IAPP CIPT Practice Questions

Shared by Mendoza on 17-08-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

What is the name of an alternative technique to counter the reduction in use of third-party cookies, where web publishers may consider utilizing data cached by a browser and returned with a subsequent request from the same resource to track unique users?

Options:

A- Web beacon tracking.
B- Browser fingerprinting.
C- Entity tagging.
D- Canvas fingerprinting.

Answer:

B

Explanation:

Browser fingerprinting is a technique used to track users by collecting information about their browser and device characteristics, which are then used to create a unique identifier. This technique can be employed as an alternative to third-party cookies and can track users across different sessions and sites.

Reference: IAPP CIPT Study Guide, 'Tracking Technologies,' which covers various methods of user tracking including cookies, web beacons, and browser fingerprinting.

Question 2

Question Type: MultipleChoice

Which of the following suggests the greatest degree of transparency?

Options:

A- A privacy disclosure statement clearly articulates general purposes for collection
B- The data subject has multiple opportunities to opt-out after collection has occurred.
C- A privacy notice accommodates broadly defined future collections for new products.

D- After reading the privacy notice, a data subject confidently infers how her information will be used.

Answer:

D

Explanation:

The option that suggests the greatest degree of transparency is After reading the privacy notice, a data subject confidently infers how her information will be used. Transparency in data protection means that data subjects should have clear, concise, and understandable information about how their data is collected, used, and shared. The ability of the data subject to confidently infer the use of their information after reading the privacy notice indicates that the notice is clear and transparent, effectively communicating the data processing practices.

GDPR, Article 12: Transparent information, communication, and modalities for the exercise of the rights of the data subject

'Privacy on the Ground: Driving Corporate Behavior' by Kenneth A. Bamberger and Deirdre K. Mulligan

Question 3

Question Type: MultipleChoice

Which option best best describes the basic concept of "Privacy by Design?"

Options:

A- The adoption of privacy enhancing technologies.
B- The integration of a privacy program with all lines of business.
C- The implementation of privacy protection through system architecture.
D- The introduction of business process to identify and assess privacy gaps.

Answer:

C

Explanation:

'Privacy by Design' is a framework that involves embedding privacy protections into the system's architecture from the ground up. This approach ensures that privacy is considered throughout the entire system development lifecycle. The IAPP documents highlight that Privacy by Design requires proactive measures to integrate privacy controls directly into technologies and business practices to prevent privacy issues before they arise, rather than addressing them reactively.

Question 4

Question Type: MultipleChoice

A privacy technologist has been asked to aid in a forensic investigation on the darknet following the compromise of a company's personal data. This will primarily involve an understanding of which of the following privacy-preserving techniques?

Options:

A- Encryption
B- Do Not Track
C- Masking
D- Tokenization

Answer:

D

Explanation:

Tokenization is a privacy-preserving technique that would be crucial in a forensic investigation on the darknet following the compromise of personal data. Tokenization involves replacing sensitive data elements with non-sensitive equivalents (tokens) that can be mapped back to the original data. This method protects the data by ensuring that even if the tokens are exposed, the actual sensitive information remains secure. The IAPP's CIPT materials detail the application of tokenization in preserving privacy during data breaches and forensic investigations.

Question 5

Question Type: MultipleChoice

Which of the following is a vulnerability of a sensitive biometrics authentication system?

Options:

A- False positives.
B- False negatives.
C- Slow recognition speeds.
D- Theft of finely individualized personal data.

Answer:

D

Explanation:

Sensitive biometrics authentication systems have several potential vulnerabilities. Here's why the theft of finely individualized personal data is a significant concern:

Data Sensitivity: Biometrics data, such as fingerprints or retinal scans, are highly sensitive and unique to individuals. If this data is stolen, it cannot be changed like a password.

Security Risks: A breach involving biometric data can have long-lasting implications because the stolen data can be used for identity theft and other malicious activities.

False Positives/Negatives: While false positives (A) and false negatives (B) are operational issues, they are not as critical as the theft of the data itself. Slow recognition speeds (C) are performance-related concerns but do not pose the same level of risk as data theft.

Regulatory Compliance: Many data protection regulations require stringent measures to protect sensitive biometric data, underscoring the importance of safeguarding this information.

Question 6

Question Type: MultipleChoice

SCENARIO

You have just been hired by Ancillary.com, a seller of accessories for everything under the sun, including waterproof stickers for pool floats and decorative bands and cases for sunglasses. The company sells cell phone cases, e-cigarette cases, wine spouts, hanging air fresheners for homes and automobiles, book ends, kitchen implements, visors and shields for computer screens, passport holders, gardening tools and lawn ornaments, and catalogs full of health and beauty

products. The list seems endless. As the CEO likes to say, Ancillary offers, without doubt, the widest assortment of low-price consumer products from a single company anywhere.

