IAPP CIPP-US Practice Questions

Shared by Humphrey on 17-08-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

What is an exception to the Electronic Communications Privacy Act of 1986 ban on interception of wire, oral and electronic communications?

Options:

A- Where one of the parties has given consent
B- Where state law permits such interception
C- If an organization intercepts an employee's purely personal call
D- Only if all parties have given consent

Answer:

A

Explanation:

The Electronic Communications Privacy Act of 1986 (ECPA) is a federal law that regulates the privacy of wire, oral, and electronic communications.The ECPA prohibits the intentional interception, use, or disclosure of such communications, unless authorized by law or by the consent of one of the parties to the communication12.The ECPA also provides exceptions for certain types of communications, such as those made in the normal course of business, those made for law enforcement purposes, or those made for foreign intelligence purposes12.

One of the exceptions to the ECPA ban on interception is where one of the parties has given consent. This means that if a person who is a party to a communication agrees to have it intercepted, the interception is lawful under the ECPA.Consent can be express or implied, depending on the circumstances and the expectations of the parties3. For example, if a person calls a customer service line and hears a recorded message that the call may be monitored or recorded, the person has impliedly consented to the interception of the call. However, if a person calls a friend and does not know that the friend has a third party listening in on the call, the person has not consented to the interception of the call.

Question 2

Question Type: MultipleChoice

Which federal agency plays a role in privacy policy, but does NOT have regulatory authority?

Options:

A- The Office of the Comptroller of the Currency.
B- The Federal Communications Commission.
C- The Department of Transportation.
D- The Department of Commerce.

Answer:

D

Explanation:

The Department of Commerce (DOC) plays a role in privacy policy by promoting the development and adoption of voluntary codes of conduct, standards, and best practices for the private sector, as well as facilitating cross-border data transfers through mechanisms such as the EU-U.S. Privacy Shield and the APEC Cross-Border Privacy Rules. However, the DOC does not have regulatory authority to enforce privacy laws or impose sanctions for privacy violations. The other agencies listed have some degree of regulatory authority over privacy issues within their respective domains. For example, the Office of the Comptroller of the Currency (OCC) supervises national banks and federal savings associations and enforces the GLBA privacy and security rules for these institutions. The Federal Communications Commission (FCC) regulates interstate and international communications and enforces the privacy and security rules for telecommunications carriers, broadband providers, and voice over internet protocol (VoIP) services. The Department of Transportation (DOT) oversees the transportation sector and enforces the privacy and security rules for airlines, travel agents, and other covered entities under the Aviation and Transportation Security Act (ATSA).Reference:

IAPP CIPP/US Certified Information Privacy Professional Study Guide, Chapter 1: Introduction to the U.S. Privacy Environment, Section 1.3: Federal Agencies with a Role in Privacy, p. 18-19

IAPP CIPP/US Body of Knowledge, Domain I: Introduction to the U.S. Privacy Environment, Objective I.B: Identify the major federal agencies with a role in privacy, Subobjective I.B.4: Identify the role of the Department of Commerce, p. 7

IAPP CIPP/US Exam Blueprint, Domain I: Introduction to the U.S. Privacy Environment, Objective I.B: Identify the major federal agencies with a role in privacy, Subobjective I.B.4: Identify the role of the Department of Commerce, p. 3

Question 3

Question Type: MultipleChoice

Which of the following laws is NOT involved in the regulation of employee background checks?

Options:

A- The Civil Rights Act.
B- The Gramm-Leach-Bliley Act (GLBA).
C- The U.S. Fair Credit Reporting Act (FCRA).
D- The California Investigative Consumer Reporting Agencies Act (ICRAA).

Answer:

B

Explanation:

The law that is not involved in the regulation of employee background checks is B. The Gramm-Leach-Bliley Act (GLBA). The GLBA is a federal law that regulates the privacy and security of financial information collected, used, or shared by financial institutions, such as banks, insurance companies, or securities firms. The GLBA does not apply to employee background checks, unless the employer is a financial institution that obtains financial information from a consumer reporting agency for employment purposes. In that case, the employer must comply with the GLBA's notice and opt-out requirements, as well as the FCRA's requirements for using consumer reports.Reference:

[IAPP CIPP/US Study Guide], Chapter 4: Workplace Privacy, pp. 113-114.

IAPP CIPP/US Body of Knowledge, Section IV: Workplace Privacy, Subsection A: Employee Privacy Expectations, Topic 3: Background Checks.

