Chapter 1

Privacy in the Modern Era

THE CIPP/US EXAM OBJECTIVES COVERED IN THIS CHAPTER INCLUDE:

✓ **Domain I. Introduction to the U.S. Privacy Environment**

- I.C. Information Management from a U.S. Perspective
  - I.C.b Privacy Program Development
  - I.C.c Managing User Preferences
  - I.C.f Accountability
  - I.C.h Online Privacy
  - I.C.i Privacy Notices

COPYRIGHTED MATERIAL

Privacy concerns surround us in our daily lives. We hear troubling reports of companies acquiring and misusing personal information about their customers. News stories inform us of data breaches where massive quantities of personal information wound up in unknown hands. Legislators at the federal and state levels debate these issues and often pass new laws regulating different aspects of privacy.

We are left to navigate a confusing environment full of ambiguous and overlapping ethical obligations, laws, regulations, and industry standards. Companies and consumers alike find themselves confused about the requirements they face and the appropriate course of action. Privacy professionals play a crucial role in helping their organizations navigate these confusing waters.

Introduction to Privacy

Privacy is one of the core rights inherent to every human being. The term is defined in many historic works, but they all share the basic tenet of individuals having the right to protect themselves and their information from unwanted intrusions by others or the government. Let's take a brief look at the historical underpinnings of privacy in the United States.

In 1890, a young lawyer named Louis D. Brandeis wrote an article for the *Harvard Law Review* titled "The Right to Privacy." In that article, Brandeis wrote:

> Recent inventions and business methods call attention to the next step which must be undertaking for the protection of the person, and for securing to the individual . . . the right "to be let alone." Instantaneous photographs and newspaper enterprises have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the house-tops." For years there has been a feeling that the law must afford some remedy for the unauthorized circulation of portraits of private persons; and the evil of the invasion of privacy by the newspapers, long keenly felt, has been but recently discussed by an able writer.

Reading that excerpt over a century later, it's easy to see echoes of Brandeis's concerns about technology in today's world. We could just as easily talk about the impact of social

media, data brokerages, and electronic surveillance as having the potential to cause "what is whispered in the closet to be proclaimed from the house-tops."

The words that this young attorney wrote might have slipped into obscurity were it not for the fact that 25 years later its author would ascend to the Supreme Court, where, as Justice Brandeis, he would take the concepts from this law review article and use them to argue for a constitutional right to privacy. In a dissenting opinion in the case *Olmstead v. United States*, Justice Brandeis wrote:

> The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness . . . They conferred, as against the Government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men. To protect that right, every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment.

This text, appearing in a dissenting opinion, was not binding upon the courts, but it has surfaced many times over the years in arguments establishing a right to privacy as that right "to be let alone." Recently, the 2018 majority opinion of the court in *Carpenter v. United States* cited *Olmstead* in an opinion declaring warrantless searches of cell phone location records unconstitutional, saying:

> As Justice Brandeis explained in his famous dissent, the Court is obligated as "[s]ubtler and more far-reaching means of invading privacy have become available to the Government"—to ensure that the "progress of science" does not erode Fourth Amendment protections. Here the progress of science has afforded law enforcement a powerful new tool to carry out its important responsibilities. At the same time, this tool risks Government encroachment of the sort the Framers, "after consulting the lessons of history," drafted the Fourth Amendment to prevent.

This is just one example of many historical precedents that firmly establish a right to privacy in U.S. law and allow the continued reinterpretation of that right in the context of technologies and tools that the authors of the Constitution could not possibly have imagined.

What Is Privacy?

It would certainly be difficult to start a book on privacy without first defining the word *privacy*, but this is a term that eludes a common definition in today's environment. Legal and privacy professionals who are asked this question often harken back to the words of Justice Brandeis, describing privacy simply as the right "to be let alone."

In their Generally Accepted Privacy Principles (GAPP), the American Institute of Certified Public Accountants (AICPA) offers a more hands-on definition, describing privacy as "the rights and obligations of individuals and organizations with respect to the collection, use, retention, disclosure, and destruction of personal information."

The GAPP definition may not be quite as pithy and elegant as Justice Brandeis's right "to be let alone," but it does provide privacy professionals with a better working definition that they can use to guide their privacy programs, so it is the definition that we will adopt in this book.

What Is Personal Information?

Now that we have privacy defined, we're led to another question. If privacy is about the protection of *personal information*, what information fits into this category? Here, we turn our attention once again to GAPP, which defines personal information as "information that is or can be about or related to an identifiable individual."

More simply, if information is about a person, that information is personal information as long as you can identify the person that it is about. For example, the fairly innocuous statement "Mike Chapple and Joe Shelley wrote this book" fits the definition of personal information. That personal information might fall into the public domain (after all, it's on the cover of this book!), but it remains personal information.

You'll often hear the term *personally identifiable information (PII)* used to describe personal information. The acronym PII is commonly used in privacy programs as a shorthand notation for all personal information.

Of course, not all personal information is in the public domain. There are many other types of information that fit into this category that most people would consider private. Our bank balances, medical records, college admissions test scores, and email communications are all personal information that we might hold sensitive. This information fits into the narrower category of *sensitive personal information (SPI)*. For example, the European Union's General Data Protection Regulation (GDPR) includes a listing of "special categories of personal data," which include

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data used for the purpose of uniquely identifying a natural person
- Health data
- Data concerning a natural person's sex life or sexual orientation

The GDPR uses this list to create special boundaries and controls around the categories of information that EU lawmakers found to be most sensitive.

What Isn't Personal Information?

With a working knowledge of personal information under our belts, it's also important to make sure that we have a clear understanding about what types of information do not fit the definition of personal information and, therefore, fall outside the scope of privacy programs.

First, clearly, if information is not about a person, it is not personal information. Information can be sensitive but not personal. For example, a business's product development plans or a military unit's equipment list might both be very sensitive, but they aren't about people, so they don't fit the definition of personal information and would not be included within the scope of a privacy program.

Second, information is not personal information if it does not provide a way to identify the person that the information is about. For example, consider the height and weight information presented in Table 1.1.

TABLE 1.1 Height and weight information

Name	Age	Gender	Height	Weight
Mary Smith	43	F	5′9″	143 lbs
Matt Jones	45	M	5′11″	224 lbs
Kevin Reynolds	32	M	5′10″	176 lbs

This information clearly fits the definition of personal information. But what if we remove the names from this table, as shown in Table 1.2?