Ancillary's operations are similarly diverse. The company originated with a team of sales consultants selling home and beauty products at small parties in the homes of customers, and this base business is still thriving. However, the company now sells online through retail sites designated for industries and demographics, sites such as ''My Cool Ride'' for automobile-related products or ''Zoomer'' for gear aimed toward young adults. The company organization includes a plethora of divisions, units and outrigger operations, as Ancillary has been built along a decentered model rewarding individual initiative and flexibility, while also acquiring key assets. The retail sites seem to all function differently, and you wonder about their compliance with regulations and industry standards. Providing tech support to these sites is also a challenge, partly due to a variety of logins and authentication protocols.

You have been asked to lead three important new projects at Ancillary:

The first is the personal data management and security component of a multi-faceted initiative to unify the company's culture. For this project, you are considering using a series of third-party servers to provide company data and approved applications to employees.

The second project involves providing point of sales technology for the home sales force, allowing them to move beyond paper checks and manual credit card imprinting.

Finally, you are charged with developing privacy protections for a single web store housing all the company's product lines as well as products from affiliates. This new omnibus site will be known, aptly, as ''Under the Sun.'' The Director of Marketing wants the site not only to sell Ancillary's products, but to link to additional products from other retailers through paid advertisements. You need to brief the executive team of security concerns posed by this approach.

What technology is under consideration in the first project in this scenario?

Options:

A- Server driven controls.
B- Cloud computing
C- Data on demand
D- MAC filtering

Answer:

B

Explanation:

The technology under consideration in the first project is cloud computing.

Cloud Computing: This involves using a network of remote servers hosted on the internet to

store, manage, and process data, rather than a local server or a personal computer. This technology provides flexibility, scalability, and cost-effectiveness.

Data Management and Security: Cloud services can unify data management across the company by providing a centralized platform where all employees can access approved applications and data securely.

Third-Party Servers: Using third-party servers, a characteristic feature of cloud computing, aligns with the project's goal to provide company data and approved applications to employees.

Security Considerations: While cloud computing offers many advantages, it also requires careful attention to data security, including encryption, access controls, and regular security audits to protect sensitive information.

IAPP Privacy Management, Information Privacy Technologist Certification Textbooks

NIST SP 800-145: The NIST Definition of Cloud Computing

Question 7

Question Type: MultipleChoice

Properly configured databases and well-written website codes are the best protection against what online threat?

Options:

A- Pharming.
B- SQL injection.
C- Malware execution.
D- System modification.

Answer:

B

Explanation:

SQL injection is a common online threat that targets databases through malicious SQL queries, potentially allowing attackers to access and manipulate database content. Properly configured databases and well-written website code are essential defenses against SQL injection attacks. Ensuring that databases are configured with least privilege access, using parameterized queries, and employing input validation are standard best practices to protect against SQL

injection. Pharming (A), malware execution (C), and system modification (D) are different types of threats that require different mitigation strategies. The emphasis on securing databases and writing secure code to prevent SQL injection is well-documented in security guidelines from the Open Web Application Security Project (OWASP) and other cybersecurity frameworks referenced by the IAPP.

Question 8

Question Type: MultipleChoice

Which option best activities would be considered the best method for an organization to achieve the privacy principle of data quality'?

Options:

A- Clash customer information with information from a data broker
B- Build a system with user access controls and approval workflows to edit customer data
C- Set a privacy notice covering the purpose for collection of a customer's data
D- Provide a customer with a copy of their data in a machine-readable format

Answer:

B

Explanation:

Building a system with user access controls and approval workflows to edit customer data is considered the best method for an organization to achieve the privacy principle of data quality. This approach ensures that data is accurate, complete, and up-to-date by allowing controlled access and modifications. The IAPP's CIPT materials discuss data quality principles, emphasizing the importance of implementing robust data management practices to maintain data integrity and accuracy.

Question 9

Question Type: MultipleChoice

Which Organization for Economic Co-operation and Development (OECD) privacy protection

principle encourages an organization to obtain an individual s consent before transferring personal information?

Options:

A- Individual participation.
B- Purpose specification.
C- Collection limitation.
D- Accountability.

Answer:

A

Explanation:

The OECD privacy protection principle that encourages an organization to obtain an individual's consent before transferring personal information is individual participation. This principle asserts that individuals should have the right to know about the collection and use of their personal data, and to consent to its transfer. It emphasizes transparency and individual control over personal information (IAPP, Certified Information Privacy Technologist (CIPT) materials).

Question 10

Question Type: MultipleChoice

Which option best provides a mechanism that allows an end-user to use a single sign-on (SSO) for multiple services?

Options:

A- The Open ID Federation.
B- PCI Data Security Standards Council
C- International Organization for Standardization.
D- Personal Information Protection and Electronic Documents Act.

Answer:

A

Explanation:

OpenID Connect, a part of the OpenID Federation, is a standard that enables single sign-on (SSO) functionality, allowing end-users to authenticate once and gain access to multiple services. This mechanism simplifies user experience by reducing the number of login credentials needed and enhances security by relying on a trusted identity provider. The IAPP notes that federated identity management solutions like OpenID Connect are essential for modern authentication processes, improving both security and user convenience (IAPP, 'Identity and Access Management').

P2P exams