IAPP CIPP/US Practice Questions, Question 150.

Question 4

Question Type: MultipleChoice

Global Manufacturing Co's Human Resources department recently purchased a new software tool. This tool helps evaluate future candidates for executive roles by scanning emails to see what those candidates say and what is said about them. This provides the HR department with an automated ''360 review'' that lets them know how the candidate thinks and operates, what their peers and direct reports say about them, and how well they interact with each other.

What is the most important step for the Human Resources Department to take when implementing this new software?

Options:

A- Making sure that the software does not unintentionally discriminate against protected groups.
B- Ensuring that the software contains a privacy notice explaining that employees have no right to privacy as long as they are running this software on organization systems to scan email systems.
C- Confirming that employees have read and signed the employee handbook where they have been advised that they have no right to privacy as long as they are using the organization's systems, regardless of the protected group or laws enforced by EEOC.
D- Providing notice to employees that their emails will be scanned by the software and creating automated profiles.
U- S. Private-Sector Privacy, Third Editionby Peter P. Swire, DeBrae Kennedy-Mayo, Chapter 4, Section 4.2.1, pp. 97-98.
U- S. Private-Sector Privacy, Third Editionby Peter P. Swire, DeBrae Kennedy-Mayo, Chapter 6, Section 6.2.1, pp. 153-154.
IAPP CIPP/US Certified Information Privacy Professional Study Guideby Mike Chapple and Joe Shelley, Chapter 4, Section 4.1, pp. 113-114.
U- S. Private-Sector Privacy, Third Editionby Peter P. Swire, DeBrae Kennedy-Mayo, Chapter 5, Section 5.2.1, pp. 125-126.

Answer:

D

Explanation:

The most important step for the HR department to take when implementing this new software is to provide notice to employees that their emails will be scanned by the software and creating automated profiles. This is because the software involves the collection and use of personal information from employees, which may implicate their privacy rights and expectations. By providing notice, the HR department can inform employees about the purpose, scope, and consequences of the software, as well as their choices and rights regarding their data. Notice is also a key element of transparency and accountability, which are essential principles of privacy management. Providing notice can also help the HR department comply with various privacy laws and regulations that may apply to the software, such as the Electronic Communications Privacy Act (ECPA), the Stored Communications Act (SCA), the Fair Credit Reporting Act (FCRA), and state privacy laws. Notice can also help the HR department avoid potential legal risks and liabilities that may arise from the software, such as claims of invasion of privacy, breach of contract, or violation of employee rights.Reference:

Question 5

Question Type: MultipleChoice

SCENARIO

Please use the following to answer the next QUESTION:

A US-based startup company is selling a new gaming application. One day, the CEO of the company receives an urgent letter from a prominent EU-based retail partner. Triggered by an unresolved complaint lodged by an EU resident, the letter describes an ongoing investigation by a supervisory authority into the retailer's data handling practices.

The complainant accuses the retailer of improperly disclosing her personal data, without consent, to parties in the United States. Further, the complainant accuses the EU-based retailer of failing to respond to her withdrawal of consent and request for erasure of her personal dat

a. Your organization, the US-based startup company, was never informed of this request for erasure by the EU-based retail partner. The supervisory authority investigating the complaint has threatened the suspension of data flows if the parties involved do not cooperate with the investigation. The letter closes with an urgent request: ''Please act immediately by identifying all personal data received from our company.''

This is an important partnership. Company executives know that its biggest fans come from Western Europe; and this retailer is primarily responsible for the startup's rapid market penetration.

As the Company's data privacy leader, you are sensitive to the criticality of the relationship with the retailer.

Upon review, the data privacy leader discovers that the Company's documented data inventory is obsolete. What is the data privacy leader's next best source of information to aid the investigation?

Options:

A- Reports on recent purchase histories
B- Database schemas held by the retailer
C- Lists of all customers, sorted by country
D- Interviews with key marketing personnel

Answer:

D

Explanation:

The data privacy leader needs to identify all the personal data that the Company has received from the retailer, as well as the purposes, retention periods, and sharing practices of such data. Since the data inventory is obsolete, the data privacy leader cannot rely on it to provide accurate and complete information. Therefore, the next best source of information is to

interview the key marketing personnel who are responsible for the partnership with the retailer and the use of the personal data. The marketing personnel can provide insights into the data flows, the data categories, the data processing activities, and the data protection measures that the Company has implemented. They can also help the data privacy leader to locate the relevant documents, contracts, and records that can support the investigation.Reference:[IAPP CIPP/US Study Guide], Chapter 5: Data Management, p. 97-98;IAPP Privacy Tech Vendor Report, Data Mapping and Inventory, p. 9-10.

