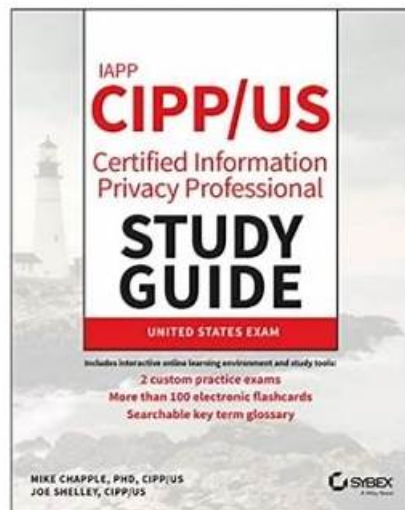


IAPP CIPP-US Study Guide Pdf & Visual CIPP-US Cert Exam

**PDF IAPP CIPP / US Certified Information Privacy
Professional Study Guide Free**



What's more, part of that PassCollection CIPP-US dumps now are free: https://drive.google.com/open?id=1WTWUi5_qkeV1EX2udFtwr5ncXp8ILLXT

Our PDF version of the CIPP-US learning braindumps can print on papers and make notes. Then windows software of the CIPP-US exam questions, which needs to install on windows software. Also, the windows software is intelligent to simulate the real test environment. Then the online engine of the CIPP-US Study Materials, which is convenient for you because it doesn't need to install on computers. It supports Windows, Mac, Android, iOS and so on. This version just can run on web browser.

PassCollection is a trusted platform that has been helping Certified Information Privacy Professional/United States (CIPP/US) CIPP-US candidates for many years. Over this long time period, countless candidates have passed their Certified Information Privacy Professional/United States (CIPP/US) CIPP-US Exam and they all got help from Certified Information Privacy Professional/United States (CIPP/US) practice questions and easily pass the final exam.

>> IAPP CIPP-US Study Guide Pdf <<

Visual CIPP-US Cert Exam - CIPP-US Latest Examprep

PassCollection can provide you with a reliable and comprehensive solution to pass IAPP certification CIPP-US exam. Our solution can 100% guarantee you to pass the exam, and also provide you with a one-year free update service. You can also try to free

download the IAPP Certification CIPP-US Exam testing software and some practice questions and answers to on PassCollection website.

IAPP CIPP-US (Certified Information Privacy Professional/United States) Exam is a globally recognized certification that validates an individual's knowledge and expertise in the field of US privacy laws and regulations. Certified Information Privacy Professional/United States (CIPP/US) certification is offered by the International Association of Privacy Professionals (IAPP), which is a leading professional association for privacy professionals worldwide. The CIPP/US certification is designed to help professionals stay updated with the latest privacy laws and regulations in the US and demonstrate their expertise to their peers and employers.

IAPP Certified Information Privacy Professional/United States (CIPP/US) Sample Questions (Q195-Q200):

NEW QUESTION # 195

John, a California resident, receives notification that a major corporation with \$500 million in annual revenue has experienced a data breach. John's personal information in their possession has been stolen, including his full name and social security numb. John also learns that the corporation did not have reasonable cybersecurity measures in place to safeguard his personal information. Which of the following answers most accurately reflects John's ability to pursue a legal claim against the corporation under the California Consumer Privacy Act (CCPA)?

- **A. John can sue the corporation for the data breach to recover monetary damages suffered as a result of the data breach, and in some circumstances seek statutory damages irrespective of whether he suffered any financial harm**
- B. John cannot sue the corporation for the data breach because only the state's Attorney General has authority to file suit under the CCPA.
- C. John can sue the corporation for the data breach but only to recover monetary damages he actually suffered as a result of the data breach.
- D. John has no right to sue the corporation because the CCPA does not address any data breach rights.