TABLE 1.2 Anonymized height and weight information

Age	Gender	Height	Weight
43	F	5′9″	143 lbs
45	M	5′11″	224 lbs
32	M	5′10″	176 lbs

Here, we have a set of information that is about an individual, but it doesn't seem to be about an *identifiable* individual, making it fall outside the definition of personal information. However, we must be careful here. What if this table was known to be the information about

individuals in a certain department? If Mary Smith is the only 43-year-old female in that department, it would be trivial to determine that the first row contains her personal information, making it once again identifiable information.

This leads us to the concept of *anonymization*, the process of taking personal information and making it impossible to identify the individual to whom the information relates. As illustrated in our height and weight example, simply removing names from a table of data does not necessarily anonymize that data. Anonymization is actually a quite challenging problem and requires the expertise of privacy professionals.

The U.S. Department of Health and Human Services (HHS) publishes a de-identification standard that may be used to render information unidentifiable using two different techniques:

The HHS de-identification standards cover medical records, so they include fields specific to medical records. You may use them as general guidance for the de-identification of other types of record, but you must also supplement them with industry-specific fields that might identify an individual. You can read the full HHS de-identification standard at `www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html#standard`.

- *Expert determination* requires the involvement of a trained statistician who analyzes a de-identified dataset and determines that there is very little risk that the information could be used to identify an individual, even if that information is combined with other publicly available information.
- *Safe harbor* requires the removal of 18 different types of information to remove direct and indirect links to an individual. These include
  - Names
  - Geographic divisions and ZIP codes containing fewer than 20,000 people
  - The month and day of a person's birth, death, hospital admission or discharge or the age in years of a person over 89
  - Telephone numbers
  - Vehicle identifiers and serial numbers, including license plate numbers
  - Fax numbers
  - Device identifiers and serial numbers
  - Email addresses
  - Web URLs
  - Social Security numbers
  - IP addresses
  - Medical record numbers
  - Biometric identifiers, including finger and voice prints

- Health plan beneficiary numbers
- Full-face photographs and any comparable images
- Account numbers
- Any other uniquely identifying number, characteristic, or code
- Certificate/license numbers

We will cover how this standard fits into the broader requirements of the Health Insurance Portability and Accountability Act (HIPAA) in Chapter 5, "Private Sector Data Collection." We only discuss it here as an example of the difficulty of anonymizing personal information.

Closely related to anonymization is the process of *aggregation*, summarizing data about a group of individuals in a manner that makes it impossible to draw conclusions about a single person. For example, we might survey all the students at a university and ask them their height and weight. If the students include any identifying information on their survey responses, those individual responses are clearly personal information. However, if we provide the summary table shown in Table 1.3, the information has been aggregated to an extent that renders it nonpersonal information. There is no way to determine the height or weight of an individual student from this data.

TABLE 1.3 Aggregated height and weight information

Gender	Average Height	Average Weight
F	5′5″	133 lbs
M	5′10″	152 lbs

Why Should We Care About Privacy?

Protecting privacy is hard work. Privacy programs require that organizations invest time and money in an effort that does not necessarily provide a direct financial return on that investment. This creates an opportunity cost, as those resources could easily be deployed in other areas of the organization to have a direct impact on the mission. Why, then, should organizations care about privacy?

Privacy is an ethical obligation. Organizations that are the custodians of personal information have a moral and ethical obligation to protect that information against unauthorized disclosure or use.

Laws and regulations require privacy protections. Depending on the nature of an organization's operations and the jurisdiction(s) where it operates, it may face legal and contractual obligations to protect privacy. Much of this book is dedicated to exploring these obligations.

Poor privacy practices reflect poorly on an organization. The failure to protect privacy presents a reputational risk to the organization, which may suddenly find its poor privacy practices covered on the front page of the *Wall Street Journal*. The reputational impact of a privacy lapse may have a lasting impact on the organization.

Generally Accepted Privacy Principles

Now that you have a basic understanding of the types of information covered by a privacy program and the reasons that organizations pay particular attention to protecting the privacy of personal information, we can start to explore the specific goals of a privacy program. These goals answer the question "What do we need to do to protect privacy?"

The *Generally Accepted Privacy Principles (GAPP)* are an attempt to establish a global framework for privacy management. GAPP includes 10 principles that were developed as a joint effort between two national accounting organizations: AICPA and the Canadian Institute of Chartered Accountants (CICA). These two organizations sought expert input to develop a set of commonly accepted privacy principles.

The 10 GAPP principles are

1. Management
2. Notice
3. Choice and consent
4. Collection
5. Use, retention, and disposal
6. Access
7. Disclosure to third parties
8. Security for privacy
9. Quality
10. Monitoring and enforcement

The remainder of this section explores each of these principles in more detail.

Exam Note

GAPP is one of many frameworks designed to help privacy professionals articulate the goals of their privacy programs and industry best practices. Other similar frameworks include the Fair Information Practice Principles (FIPPs) and the Organisation for Economic Co-operation and Development's Privacy Guidelines.

We present GAPP to you in this chapter as a framework to help you understand the basic requirements of privacy programs. The GAPP principles are not included in the CIPP/US exam objectives, so you shouldn't see exam questions specifically covering them.

You will see many of these principles come up repeatedly in federal, state, and international laws that *are* covered by the exam objectives, so expect to see questions covering these concepts, just not in the context of GAPP.

Management

Management is the first of the 10 privacy principles, and GAPP defines it as follows: "The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures." The GAPP standard then goes on to list a set of criteria that organizations should follow to establish control over the management of their privacy program.

These criteria include

- Creating written privacy policies and communicating those policies to personnel
- Assigning responsibility and accountability for those policies to a person or team
- Establishing procedures for the review and approval of privacy policies and changes to those policies
- Ensuring that privacy policies are consistent with applicable laws and regulations
- Performing privacy risk assessments on at least an annual basis
- Ensuring that contractual obligations to customers, vendors, and partners are consistent with privacy policies
- Assessing privacy risks when implementing or changing technology infrastructure
- Creating and maintaining a privacy incident management process
- Conducting privacy awareness and training and establishing qualifications for employees with privacy responsibilities

Notice

The second GAPP principle, *notice*, requires that organizations inform individuals about their privacy practices. GAPP defines notice as follows: "The entity provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained, and disclosed."

