



**Free Questions for CIPP-US by dumpshq**

**Shared by Porter on 29-01-2024**

**For More Free Questions and Preparation Resources**

**Check the Links on Last Page**

## Question 1

---

**Question Type:** MultipleChoice

---

In March 2012, the FTC released a privacy report that outlined three core principles for companies handling consumer data.

a. Which was NOT one of these principles?

**Options:**

---

- A- Simplifying consumer choice.
- B- Enhancing security measures.
- C- Practicing Privacy by Design.
- D- Providing greater transparency.

**Answer:**

---

B

## Question 2

---

**Question Type:** MultipleChoice

---

Based on the 2012 Federal Trade Commission report "Protecting Consumer Privacy in an Era of Rapid Change", which of the following directives is most important for businesses?

**Options:**

---

- A- Announcing the tracking of online behavior for advertising purposes.
- B- Integrating privacy protections during product development.
- C- Allowing consumers to opt in before collecting any data.
- D- Mitigating harm to consumers after a security breach.

**Answer:**

---

B

**Explanation:**

---

<https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf>

## Question 3

---

**Question Type:** MultipleChoice

---

The U.S. Supreme Court has recognized an individual's right to privacy over personal issues, such as contraception, by acknowledging which of the following?

### Options:

---

- A- Federal preemption of state constitutions that expressly recognize an individual right to privacy.
- B- A "penumbra" of unenumerated constitutional rights as well as more general protections of due process of law.
- C- An interpretation of the U.S. Constitution's explicit definition of privacy that extends to personal issues.
- D- The doctrine of stare decisis, which allows the U.S. Supreme Court to follow the precedent of previously decided case law.

### Answer:

---

B

## Question 4

---

**Question Type:** MultipleChoice

---

In a case of civil litigation, what might a defendant who is being sued for distributing an employee's private information face?

**Options:**

---

- A- Probation.
- B- Criminal fines.
- C- An injunction.
- D- A jail sentence.

**Answer:**

---

C

## Question 5

---

**Question Type: MultipleChoice**

---

SCENARIO

Please use the following to answer the next QUESTION

Matt went into his son's bedroom one evening and found him stretched out on his bed typing on his laptop. "Doing your homework?" Matt asked hopefully.

"No," the boy said. "I'm filling out a survey."

Matt looked over his son's shoulder at his computer screen. "What kind of survey?" "It's asking QUESTIONS about my opinions."

"Let me see," Matt said, and began reading the list of

QUESTION s that his son had already answered. "It's asking your opinions about the government and citizenship. That's a little odd. You're only ten."

Matt wondered how the web link to the survey had ended up in his son's email inbox. Thinking the message might have been sent to his son by mistake he opened it and read it. It had come from an entity called the Leadership Project, and the content and the graphics indicated that it was intended for children. As Matt read further he learned that kids who took the survey were automatically registered in a contest to win the first book in a series about famous leaders.

To Matt, this clearly seemed like a marketing ploy to solicit goods and services to children. He asked his son if he had been prompted to give information about himself in order to take the survey. His son told him he had been asked to give his name, address, telephone number, and date of birth, and to answer

QUESTIONS about his favorite games and toys.

Matt was concerned. He doubted if it was legal for the marketer to collect information from his son in the way that it was. Then he noticed several other commercial emails from marketers advertising products for children in his son's inbox, and he decided it was time to report the incident to the proper authorities.

Depending on where Matt lives, the marketer could be prosecuted for violating which of the following?

**Options:**

---

- A- Investigative Consumer Reporting Agencies Act.
- B- Unfair and Deceptive Acts and Practices laws.
- C- Consumer Bill of Rights.
- D- Red Flag Rules.

**Answer:**

---

B

## Question 6

---

**Question Type:** MultipleChoice

---

SCENARIO

Please use the following to answer the next QUESTION

When there was a data breach involving customer personal and financial information at a large retail store, the company's directors were shocked. However, Roberta, a privacy analyst at the company and a victim of identity theft herself, was not. Prior to the breach, she had been working on a privacy program report for the executives. How the company shared and handled data across its organization was a major concern. There were neither adequate rules about access to customer information nor

procedures for purging and destroying outdated data

a. In her research, Roberta had discovered that even low-level employees had access to all of the company's customer data, including financial records, and that the company still had in its possession obsolete customer data going back to the 1980s.

Her report recommended three main reforms. First, permit access on an as-needs-to-know basis. This would mean restricting employees' access to customer information to data that was relevant to the work performed. Second, create a highly secure database for storing customers' financial information (e.g., credit card and bank account numbers) separate from less sensitive information. Third, identify outdated customer information and then develop a process for securely disposing of it.

When the breach occurred, the company's executives called Roberta to a meeting where she presented the recommendations in her report. She explained that the company having a national customer base meant it would have to ensure that it complied with all relevant state breach notification laws. Thanks to Roberta's guidance, the company was able to notify customers quickly and within the specific timeframes set by state breach notification laws.

Soon after, the executives approved the changes to the privacy program that Roberta recommended in her report. The privacy program is far more effective now because of these changes and, also, because privacy and security are now considered the responsibility of every employee.

What could the company have done differently prior to the breach to reduce their risk?



### Options:

---

- A- Implemented a comprehensive policy for accessing customer information.
- B- Honored the promise of its privacy policy to acquire information by using an opt-in method.
- C- Looked for any persistent threats to security that could compromise the company's network.
- D- Communicated requests for changes to users' preferences across the organization and with third parties.