Answer: A

Explanation:

The CCPA provides consumers with a private right of action to pursue statutory damages following data security breaches that impact certain sensitive categories of personal information and are caused by a business's failure to institute reasonable and appropriate security. The CCPA defines personal information for this purpose as an individual's name in combination with any of the following: social security number, driver's license number, account number, credit or debit card number, medical information, or health insurance information. The CCPA allows consumers to seek damages between \$100 and \$750 per consumer per incident, or actual damages, whichever is greater. The CCPA also requires consumers to provide the business with 30 days' written notice and an opportunity to cure the violation before initiating an action. Additionally, the CCPA requires consumers to notify the Attorney General within 30 days of filing the action and obtain the Attorney General's approval or nonobjection before proceeding with the action. Therefore, John can sue the corporation for the data breach to recover monetary damages suffered as a result of the data breach, and in some circumstances seek statutory damages irrespective of whether he suffered any financial harm, as long as he meets the requirements of the CCPA. References:

- * CCPA Provides Private Right of Action for Data Security Breaches
- * CCPA Private Right of Action - Data Breach Security Requirement
- * CCPA Fines & Penalties for Data Protection Violations | MatrixPoint

NEW QUESTION # 196

In 2011, the FTC announced a settlement with Google regarding its social networking service Google Buzz. The FTC alleged that in the process of launching the service, the company did all of the following EXCEPT?

- **A. Failed to employ sufficient security safeguards.**
- B. Failed to comply with Safe Harbor principles.
- C. Engaged in deceptive trade practices.
- D. Violated its own privacy policies.

Answer: A

Explanation:

The FTC alleged that Google violated its own privacy policies, engaged in deceptive trade practices, and failed to comply with Safe Harbor principles when it launched Google Buzz, a social networking service that automatically enrolled Gmail users and exposed their email contacts and other personal information without their consent or control. The FTC did not allege that Google failed to

employ sufficient security safeguards, although it did require Google to implement a comprehensive privacy program and submit to regular privacy audits as part of the settlement. The other statements are incorrect because:

* A. Violated its own privacy policies: The FTC alleged that Google violated its own privacy policies by using information collected from Gmail users for a purpose that was incompatible with the purpose for which the information was collected, without obtaining their affirmative consent. Google's privacy policy stated that "When you sign up for a particular service that requires registration, we ask you to provide personal information. If we use this information in a manner different than the purpose for which it was collected, then we will ask for your consent prior to such use."¹

* B. Engaged in deceptive trade practices: The FTC alleged that Google engaged in deceptive trade practices by misrepresenting the extent to which consumers could exercise control over the collection, use, and sharing of their personal information through Google Buzz. For example, Google offered consumers the option to decline or turn off Google Buzz, but the option was ineffective and did not fully remove the consumer from the social network. Google also misled consumers about how their email contacts would be treated on Google Buzz, and failed to disclose that certain information, such as the user's frequent email contacts, would be made public by default.¹

* C. Failed to comply with Safe Harbor principles: The FTC alleged that Google failed to comply with the U.S.-EU Safe Harbor Framework, which provides a method for U.S. companies to transfer personal data from the European Union to the United States in a way that meets EU data protection requirements.

Google had self-certified to the Department of Commerce that it adhered to the Safe Harbor Privacy Principles, which include notice, choice, access, and enforcement. The FTC alleged that Google's conduct violated the notice and choice principles, as well as the requirement to adhere to the Safe Harbor FAQs.¹ References: FTC Charges Deceptive Privacy Practices in Google's Rollout of Its Buzz Social Network, Google, Inc., In the Matter of, Google settles with FTC over Buzz; Privacy policies to be audited for two decades, Google Settles FTC Complaint over Google Buzz Privacy

NEW QUESTION # 197

Which of the following best describes private-sector workplace monitoring in the United States?

- A. Employers have broad authority to monitor their employees
- B. U.S. federal law restricts monitoring only to industries for which it is necessary
- C. Judgments in private lawsuits have severely limited the monitoring of employees
- D. Most employees are protected from workplace monitoring by the U.S. Constitution

Answer: A

Explanation:

In the United States, there is no comprehensive federal law that regulates employee monitoring in the private sector. Instead, there are various federal and state laws that address specific aspects of monitoring, such as electronic communications, video surveillance, GPS tracking, and biometric data. Generally, these laws provide more protection for employees' privacy when they are using their own devices or personal accounts, or when they are outside of work hours or premises. However, when employees are using company-owned devices or accounts, or when they are performing work-related tasks, employers have broad authority to monitor their activities, as long as they have a legitimate business interest and do not violate any specific laws. Employers are also advised to inform employees of their monitoring practices and obtain their consent, either explicitly or implicitly, to avoid potential legal disputes or employee backlash.^{1 2 3} References: <https://www.jibbble.io/article/us-employee-monitoring>
<https://www.worktime.com/most-asked-questions-on-us-employee-monitoring-laws>

NEW QUESTION # 198

Which of the following best describes the ASIA-Pacific Economic Cooperation (APEC) principles?