The notice principle incorporates the following criteria:

- Including notice practices in the organization's privacy policies
- Notifying individuals about the purpose of collecting personal information and the organization's policies surrounding the other GAPP principles

- Providing notice to individuals at the time of data collection, when policies and procedures change, and when the organization intends to use information for new purposes not disclosed in earlier notices
- Writing privacy notices in plain and simple language and posting it conspicuously

Choice and Consent

Choice and consent is the third GAPP principle, allowing individuals to retain control over the use of their personal information. GAPP defines choice and consent as follows: "The entity describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, and disclosure of personal information."

The criteria associated with the principle of choice and consent are as follows:

- Including choice and consent practices in the organization's privacy policies
- Informing individuals about the choice and consent options available to them and the consequences of refusing to provide personal information or withdrawing consent to use personal information
- Obtaining implicit or explicit consent at or before the time that personal information is collected
- Notifying individuals of proposed new uses for previously collected information and obtaining additional consent for those new uses
- Obtaining direct explicit consent from individuals when the organization collects, uses, or discloses sensitive personal information
- Obtaining consent before transferring personal information to or from an individual's computer or device

Collection

The principle of *collection* governs the ways that organizations come into the possession of personal information. GAPP defines this principle as follows: "The entity collects personal information only for the purposes identified in the notice."

The criteria associated with the collection principle are as follows:

- Including collection practices in the organization's privacy policies
- Informing individuals that their personal information will only be collected for identified purposes
- Including details on the methods used to collect data and the types of data collected in the organization's privacy notice
- Collecting information using fair and lawful means and only for the purposes identified in the privacy notice

- Confirming that any third parties that provide the organization with personal information have collected it fairly and lawfully and that the information is reliable
- Informing individuals if the organization obtains additional information about them

Use, Retention, and Disposal

Organizations must maintain the privacy of personal information throughout its lifecycle. That's where the principle of *use, retention, and disposal* plays an important role. GAPP defines this principle as follows: "The entity limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. The entity retains personal information for only as long as necessary to fulfill the stated purposes or as required by law or regulations and thereafter appropriately disposes of such information."

The criteria associated with the use, retention, and disposal principle are as follows:

- Including collection practices in the organization's privacy policies
- Informing individuals that their personal information will only be used for disclosed purposes for which the organization has obtained consent and then abiding by that statement
- Informing individuals that their data will be retained for no longer than necessary and then abiding by that statement
- Informing individuals that information that is no longer needed will be disposed of securely and then abiding by that statement

Access

One of the core elements of individual privacy is the belief that individuals should have the right to access information that an organization holds about them and, when necessary, to correct that information. The GAPP definition of the *access* principle as follows: "The entity provides individuals with access to their personal information for review and update."

The criteria associated with the access principle are as follows:

- Including practices around access to personal information in the organization's privacy policies
- Informing individuals about the procedures for reviewing, updating, and correcting their personal information
- Providing individuals with a mechanism to determine whether the organization maintains personal information about them and to review any such information
- Authenticating an individual's identity before providing them with access to personal information

- Providing access to information in an understandable format within a reasonable period of time and either for a reasonable charge that is based on the organization's actual costs or at no cost
- Informing individuals in writing why any requests to access or update personal information were denied and informing them of any appeal rights they may have
- Providing a mechanism for individuals to update or correct personal information and providing that updated information to third parties that received it from the organization

Disclosure to Third Parties

Some challenging privacy issues arise when organizations maintain personal information about an individual and then choose to share that information with third parties in the course of doing business. GAPP defines the *disclosure to third parties* principle as follows: "The entity discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual."

The criteria associated with the disclosure to third parties principle are as follows:

- Including third-party disclosure practices in the organization's privacy policies
- Informing individuals of any third-party disclosures that take place and the purpose of those disclosures
- Informing third parties that receive personal information from the organization that they must comply with the organization's privacy policy and handling practices
- Disclosing personal information to third parties without notice or for purposes other than those disclosed in the notice only when required to do so by law
- Disclosing information to third parties only under the auspices of an agreement that the third party will protect the information consistent with the organization's privacy policy
- Implementing procedures designed to verify that the privacy controls of third parties receiving personal information from the organization are functioning effectively
- Taking remedial action when the organization learns that a third party has mishandled personal information shared by the organization

Security for Privacy

Protecting the security of personal information is deeply entwined with protecting the privacy of that information. Organizations can't provide individuals with assurances about the handling of personal data if they can't protect that information from unauthorized access. GAPP defines *security for privacy* as follows: "The entity protects personal information against unauthorized access (both physical and logical)." We will revisit this topic in more detail later in this chapter.

The criteria associated with the security for privacy principle are as follows:

- Including security practices in the organization's privacy policies
- Informing individuals that the organization takes precautions to protect the privacy of their personal information
- Developing, documenting, and implementing an information security program that addresses the major privacy-related areas of security listed in ISO 27002:
  - Risk assessment and treatment
  - Security policy
  - Organization of information security
  - Asset management
  - Human resources security
  - Physical and environmental security
  - Communications and operations management
  - Access control
  - Information systems acquisition, development, and maintenance
  - Information security incident management
  - Business continuity management
  - Compliance

This list includes the ISO 27002 elements that are relevant to privacy efforts and, therefore, our discussion. ISO 27002 does include other recommended security controls that fall outside the scope of a privacy effort.

- Restricting logical access to personal information through the use of strong identification, authentication, and authorization practices
- Restricting physical access to personal information through the use of physical security controls
- Protecting personal information from accidental disclosure due to natural disasters and other environmental hazards
- Applying strong encryption to any personal information that is transmitted over public networks
- Avoiding the storage of personal information on portable media, unless absolutely necessary, and using encryption to protect any personal information that must be stored on portable media
- Conducting periodic tests of security safeguards used to protect personal information

Quality

When we think about the issues associated with protecting the privacy of personal information, we often first think about issues related to the proper collection and use of that information along with potential unauthorized disclosure of that information. However, it's also important to consider the accuracy of that information. Individuals may be damaged by incorrect information just as much, if not more, than they might be damaged by information that is improperly handled. The GAPP *quality* principle states that "The entity maintains accurate, complete, and relevant personal information for the purposes identified in the notice."