### Answer:

---

A

## Question 7

---

**Question Type: MultipleChoice**

---

### SCENARIO

Please use the following to answer the next QUESTION

When there was a data breach involving customer personal and financial information at a large retail store, the company's directors were shocked. However, Roberta, a privacy analyst at the company and a victim of identity theft herself, was not. Prior to the breach, she had been working on a privacy program report for the executives. How the company shared and handled data across its organization was a major concern. There were neither adequate rules about access to customer information nor

procedures for purging and destroying outdated data

a. In her research, Roberta had discovered that even low-level employees had access to all of the company's customer data, including financial records, and that the company still had in its possession obsolete customer data going back to the 1980s.

Her report recommended three main reforms. First, permit access on an as-needs-to-know basis. This would mean restricting employees' access to customer information to data that was relevant to the work performed. Second, create a highly secure database for storing customers' financial information (e.g., credit card and bank account numbers) separate from less sensitive information. Third, identify outdated customer information and then develop a process for securely disposing of it.

When the breach occurred, the company's executives called Roberta to a meeting where she presented the recommendations in her report. She explained that the company having a national customer base meant it would have to ensure that it complied with all relevant state breach notification laws. Thanks to Roberta's guidance, the company was able to notify customers quickly and within the specific timeframes set by state breach notification laws.

Soon after, the executives approved the changes to the privacy program that Roberta recommended in her report. The privacy program is far more effective now because of these changes and, also, because privacy and security are now considered the responsibility of every employee.

Which principle of the Consumer Privacy Bill of Rights, if adopted, would best reform the company's privacy program?

**Options:**

---

**A-** Consumers have a right to exercise control over how companies use their personal data.

**B-** Consumers have a right to reasonable limits on the personal data that a company retains.

**C-** Consumers have a right to easily accessible information about privacy and security practices.

**D-** Consumers have a right to correct personal data in a manner that is appropriate to the sensitivity.

**Answer:**

---

B

## Question 8

---

**Question Type: MultipleChoice**

---

SCENARIO

Please use the following to answer the next QUESTION

When there was a data breach involving customer personal and financial information at a large retail store, the company's directors were shocked. However, Roberta, a privacy analyst at the company and a victim of identity theft herself, was not. Prior to the breach, she had been working on a privacy program report for the executives. How the company shared and handled data across its organization was a major concern. There were neither adequate rules about access to customer information nor

procedures for purging and destroying outdated dat

a. In her research, Roberta had discovered that even low- level employees had access to all of the company's customer data, including financial records, and that the company still had in its possession obsolete customer data going back to the 1980s.

Her report recommended three main reforms. First, permit access on an as-needs-to-know basis. This would mean restricting employees' access to customer information to data that was relevant to the work performed. Second, create a highly secure database for storing customers' financial information (e.g., credit card and bank account numbers) separate from less sensitive information. Third, identify outdated customer information and then develop a process for securely disposing of it.

When the breach occurred, the company's executives called Roberta to a meeting where she presented the recommendations in her report. She explained that the company having a national customer base meant it would have to ensure that it complied with all relevant state breach notification laws. Thanks to Roberta's guidance, the company was able to notify customers quickly and within the specific timeframes set by state breach notification laws.

Soon after, the executives approved the changes to the privacy program that Roberta recommended in her report. The privacy program is far more effective now because of these changes and, also, because privacy and security are now considered the responsibility of every employee.

Based on the problems with the company's privacy security that Roberta identifies, what is the most likely cause of the breach?

### **Options:**

---

- A-** Mishandling of information caused by lack of access controls.
- B-** Unintended disclosure of information shared with a third party.
- C-** Fraud involving credit card theft at point-of-service terminals.
- D-** Lost company property such as a computer or flash drive.

### **Answer:**

---

A

## Question 9

---

**Question Type:** MultipleChoice

---

Which of the following accurately describes the purpose of a particular federal enforcement agency?

### Options:

---

- A-** The National Institute of Standards and Technology (NIST) has established mandatory privacy standards that can then be enforced against all for-profit organizations by the Department of Justice (DOJ).
- B-** The Cybersecurity and Infrastructure Security Agency (CISA) is authorized to bring civil enforcement actions against organizations whose website or other online service fails to adequately secure personal information.
- C-** The Federal Communications Commission (FCC) regulates privacy practices on the internet and enforces violations relating to websites' posted privacy disclosures.
- D-** The Federal Trade Commission (FTC) is typically recognized as having the broadest authority under the FTC Act to address unfair or deceptive privacy practices.

### Answer:

---

D

## Question 10

---

**Question Type:** MultipleChoice

---

Even when dealing with an organization subject to the CCPA, California residents are NOT legally entitled to request that the organization do what?

### Options:

---

- A- Delete their personal information.
- B- Correct their personal information.
- C- Disclose their personal information to them.
- D- Refrain from selling their personal information to third parties.

### Answer:

---

C

### Explanation:

---

## Question 11

---

**Question Type:** MultipleChoice

---

Which of the following best describes how federal anti-discrimination laws protect the privacy of private-sector employees in the United States?

**Options:**

---

- A- They prescribe working environments that are safe and comfortable.
- B- They limit the amount of time a potential employee can be interviewed.
- C- They promote a workforce of employees with diverse skills and interests.
- D- They limit the types of information that employers can collect about employees.

**Answer:**

---

D

**To Get Premium Files for CIPP-US Visit**

**<https://www.p2pexams.com/products/cipp-us>**

**For More Free Questions Visit**

**<https://www.p2pexams.com/iapp/pdf/cipp-us>**