Question 6

Question Type: MultipleChoice

In which situation would a policy of ''no consumer choice'' or ''no option'' be expected?

Options:

A- When a job applicant's credit report is provided to an employer
B- When a customer's financial information is requested by the government
C- When a patient's health record is made available to a pharmaceutical company
D- When a customer's street address is shared with a shipping company

Answer:

B

Explanation:

According to the Family Educational Rights and Privacy Act (FERPA), a policy of ''no consumer choice'' or ''no option'' means that an educational agency or institution may disclose personally identifiable information (PII) from education records without the prior written consent of the parent or eligible student, subject to certain conditions and exceptions1.One of the exceptions is when the disclosure is to comply with a judicial order or lawfully issued subpoena, or to respond to an ex parte order from the Attorney General of the United States or his designee in connection with the investigation or prosecution of terrorism crimes12.In such cases, the educational agency or institution must make a reasonable effort to notify the parent or eligible student of the order or subpoena in advance of compliance, unless the order or subpoena specifies not to do so12.Therefore, when a customer's financial information, which may be part of the education records, is requested by the government under a valid legal authority, the customer does not have the option to prevent the disclosure and the educational agency or institution does not need to obtain the customer's consent.Reference:1: FERPA, 34 CFR Part 99, Subpart D,2.2: The Family Educational Rights and Privacy Act Guidance for Parents, Student Privacy Policy Office, U.S. Department of Education,1.

Question 7

Question Type: MultipleChoice

A law enforcement subpoenas the ACME telecommunications company for access to text message records of a person suspected of planning a terrorist attack. The company had previously encrypted its text message records so that only the suspect could access this data.

What law did ACME violate by designing the service to prevent access to the information by a law enforcement agency?

Options:

A- SCA
B- ECPA
C- CALEA
D- USA Freedom Act

Answer:

C

Explanation:

The law that ACME violated by designing the service to prevent access to the information by a law enforcement agency is theCommunications Assistance for Law Enforcement Act (CALEA)1.CALEA is a federal law that requires telecommunications carriers and manufacturers of telecommunications equipment to design their equipment, facilities, and services to ensure that they have the necessary surveillance capabilities to comply with legal requests for interception of communications2.CALEA applies to all commercial messages, including text messages, and gives law enforcement agencies the authority to subpoena the records of such communications from the service providers3.By encrypting its text message records so that only the suspect could access this data, ACME violated CALEA's duty to cooperate in the interception of communications for law enforcement purposes.Reference:1:Communications Assistance for Law Enforcement Act - Wikipedia2:Home | CALEA | The Commission on Accreditation for Law Enforcement Agencies, Inc.3:Communications Assistance for Law Enforcement Act: IAPP CIPP/US Certified Information Privacy Professional Study Guide, Chapter 6: Law Enforcement and National Security Access, p. 177

Question 8

Question Type: MultipleChoice

Why was the Privacy Protection Act of 1980 drafted?

Options:

A- To respond to police searches of newspaper facilities
B- To assist prosecutors in civil litigation against newspaper companies
C- To assist in the prosecution of white-collar crimes
D- To protect individuals from personal privacy invasion by the police

Answer:

B

Explanation:

The Privacy Protection Act of 1980 (PPA) is a federal law that protects journalists and newsrooms from search and seizure by government officials in connection with criminal investigations or prosecutions. The PPA prohibits the government from searching for or seizing any work product materials or documentary materials possessed by a person who intends to disseminate them to the public through a newspaper, book, broadcast, or other similar form of public communication, unless certain exceptions apply. The PPA was drafted in response to the Supreme Court's decision in Zurcher v. Stanford Daily, which upheld the constitutionality of a police search of a student newspaper's office without a subpoena, based on probable cause that the newspaper had evidence of a crime.The PPA was intended to protect the First Amendment rights of the press and the privacy interests of journalists and their sources from unreasonable government intrusion123.Reference:

1: IAPP, Privacy Protection Act of 1980, https://epic.org/the-privacy-protection-act-of-1980/

2: DOJ, Privacy Protection Act of 1980, https://www.justice.gov/archives/jm/criminal-resource-manual-661-privacy-protection-act-1980

3: Wikipedia, Privacy Protection Act of 1980, https://en.wikipedia.org/wiki/Privacy_Protection_Act_of_1980