The criteria associated with the quality principle are as follows:

- Including data quality practices in the organization's privacy policies
- Informing individuals that they bear responsibility for providing the organization with accurate and complete personal information and informing the organization if corrections are required
- Maintaining personal information that is accurate, complete, and relevant for the purposes for which it will be used

Monitoring and Enforcement

Privacy programs are not a one-time project. It's true that organizations may make a substantial initial investment of time and energy to build up their privacy practices, but those practices must be monitored over time to ensure that they continue to operate effectively and meet the organization's privacy obligations as business needs and information practices evolve. The GAPP *monitoring and enforcement* principle states that "The entity monitors compliance with its privacy policies and procedures and has procedures to address privacy related inquires, complaints, and disputes."

The criteria associated with the monitoring and enforcement principle are as follows:

- Including monitoring and enforcement practices in the organization's privacy policies
- Informing individuals about how they should contact the organization if they have questions, complaints, or disputes regarding privacy practices
- Maintaining a dispute resolution process that ensures that every complaint is addressed and that the individual who raised the complaint is provided with a documented response
- Reviewing compliance with privacy policies, procedures, laws, regulations, and contractual obligations on an annual basis
- Developing and implementing remediation plans for any issues identified during privacy compliance reviews
- Documenting cases where privacy policies were violated and taking any necessary corrective action
- Performing ongoing monitoring of the privacy program based on a risk assessment

Developing a Privacy Program

At this point in the chapter, you should have a reasonable understanding of the fact that privacy issues are both complex and nuanced. There are no "quick fix" solutions to protecting the privacy of personal information. Organizations developing a privacy program for the first time will need to expend considerable effort designing that program, implementing appropriate privacy controls, and monitoring the program's ongoing effectiveness to ensure that it continues to meet the organization's legal obligations and privacy objectives.

Crafting Strategy, Goals, and Objectives

At the outset of a privacy initiative, senior leadership should outline the purpose, strategy, and goals of the privacy program. These provide the high-level direction that those implementing the program will need to guide their efforts. For example, the U.S. Department of Commerce (DOC) offers the following mission statement for their privacy program:

> The DOC is committed to safeguarding personal privacy. Individual trust in the privacy and security of personally identifiable information is a foundation of trust in government and commerce in the 21st Century. As an employer, a collector of data on millions of individuals and companies, the developer of information management standards and a federal advisor on information management policy, the Department strives to be a leader in best privacy practices and privacy policy. To further this goal, the Department assigns a high priority to privacy consideration in all systems, programs, and policies.

That's a very high-level statement that clearly explains the purpose of the program. Notice that it doesn't contain any specific objectives or measures. The privacy obligations and controls used by the DOC might change over time, but it is very likely that this strategic-level mission statement will remain appropriate (at least through the end of the 21st century!). The program document also contains goals that the DOC has to guide the execution of a privacy program in support of its mission. The four goals of its plan are as follows:

1. Foster a culture of privacy and disclosure and demonstrate leadership through policy and partnerships.
2. Provide outreach, education, training, and reports in order to promote privacy and transparency.
3. Conduct robust compliance and oversight programs to ensure adherence with federal privacy and disclosure laws and policies in all DOC activities.
4. Develop and maintain the best privacy and disclosure professionals in the federal government.

These goals now start to get into the details of *how* the DOC will carry out its privacy mission. They provide four key deliverables that privacy officials can then use to align their work with the DOC's strategy.

Underneath each of these goals, the DOC then provides a series of specific objectives that will satisfy each goal. These are the activities that the DOC plans to undertake to meet its goal and, therefore, achieve the privacy program's strategic purpose. For brevity's sake, we won't cover all the objectives in this book, but let's take a look at the four objectives that align with the DOC's third privacy goal to conduct robust compliance and oversight programs:

1. Review, assess, and provide guidance to DOC programs, systems, projects, information sharing arrangements, and other initiatives to reduce the impact on privacy and ensure compliance.
2. Promote privacy best practices and guidance to the DOC's information sharing and intelligence activities.
3. Ensure that complaints and incidents at DOC are reported systematically, processed efficiently, and mitigated appropriately in accordance with federal and DOC privacy policies and procedures.
4. Evaluate DOC programs and activities for compliance with privacy and disclosure laws.

These objectives are highly specific, and you might imagine them being handed to a middle manager to execute. They also might change much more frequently than the program's high-level purpose in order to meet the changing needs of the DOC.

Throughout this section, we draw examples from the Department of Commerce's Privacy Plan. If you'd like to review this plan in more detail, you can download it from `osec.doc.gov/opog/privacy/Memorandums/PRIVACY_PROGRAM_PLAN_2017.pdf`.

Appointing a Privacy Official

Organizations should appoint a senior leader with overall responsibility for the organization's privacy program. This establishes senior-level accountability for the program's success and provides the privacy program a seat at the executive table. This role is commonly referred to as an organization's *chief privacy officer (CPO)*, although it may also be implemented using other titles, such as director of privacy or privacy program manager.

In the DOC Privacy Plan that we have been using as an example in this section, the department identifies a position within the office of the Secretary of Commerce as the DOC's chief privacy officer. The program includes a detailed set of responsibilities for this position. Here is an abbreviated set of those responsibilities, paraphrased for brevity:

- Serve as the senior privacy policy authority
- Develop and oversee implementation of privacy policies

- Communicate the privacy vision, principles, and policy internally and externally
- Ensure the department complies with applicable privacy laws and regulations
- Advocate privacy-preserving strategies for information collection and dissemination
- Manage privacy risks
- Ensure employees and contractors receive appropriate privacy training
- Facilitate relationships with senior DOC leaders, other federal agencies, and private industry

Of course, the DOC is a very large organization, and it would be impossible for one person to be involved in all aspects of its privacy program in any type of thorough manner. For this reason, the DOC policy also specifies that each operating unit should have its own CPO and that those CPOs should meet regularly as the Department of Commerce Privacy Council.

This type of hierarchical privacy authority is common in government agencies and other large organizations. It may not be necessary in smaller organizations, depending on the nature of the organization and the scope of its privacy program. Some organizations opt to use the role of "privacy liaisons" distributed throughout the organization. These liaisons serve as the primary point of privacy contact for their organization and work directly with the CPO office. Depending on the size of the unit they serve, the liaison role may be a full-time position or a secondary responsibility for someone in another primary role.

Privacy Roles

Depending on the nature of an individual or organization's involvement in the collection and processing of information, they may take on one or more data roles. The three primary roles are as follows:

- *Data subjects* are the individuals about whom personal information is collected. These may be the customers or employees of an organization or any other individuals about whom the organization collects personal information.
- *Data controllers* are the organizations that determine the purposes and means of collecting personal information from data subjects. If an organization collects and/or processes personal information for its own business needs, it is a data controller. It remains a data controller even if it outsources some of that collection or processing to service providers.
- *Data processors* are service providers that collect or process personal information on behalf of data controllers. For example, cloud service providers often serve in the role of data processor for their customers.

