PII with privacy protection in place. Both concepts need to be considered through the design, implementation, and operation of IT systems containing PII.

2.7 Key Terms and Review Questions

Key Terms

accreditation	personally identifiable information (PII)
auditing	privacy
certification	privacy by design (PbD)
end user testing	privacy control
functional testing	privacy engineering
incident response	privacy impact assessment (PIA)
information privacy	privacy-related asset
penetration testing	privacy requirements

privacy threat	system owner
privacy vulnerability	threat action
risk assessment	usability
risk management	user testing
security	utility
stakeholder	V model
system development life cycle (SDLC)	

Review Questions

1. Explain the term *information privacy*.
2. What is personally identifiable information?
3. Explain the manner in which privacy by design and privacy engineering operate together.
4. What are the commonly accepted foundational principles for privacy by design?
5. What elements are involved in privacy risk assessment?
6. Describe the various types of privacy controls.
7. What issues should be considered in selecting privacy controls?
8. Explain the difference between privacy risk assessment and privacy impact assessment.
9. What are the types of privacy testing?
10. What are the overlapping and non-overlapping areas of concern with respect to information security and information privacy?
11. Explain the trade-off between privacy and utility.
12. What is the difference between usability and utility?

2.8 References

BAKI05: Bakis, B. *Privacy Fundamentals: What an Information Security Officer Needs to Know*. Mitre Technical Paper, October 18, 2005. https://www.mitre.org/publications/technical-papers

CAVO09: Cavoukian, A. *Privacy by Design: The 7 Foundational Principles.* Information and Privacy Commissioner of Ontario, Canada, 2009.

CLAR14: Clark, D., Berson, T., and Lin, H. (eds.). *At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues.* National Research Council, 2014.

DECE18: DeCew, J. "Privacy." *The Stanford Encyclopedia of Philosophy*, Spring 2018, Edward N. Zalta (ed.), https://plato.stanford.edu/archives/spr2018/entries/privacy

EDPS18: European Data Protection Supervisor. *Preliminary Opinion on Privacy by Design.* May 31, 2018. https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf

ICDP10: International Conference of Data Protection and Privacy Commissioners. *Resolution on Privacy by Design*. October 2010. https://icdppc.org/document-archive/adopted-resolutions/

JUDY14: Judy, H., et al. "Privacy in Cyberspace." In Bosworth, S., Kabay, M., and Whyne, E. (eds.). *Computer Security Handbook.* New York: Wiley, 2014.

NRC10: National Research Council. *Toward Better Usability, Security, and Privacy of Information Technology.* The National Academies Press, 2010.

SANK11: Sankar, L., and Poor, H. "Utility–Privacy Tradeoffs in Databases: An Information-Theoretic Approach." *IEEE Transactions on Information Forensics and Security*. February 2011.