- A. A bill of rights for individuals seeking access to their personal information.
- B. A code of responsibilities for medical establishments to uphold privacy laws.
- C. A baseline of marketers' minimum responsibilities for providing opt-out mechanisms.
- D. An international court ruling on personal information held in the commercial sector.

Answer: A

Explanation:

Explanation/Reference: <http://documents1.worldbank.org/curated/en/751621525705087132/text/WPS8431.txt>

NEW QUESTION # 199

SCENARIO

Please use the following to answer the next QUESTION

Noah is trying to get a new job involving the management of money. He has a poor personal credit rating, but he has made better financial decisions in the past two years.

One potential employer, Arnie's Emporium, recently called to tell Noah he did not get a position. As part of the application process, Noah signed a consent form allowing the employer to request his credit report from a consumer reporting agency (CRA). Noah thinks that the report hurt his chances, but believes that he may not ever know whether it was his credit that cost him the job.

However, Noah is somewhat relieved that he was not offered this particular position. He noticed that the store where he interviewed was extremely disorganized. He imagines that his credit report could still be sitting in the office, unsecured.

Two days ago, Noah got another interview for a position at Sam's Market. The interviewer told Noah that his credit report would be a factor in the hiring decision. Noah was surprised because he had not seen anything on paper about this when he applied.

Regardless, the effect of Noah's credit on his employability troubles him, especially since he has tried so hard to improve it. Noah made his worst financial decisions fifteen years ago, and they led to bankruptcy. These were decisions he made as a young man, and most of his debt at the time consisted of student loans, credit card debt, and a few unpaid bills - all of which Noah is still working to pay off. He often laments that decisions he made fifteen years ago are still affecting him today.

In addition, Noah feels that an experience investing with a large bank may have contributed to his financial troubles. In 2007, in an effort to earn money to help pay off his debt, Noah talked to a customer service representative at a large investment company who urged him to purchase stocks. Without understanding the risks, Noah agreed. Unfortunately, Noah lost a great deal of money.

After losing the money, Noah was a customer of another financial institution that suffered a large security breach. Noah was one of millions of customers whose personal information was compromised. He wonders if he may have been a victim of identity theft and whether this may have negatively affected his credit.

Noah hopes that he will soon be able to put these challenges behind him, build excellent credit, and find the perfect job.

Based on the scenario, which legislation should ease Noah's worry about his credit report as a result of applying at Arnie's Emporium?

- A. The Safeguards Rule under the Gramm-Leach-Bliley Act (GLBA).
- B. The Privacy Rule under the Gramm-Leach-Bliley Act (GLBA).
- **C. The Disposal Rule under the Fair and Accurate Credit Transactions Act (FACTA).**
- D. The Red Flags Rule under the Fair and Accurate Credit Transactions Act (FACTA).

Answer: C

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). References:

* 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

NEW QUESTION # 200

.....

PassCollection's IAPP CIPP-US Exam Training materials provide the two most popular download formats. One is PDF, and other is software, it is easy to download. The IT professionals and industrious experts in PassCollection make full use of their knowledge and experience to provide the best products for the candidates. We can help you to achieve your goals.

Visual CIPP-US Cert Exam: https://www.passcollection.com/CIPP-US_real-exams.html

- BONUS!!! Download part of PassCollection CIPP-US dumps for free: https://drive.google.com/open?id=1WTWUi5_qkeV1EX2udFtwr5ncXp8ILLXT

BONUS!!! Download part of PassCollection CIPP-US dumps for free: https://drive.google.com/open?id=1WTWUi5_qkeV1EX2udFtwr5ncXp8ILLXT