These terms take on particular importance when interpreting how laws and regulations apply to an organization. For example, some regulations allow data controllers to transfer some privacy and security responsibility to service providers, as long as the controller chooses a service provider that has gone through a certification process. Regulations, including the EU's GDPR, may also have very specific definitions of these terms, as you will discover later in this book as we explore those regulations in more detail.

Building Inventories

Once an organization has established accountable officials and privacy roles, the next step in developing a privacy program is to create a comprehensive inventory of the personal information that the organization collects, processes, and maintains and the systems, storage locations, and processes involved in those activities.

This inventory may take many different forms, depending on the nature of the organization and the level of formality desired. The end goal is for the organization to have a clear picture of the personal information that it handles and the locations where that information is stored and processed. This inventory should be maintained as a living repository of data updated when privacy practices change. It may then be used as the basis for conducting privacy assessments and implementing privacy controls.

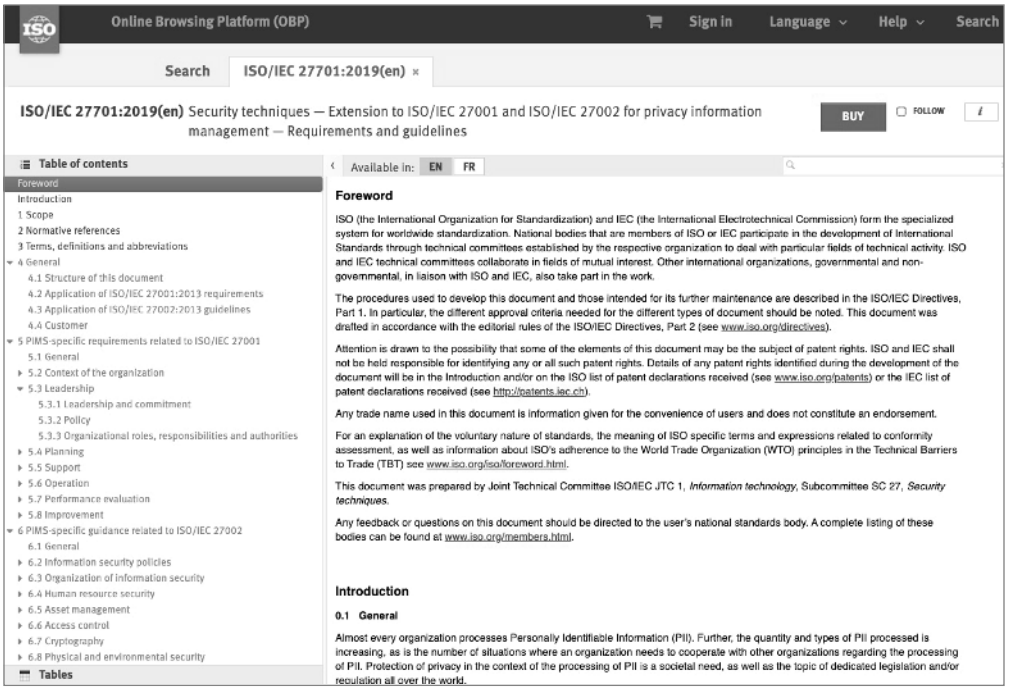
Information security programs also depend on a similar inventory of all sensitive information maintained by the organization. The information included in a privacy-focused inventory is a subset of that sensitive information inventory. This offers an excellent opportunity for privacy and information security programs to partner and avoid redundant activity by simply including a personal information tag in the broader sensitive information inventory.

Conducting a Privacy Assessment

With a personal information inventory in hand, the organization may now turn to an assessment of the current state of its privacy program. This assessment should use a standard set of privacy practices, derived from either an industry standard framework or the regulatory requirements facing the organization. The remainder of this book will dive deeply into many of these frameworks and requirements.

For example, an organization might choose to adopt the privacy framework from the International Organization for Standardization titled "Security techniques—Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management—Requirements and guidelines" and documented in ISO 27701. An excerpt from this document appears in Figure 1.1.

FIGURE 1.1 Excerpt from ISO 27701



ISO 27701 is closely linked to ISO 27001 and 27002, the two ISO standards governing information security. This is another opportunity to align the interests of privacy and security programs. Annex F of ISO 27701 provides advice on applying the privacy standard in an organization that already uses the information security standards. These standards are also tightly linked to the National Institute for Standards and Technology's Cybersecurity Framework (CSF), allowing organizations to cleanly map controls between standards and frameworks that they adopt for both privacy and security.

The end result of the privacy assessment should be a *gap analysis* that identifies any places where the organization's current practices do not meet the level of control desired by the standard under which the assessment was performed. This gap analysis may then be used in remediation efforts to bring the organization up to the desired level of privacy performance.

Implementing Privacy Controls

The primary means that the organization uses to remediate privacy deficiencies is the implementation of *privacy controls* that are technical or administrative measures that improve privacy. For example, implementing mechanisms that fulfill the many GAPP criteria discussed earlier in this chapter qualify as privacy controls. Here are some examples of common privacy controls:

- Creation, review, or modification of privacy policies
- Use of encryption to protect personal information
- Purging personal information when it is no longer needed to meet the purposes disclosed when it was collected
- Configuring access controls to limit the use of personal information to authorized individuals
- Implementing and maintaining a process to manage user privacy preferences
- Developing a standard process for investigating privacy complaints and following up on potential privacy incidents
- Conducting periodic testing and assessment of the organization's privacy program

Notice that some, but not all, of these controls are technical in nature, but all the controls advance the organization's privacy efforts.

Ongoing Operation and Monitoring

Once a privacy program is well established, the organization should continue to operate the program and monitor its effectiveness. This is normally done through a combination of periodic reviews, regular updates to the privacy assessment, and dashboard-style monitoring of the program's key metrics, such as compliance with data retention and disposal standards, turnaround time for processing privacy requests, and the number and severity of privacy incidents.

Organizations may also find themselves the subject of *privacy audits* based on legal or regulatory requirements. Audits are similar to assessments in nature, because they compare the current state of the privacy program to an external standard. However, unlike assessments, audits are always performed by an independent auditor who does not have a vested interest in the outcome. Audits may be performed at the request of internal management, a board of directors, or regulatory authorities.

