CIPP-C Q&As

Certified Information Privacy Professional/ Canada (CIPP/C)

Pass IAPP CIPP-C Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.certbus.com/cipp-c.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by IAPP Official Exam Center

QUESTION 1

Although an employer may have a strong incentive or legal obligation to monitor employees\\' conduct or behavior, some excessive monitoring may be considered an intrusion on employees\\' privacy? Which of the following is the strongest example of excessive monitoring by the employer?

A. An employer who installs a video monitor in physical locations, such as a warehouse, to ensure employees are performing tasks in a safe manner and environment.

B. An employer who installs data loss prevention software on all employee computers to limit transmission of confidential company information.

C. An employer who installs video monitors in physical locations, such as a changing room, to reduce the

D. risk of sexual harassment.

E. An employer who records all employee phone calls that involve financial transactions with customers completed over the phone.

Correct Answer: C

QUESTION 2

What is the most likely reason that states have adopted their own data breach notification laws?

A. Many states have unique types of businesses that require specific legislation

B. Many lawmakers believe that federal enforcement of current laws has not been effective

C. Many types of organizations are not currently subject to federal laws regarding breaches

D. Many large businesses have intentionally breached the personal information of their customers

Correct Answer: B

QUESTION 3

The "Consumer Privacy Bill of Rights" presented in a 2012 Obama administration report is generally based on?

A. The 1974 Privacy Act

B. Common law principles

C. European Union Directive

D. Traditional fair information practices

Correct Answer: C

QUESTION 4

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?

A. SCA

B.

C. ECPA

D. CALEA

E. USA Freedom Act

Correct Answer: C

QUESTION 5

What is a key way that the Gramm-Leach-Bliley Act (GLBA) prevents unauthorized access into a person\\'s back account?

A. By requiring immediate public disclosure after a suspected security breach.

B. By requiring the amount of customer personal information printed on paper.

C. By requiring the financial institutions limit the collection of personal information.

D.

E. By restricting the disclosure of customer account numbers by financial institutions.

Correct Answer: D

QUESTION 6

Which statute is considered part of U.S. federal privacy law?

A. The Fair Credit Reporting Act.

B. SB 1386.

C. The Personal Information Protection and Electronic Documents Act.

D. The e-Privacy Directive.

Correct Answer: A

QUESTION 7

Felicia is also in favor of strict employee oversight. In addition to protecting the inventory, she wants to prevent mistakes during transactions, which will require video monitoring. She also wants to regularly check the company vehicle\\'s GPS for locations visited by employees. She also believes that employees who use their own devices for work-related purposes should agree to a certain amount of supervision.

Given her high standards, Felicia is skeptical about the proposed location of the store. She has been told that many types of background checks are not allowed under California law. Her friend Celeste thinks these worries are unfounded, as long as applicants verbally agree to the checks and are offered access to the results. Nor does Celeste share Felicia\\'s concern about state breach notification laws, which, she claims, would be costly to implement even on a minor scale. Celeste believes that

even if the business grows a customer database of a few thousand, it\\'s unlikely that a state agency would hassle an honest business if an accidental security incident were to occur.

In any case, Celeste feels that all they need is common sense ?like remembering to tear up sensitive documents before throwing them in the recycling bin. Felicia hopes that she\\'s right, and that all of her concerns will be put to rest next month when their new business consultant (who is also a privacy professional) arrives from North Carolina.

Which law will be most relevant to Felicia\\'s plan to ask applicants about drug addiction?

A.

B. The Americans with Disabilities Act (ADA).

C. The Occupational Safety and Health Act (OSHA).

D. The Genetic Information Nondiscrimination Act of 2008.

E. The Health Insurance Portability and Accountability Act (HIPAA).

Correct Answer: A

QUESTION 8

In 2012, the White House and the FTC both issued reports advocating a new approach to privacy enforcement that can best be described as what?

A. Harm-based.

B. Self-regulatory.

C. Comprehensive.

D. Notice and choice.

Correct Answer: B

QUESTION 9

What is the main reason a country might adopt an "ombudsman" model of privacy oversight?

A. It provides a more streamlined process of complaint resolution.

B. It increases the power of the commissioner to enforce decisions.

C. It reduces the perception that compliance is a confrontational process.

D. It provides a more detailed set of guidelines regarding possible violations.

Correct Answer: C

QUESTION 10

What is the primary motivation for a federal government entity to complete a Privacy Impact Assessment (PIA)?

A. Introducing new legislation in the House of Commons

B. Receiving program approvals from the Treasury Board of Canada.

C. Obtaining program expertise from the Privacy Commissioner of Canada.

D. Improving collection methods through its information technology systems.

Correct Answer: B

QUESTION 11

According to PIPEDA, all of the following data is considered sensitive: physical disability, ethnicity, sexual orientation and?

A. Age

B. Gender

C. Locality

D. Religion

Correct Answer: D

QUESTION 12

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?

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.

Correct Answer: A

QUESTION 13

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. 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?

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.

Correct Answer: C

QUESTION 14

When does the Telemarketing Sales Rule require an entity to share a do-not-call request across its organization?

A. When the operational structures of its divisions are not transparent

B. When the goods and services sold by its divisions are very similar

C. When a call is not the result of an error or other unforeseen cause

D. When the entity manages user preferences through multiple platforms

Correct Answer: C

QUESTION 15

SCENARIO

Please use the following to answer the next QUESTION:

Larry has become increasingly dissatisfied with his telemarketing position at SunriseLynx, and particularly with his supervisor, Evan. Just last week, he overheard Evan mocking the state\\'s Do Not Call list, as well as the people on it. "If they were really serious about not being bothered," Evan said, "They\\'d be on the national DNC list. That\\'s the only one we\\'re required to follow. At SunriseLynx, we call until they ask us not to."

Bizarrely, Evan requires telemarketers to keep records of recipients who ask them to call "another time." This, to Larry, is a clear indication that they don\\'t want to be called at all. Evan doesn\\'t see it that way.

Larry believes that Evan\\'s arrogance also affects the way he treats employees. The U.S. Constitution protects American workers, and Larry believes that the rights of those at SunriseLynx are violated regularly. At first Evan seemed friendly, even connecting with employees on social media. However, following Evan\\'s political posts, it became clear to Larry that employees with similar affiliations were the only ones offered promotions.

Further, Larry occasionally has packages containing personal-use items mailed to work. Several times, these have come to him already opened, even though this name was clearly marked. Larry thinks the opening of personal mail is common at SunriseLynx, and that Fourth Amendment rights are being trampled under Evan\\'s leadership.

Larry has also been dismayed to overhear discussions about his coworker, Sadie. Telemarketing calls are regularly recorded for quality assurance, and although Sadie is always professional during business, her personal conversations sometimes contain sexual comments. This too is something Larry has heard Evan laughing about. When he mentioned this to a coworker, his concern was met with a shrug. It was the coworker\\'s belief that employees agreed to be monitored when they signed on. Although personal devices are left alone, phone calls, emails and browsing histories are all subject to surveillance. In fact, Larry knows of one case in which an employee was fired after an undercover investigation by an outside firm turned up evidence of misconduct. Although the employee may have stolen from the company, Evan could have simply contacted the authorities when he first suspected something amiss. Larry wants to take action, but is uncertain how to proceed.

In what area does Larry have a misconception about private-sector employee rights?

A. The applicability of federal law

B. The enforceability of local law

C. The strict nature of state law

D. The definition of tort law

Correct Answer: A