Online Privacy

Consumers often provide information to companies and organizations online. This may consist of *active data collection*, where the consumer directly fills out forms, or *passive data collection*, where the organization gathers information from the individual automatically when they visit a website or engage in other online activity.

An organization's privacy policy should apply to all online data collection, whether that collection is active or passive.

Privacy Notices

The *privacy notice* is the primary means that an organization uses to convey the details of its privacy policy to end users. The contents of this notice are often driven by regulatory requirements. For example, a data controller subject to the EU's GDPR might include the following:

- Contact information for the data controller and the controller's data protection officer (DPO)
- Purposes for which the organization collects personal information
- Description of the categories of data subjects from whom the organization collects information
- Description of the categories of personal information collected by the organization
- Categories of recipients to whom personal information has or will be disclosed
- Identification of any third countries or international organizations that will receive data and the safeguards put in place to protect those transfers
- Time limits for the erasure of different categories of data
- General descriptions of the technical and administrative security mechanisms used to protect personal information

Privacy notices must strike a balance between satisfying legal and ethical disclosure obligations and remaining readable to the layperson attempting to decipher the document. LinkedIn's privacy policy does an excellent job of balancing these two requirements by providing large-type summaries of each section written in plain language accompanied by the more detailed legal language of the policy. This approach, offering a brief summary of the privacy policy in plain language along with the detailed legalese, is known as a *layered privacy notice*.

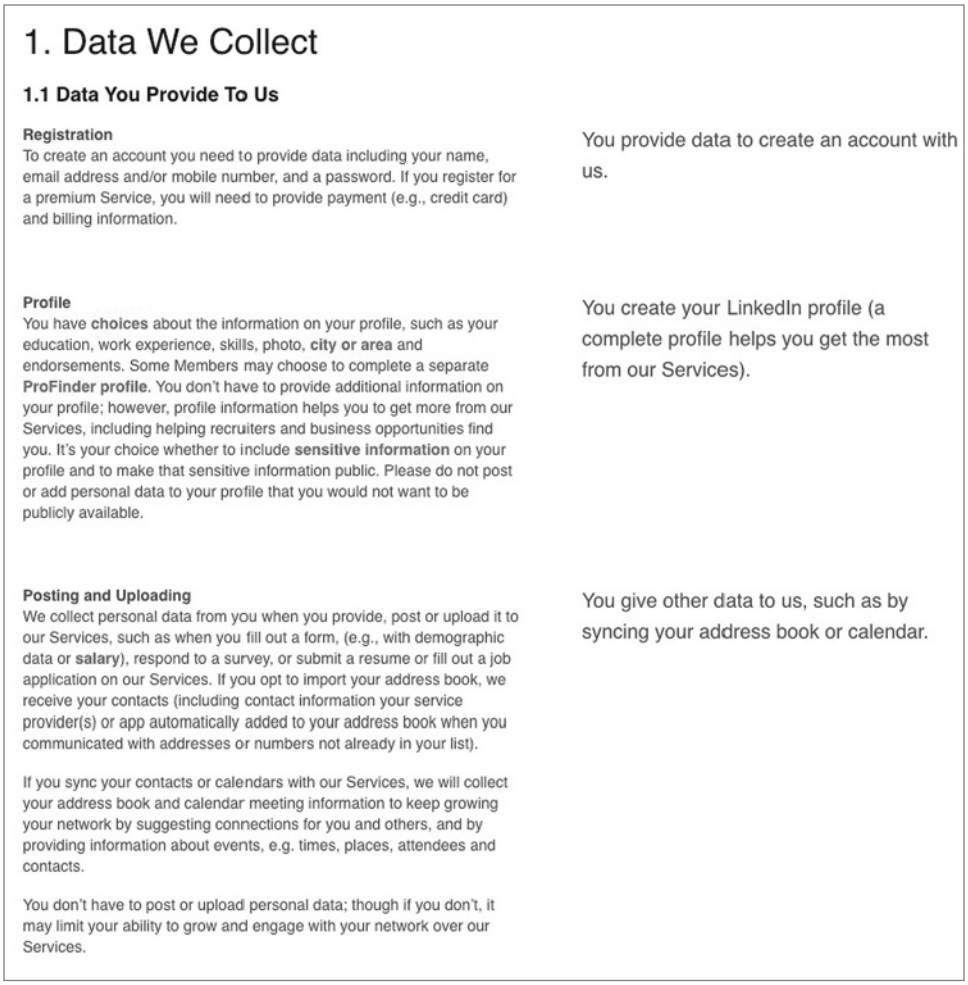
Figure 1.2 shows an excerpt illustrating the layered notice approach. You can view LinkedIn's entire policy at `www.linkedin.com/legal/privacy-policy`.

Privacy and Cybersecurity

The fields of privacy and cybersecurity are closely related and interdependent. This occurs to such an extent that many people who do not work in either field consider them the same. However, although these fields are related to each other, they remain separate and distinct.

As you've already read, the purpose of a privacy program is to safeguard the privacy rights that individuals have to their personal information. The purpose of a cybersecurity program is to protect the confidentiality, integrity, and availability of data maintained by an

FIGURE 1.2 Excerpt from the LinkedIn privacy policy



1. Data We Collect

1.1 Data You Provide To Us

Registration
To create an account you need to provide data including your name, email address and/or mobile number, and a password. If you register for a premium Service, you will need to provide payment (e.g., credit card) and billing information.

You provide data to create an account with us.

Profile
You have **choices** about the information on your profile, such as your education, work experience, skills, photo, **city or area** and endorsements. Some Members may choose to complete a separate **ProFinder profile**. You don't have to provide additional information on your profile; however, profile information helps you to get more from our Services, including helping recruiters and business opportunities find you. It's your choice whether to include **sensitive information** on your profile and to make that sensitive information public. Please do not post or add personal data to your profile that you would not want to be publicly available.

You create your LinkedIn profile (a complete profile helps you get the most from our Services).

Posting and Uploading
We collect personal data from you when you provide, post or upload it to our Services, such as when you fill out a form, (e.g., with demographic data or **salary**), respond to a survey, or submit a resume or fill out a job application on our Services. If you opt to import your address book, we receive your contacts (including contact information your service provider(s) or app automatically added to your address book when you communicated with addresses or numbers not already in your list).

If you sync your contacts or calendars with our Services, we will collect your address book and calendar meeting information to keep growing your network by suggesting connections for you and others, and by providing information about events, e.g. times, places, attendees and contacts.

You don't have to post or upload personal data; though if you don't, it may limit your ability to grow and engage with your network over our Services.

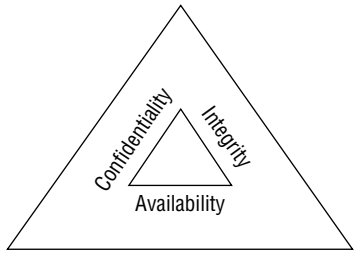
You give other data to us, such as by syncing your address book or calendar.

organization. Before we describe the relationship between the two, let's take a deeper look at the goals of a cybersecurity program.

Cybersecurity Goals

When most people think of cybersecurity, they imagine hackers trying to break into an organization's system and steal sensitive information, ranging from Social Security numbers and credit cards to top-secret military information. Although protecting sensitive information from unauthorized disclosure is certainly one element of a cybersecurity program, it is

FIGURE 1.3 The three key objectives of cybersecurity programs are confidentiality, integrity, and availability.



important to understand that cybersecurity actually has three complementary objectives, as shown in Figure 1.3.

Confidentiality ensures that unauthorized individuals are not able to gain access to sensitive information. Cybersecurity professionals develop and implement security controls, including firewalls, access control lists, and encryption, to prevent unauthorized access to information. Attackers may seek to undermine confidentiality controls to achieve one of their goals: the unauthorized disclosure of sensitive information.

Integrity ensures that there are no unauthorized modifications to information or systems, either intentionally or unintentionally. Integrity controls, such as hashing and integrity monitoring solutions, seek to enforce this requirement. Integrity threats may come from attackers seeking the alteration of information without authorization or nonmalicious sources, such as a power spike causing the corruption of information.

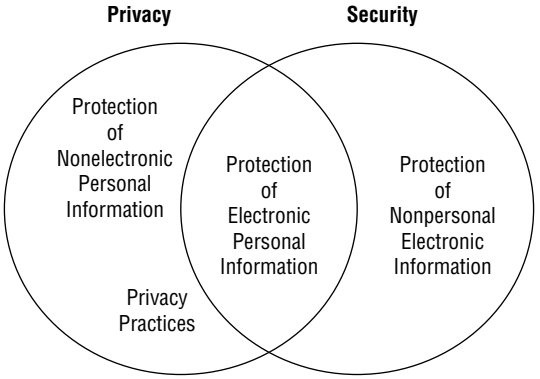
Availability ensures that information and systems are ready to meet the needs of legitimate users at the time those users request them. Availability controls, such as fault tolerance, clustering, and backups, seek to ensure that legitimate users may gain access as needed. Similar to integrity threats, availability threats may come either from attackers seeking the disruption of access or nonmalicious sources, such as a fire destroying a datacenter that contains valuable information or services.

Cybersecurity analysts often refer to these three goals, known as the CIA Triad, when performing their work. They often characterize risks, attacks, and security controls as meeting one or more of the three CIA Triad goals when describing them.

Relationship Between Privacy and Cybersecurity

Now that you have a good understanding of the nature of privacy and security programs, you may already be developing a sense of the relationship between the two. Privacy depends on cybersecurity. In fact, you've already read that security for privacy is one of the 10 GAPP principles. The bottom line is that you can't protect the privacy of information unless you can guarantee the security of that information.

FIGURE 1.4 The relationship between privacy and security



The relationship is more complex than that, however, as shown in Figure 1.4.

Cybersecurity and privacy programs share a common goal: the protection of electronic personal information. They each also have their own independent goals.

Privacy programs must also concern themselves with the protection of nonelectronic personal information, such as paper records. They also must be concerned about all 10 GAPP principles, not just security. Principles such as notice, choice and consent, and quality generally fall outside the scope of security programs.

Security programs concern themselves with the confidentiality, integrity, and availability of *all* sensitive electronic information. This includes sensitive, but nonpersonal, information, such as business plans, trade secrets, and product designs.

All differences aside, privacy and cybersecurity are close cousins in the business world. Privacy and security professionals often share a common ethos and understanding of each other's work, but it is also important that they understand the fundamental differences between their goals.

Privacy by Design

The discipline of *Privacy by Design* seeks to incorporate strong privacy practices into the design and implementation of technology systems, rather than seeking to "bolt on" privacy controls after a system is already in place. This approach leads to more effective privacy controls, more efficient design and implementation processes, and reduced rework.

Ann Cavoukian, the Information and Privacy Commissioner of Ontario, Canada, developed the concept of Privacy by Design and outlined seven foundational principles that are crucial to ensuring that individuals retain control over their personal information:

1. *Proactive, Not reactive; preventive, Not remedial*. Systems should be designed to prevent privacy risks from occurring in the first place, not to respond to privacy lapses that do occur.

2. *Privacy as the default setting*. Systems should protect the privacy of individuals even if they do not act in any way. The default approach of any system should be to protect privacy unless the user specifically chooses to take actions that reduce the level of privacy.
3. *Privacy embedded into design*. Privacy should be a primary design consideration, not a "bolted-on" afterthought. Privacy is a core requirement of the system.
4. *Full functionality—positive-sum, Not zero-sum*. Privacy should not be treated as requiring trade-offs with the business, security, or other objectives. Privacy by Design seeks "win-win" situations where privacy objectives may be achieved alongside other objectives.
5. *End-to-end security—full lifecycle protection*. Security practices should persist throughout the entire information lifecycle. Information should be securely collected, retained, and disposed of to preserve individual privacy.
6. *Visibility and transparency—Keep it open*. The component parts of systems preserving Privacy by Design should be open for inspection by users and providers alike.
7. *Respect for user privacy—Keep it user-centric*. Privacy is about protecting personal information and personal information belongs to individuals. Therefore, Privacy by Design practices maintain a focus on the individual, empowering data subjects with user-friendly privacy practices.

The principles of Privacy by Design offer an outstanding starting point for integrating privacy thinking into a systems engineering practice.

Summary

Privacy is a complex undertaking, requiring that organizations put careful thought into the nature of the personal information that they collect and process and the controls used to safeguard that information. The Generally Accepted Privacy Principles (GAPP) outline 10 principles that organizations should consider when designing their privacy programs: management; notice; choice and consent; collection; use, retention, and disposal; access; disclosure to third parties; security for privacy; quality; and monitoring and enforcement.

Organizations should consider these principles when designing privacy controls. These controls should remediate gaps discovered during privacy assessments and bring the organization up to an acceptable level of privacy practice. Ongoing audits and assessments ensure that those controls continue to operate effectively.

Exam Essentials

Know how to designate a senior individual accountable for the privacy program. Placing responsibility for the design, implementation, maintenance, and monitoring of a privacy program in the hands of a senior official provides direct accountability for the program's

goals and objectives. Organizations commonly designate a chief privacy officer (CPO) to hold these responsibilities, and that CPO may also serve as the organization's point of contact for privacy regulators.

Be able to develop a privacy program designed to achieve the organization's privacy mission. Privacy programs consist of the policies, procedures, tools, and practices used to achieve the desired level of privacy in an organization. Privacy programs should have a high-level strategic purpose/mission that is mapped to more tactical goals and even more specific objectives for achieving those goals. The purpose of a privacy program should change infrequently, whereas goals and objectives may change more frequently.

Understand that privacy programs should have strong processes for managing user preferences. Abiding by the principle of choice and consent requires that privacy programs acknowledge user preferences for the handling of their personal information. This requires implementing procedures and mechanisms that allow users to state those preferences and for the organization to track and honor them. These activities are good privacy practices and may be required by law in some jurisdictions and industries.

Know how organizations should protect consumer privacy online and disclose their privacy practices. Privacy notices are the primary means that an organization uses to communicate its privacy practices to data subjects. These privacy notices should be posted conspicuously on the organization's website and written in plain language accessible to the data subjects.

Review Questions

1. Which of the following types of information should be protected by a privacy program?
   - **A.** Customer records
   - **B.** Product plans
   - **C.** Trade secrets
   - **D.** All of the above

2. Barry is consulting with his organization's cybersecurity team on the development of their cybersecurity program. Which one of the following would not be a typical objective of such a program?
   - **A.** Privacy
   - **B.** Confidentiality
   - **C.** Availability
   - **D.** Integrity

3. Howard is assisting his firm in developing a new privacy program and wants to incorporate a privacy risk assessment process into the program. If Howard wishes to comply with industry best practices, how often should the firm conduct these risk assessments?
   - **A.** Monthly
   - **B.** Semiannually
   - **C.** Annually
   - **D.** Biannually

4. Of the following fields, which fits into the "special categories of personal data" under GDPR?
   - **A.** Banking records
   - **B.** Union membership records
   - **C.** Educational records
   - **D.** Employment records

5. Katie is assessing her organization's privacy practices and determines that the organization previously collected customer addresses for the purpose of shipping goods and is now using those addresses to mail promotional materials. If this possibility was not previously disclosed, what privacy principle is the organization most likely violating?
   - **A.** Quality
   - **B.** Management
   - **C.** Notice
   - **D.** Security

6. Kara is the chief privacy officer of an organization that maintains a database of customer information for marketing purposes. What term best describes the role of Kara's organization with respect to that database?
   - **A.** Data subject
   - **B.** Data custodian
   - **C.** Data controller
   - **D.** Data processor

7. Richard would like to use an industry standard reference for designing his organization's privacy controls. Which one of the following ISO standards is best suited for this purpose?
   - **A.** ISO 27001
   - **B.** ISO 27002
   - **C.** ISO 27701
   - **D.** ISO 27702

8. Which of the following organizations commonly requests a formal audit of a privacy program?
   - **A.** Management
   - **B.** Board of directors
   - **C.** Regulators
   - **D.** All of the above

9. Which element of a privacy program is likely to remain unchanged for long periods of time?
   - **A.** Mission
   - **B.** Goals
   - **C.** Objectives
   - **D.** Procedures

10. Tonya is seeking to de-identify a set of records about her organization's customers. She is following the HHS guidelines for de-identifying records and is removing ZIP codes associated with small towns. What is the smallest population size for which she may retain a ZIP code?
    - **A.** 1,000
    - **B.** 2,000
    - **C.** 10,000
    - **D.** 20,000

11. Which one of the following statements is not correct about privacy best practices?
    - **A.** Organizations should maintain personal information that is accurate, complete, and relevant.
    - **B.** Organizations should inform data subjects of their privacy practices.
    - **C.** Organizations should retain a third-party dispute resolution service for handling privacy complaints.
    - **D.** Organizations should restrict physical and logical access to personal information.

12. Which one of the following is not a common responsibility for an organization's chief privacy officer?

A. Managing privacy risks

B. Encrypting personal information

C. Developing privacy policy

D. Advocating privacy strategies

13. When designing privacy controls, an organization should be informed by the results of what type of analysis?

A. Impact analysis

B. Gap analysis

C. Business analysis

D. Authorization analysis

14. Which one of the following is an example of active online data collection?

A. Users completing an online survey

B. Collecting IP addresses from website visitors

C. Tracking user activity with web cookies

D. Analyzing the geographic locations of site visitors

15. Which one of the following would not normally appear in an organization's privacy notice?

A. Types of information collected

B. Contact information for the data controller

C. Detailed descriptions of security controls

D. Categories of recipients to whom personal information is disclosed

16. Gwen is investigating a security incident where attackers deleted important medical records from a hospital's electronic system. There are no backups and the information was irretrievably lost. What cybersecurity goal was most directly affected?

A. Integrity

B. Privacy

C. Confidentiality

D. Availability

17. When creating his organization's privacy policy, Chris wrote a simplified version of the policy and placed it at the top of the document, following it with the legal detail. What term best describes this approach?

A. Layered policy

B. Filtered policy

C. Redacted policy

D. Condensed policy

18. Under the Privacy by Design philosophy, which statement is correct?

- **A.** Organizations should design systems to respond to privacy lapses that occur.
- **B.** Privacy should be treated as requiring trade-offs with business objectives.
- **C.** Organizations should strictly limit the disclosure of their privacy practices.
- **D.** Privacy should be embedded into design.

19. In what Supreme Court case did the term "right to be let alone" first appear?

- **A.** *Olmstead v. United States*
- **B.** *Carpenter v. United States*
- **C.** *Roe v. Wade*
- **D.** *Katz v. United States*

20. Matt wants to share some information gathered from student records but is concerned about disclosing personal information. To protect privacy, he discloses only a table of summary statistics about overall student performance. What technique has he used?

- **A.** Anonymization
- **B.** Deidentification
- **C.** Aggregation
- **D.** Redaction