"Please note that these files may not be up to date. However, the questions will help you understand the exam format and typical question patterns."

Warning: Keep connected with our support team for latest updates

Question: 1

Which jurisdiction must courts have in order to hear a particular case?

A. Subject matter jurisdiction and regulatory jurisdiction
B. Subject matter jurisdiction and professional jurisdiction
C. Personal jurisdiction and subject matter jurisdiction
D. Personal jurisdiction and professional jurisdiction

Answer: C

Explanation:

In order for a court to hear a case, it must have both personal jurisdiction and subject matter jurisdiction. Personal jurisdiction refers to the authority of a court over the parties to a case, while subject matter jurisdiction refers to the authority of a court to hear a particular type of case. For example, a federal court may have subject matter jurisdiction over a case involving a federal law, but it may not have personal jurisdiction over a defendant who has no contacts with the state where the court is located. Similarly, a state court may have personal jurisdiction over a resident of the state, but it may not have subject matter jurisdiction over a case involving a foreign treaty. Reference: [IAPP CIPP/US Study Guide], Chapter 2: Introduction to U.S. Law, p. 25-26; Wex Legal Dictionary, Subject Matter Jurisdiction and Personal Jurisdiction.

Question: 2

Which authority supervises and enforces laws regarding advertising to children via the Internet?

A. The Office for Civil Rights
B. The Federal Trade Commission
C. The Federal Communications Commission
D. The Department of Homeland Security

Answer: B

Explanation:

The Federal Trade Commission (FTC) is the primary federal agency that regulates advertising and marketing

practices in the United States, including those targeting children via the Internet. The FTC enforces the Children's Online Privacy Protection Act (COPPA), which requires operators of websites and online services directed to children under 13 to obtain verifiable parental consent before collecting, using, or disclosing personal information from children. The FTC also enforces the FTC Act, which prohibits unfair or deceptive acts or practices in commerce, such as making false or misleading claims in advertising. The FTC has issued guidelines and reports on various aspects of digital advertising to children, such as sponsored content, influencers, data collection, persuasive design, and behavioral marketing. The FTC also hosts workshops and events to examine the impact of digital advertising on children and their ability to distinguish ads from entertainment. Reference: FTC website

Digital Advertising to Children

IAPP CIPP/US Study Guide, Chapter 5: Marketing and Privacy, pp. 169-170

Question: 3

According to Section 5 of the FTC Act, self-regulation primarily involves a company's right to do what?

A. Determine which bodies will be involved in adjudication
B. Decide if any enforcement actions are justified
C. Adhere to its industry's code of conduct
D. Appeal decisions made against it

Answer: C

Explanation:

According to Section 5 of the FTC Act, self-regulation primarily involves a company's right to adhere to its industry's code of conduct. Self-regulation is a process by which an industry or a group of companies voluntarily adopts and enforces standards or guidelines to protect consumers and promote fair competition. The FTC encourages self-regulation as a way to complement its enforcement efforts and address emerging issues in the marketplace. The FTC also monitors self- regulatory programs and may take action against companies that fail to comply with their own codes of conduct or misrepresent their participation in such programs. Reference:

Federal Trade Commission Act, Section 5 of

Self-Regulation | Federal Trade Commission

[IAPP CIPP/US Certified Information Privacy Professional Study Guide], Chapter 3, page 79

Question: 4

Which was NOT one of the five priority areas listed by the Federal Trade Commission in its 2012 report, "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers"?

A. International data transfers
B. Large platform providers
C. Promoting enforceable self-regulatory codes
D. Do Not Track

Answer: D

Explanation:

The Federal Trade Commission (FTC) issued its 2012 report, "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers"1, which outlined a framework for privacy protection based on three main principles: privacy by design, simplified consumer choice, and greater transparency. The report also identified five priority areas for the FTC's privacy enforcement and policy efforts, which were: Data brokers

Large platform providers

Mobile

Promoting enforceable self-regulatory codes

International data transfers

Do Not Track was not one of the five priority areas, but rather a specific mechanism for implementing the principle of simplified consumer choice. The report endorsed the development of a Do Not Track system that would allow consumers to opt out of online behavioral advertising across websites and platforms1. The report also noted the progress made by various stakeholders, such as the World Wide Web Consortium (W3C), the Digital Advertising Alliance (DAA), and browser companies, in advancing the Do Not Track initiative1.

Reference: 1: Federal Trade Commission, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers (March 2012), available at 1.

Question: 5

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

Answer: D

Explanation:

The Consumer Privacy Bill of Rights is a set of principles that the Obama administration proposed in 2012 to guide the development of privacy legislation and policies in the United States. The report that introduced the bill of rights stated that it was "generally based on the widely accepted Fair Information Practice Principles (FIPPs)"1, which are a set of standards that originated in the 1970s and have influenced many privacy laws and frameworks around the world. The FIPPs include concepts such as individual control, transparency, security, accountability, and data minimization2. The Consumer Privacy Bill of Rights adapted and expanded these principles to address the challenges and opportunities of the digital economy1. Reference: 1: Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy2, page 92: IAPP CIPP/US Certified Information Privacy Professional Study Guide3, page 17.

Question: 6

What is a legal document approved by a judge that formalizes an agreement between a governmental agency and an adverse party called?

A. A consent decree
B. Stare decisis decree
C. A judgment rider
D. Common law judgment

Answer: A

Explanation:
A consent decree is a legal document that resolves a dispute between a governmental agency and an adverse party without admission of guilt or liability by either side. It is approved by a judge and has the force of a court order. A consent decree may include terms such as compliance, monitoring, reporting, or remediation. A consent decree is often used to settle civil enforcement actions brought by federal agencies such as the Federal Trade Commission (FTC), the Environmental Protection Agency (EPA), or the Department of Justice (DOJ). Reference:
IAPP Glossary, entry for "consent decree"
[IAPP CIPP/US Study Guide], p. 39, section 2.1.3
[IAPP CIPP/US Body of Knowledge], p. 9, section B.1.a

Question: 7

Read this notice:

Our website uses cookies. Cookies allow us to identify the computer or device you're using to access the site, but they don't identify you personally. For instructions on setting your Web browser to refuse cookies, click here.

What type of legal choice does not notice provide?

A. Mandatory
B. Implied consent
C. Opt-in
D. Opt-out

Answer: B

Explanation:
A cookie is a small piece of data that a website sends to a user's browser and stores on the user's device, usually for the purpose of remembering the user's preferences, settings, or actions1.
A cookie notice is a message that informs the user about the website's use of cookies and the user's choices regarding the acceptance or rejection of cookies2.
A legal choice is the mechanism that the website provides to the user to express their consent or dissent to the use of cookies2.
There are different types of legal choices for cookie notices, depending on the applicable laws and regulations, such as the General Data Protection Regulation (GDPR) in the European Union or the California Consumer

Privacy Act (CCPA) in the United States34.

The four types of legal choices mentioned in the question are:

Mandatory: The website does not allow the user to access the site unless they accept the use of cookies. This type of choice is generally considered unlawful and non-compliant with the GDPR and the CCPA34.

Implied consent: The website assumes that the user consents to the use of cookies by continuing to browse the site or by dismissing the cookie notice. This type of choice is often used by websites that operate in the U.S. or other jurisdictions that do not have strict cookie laws, but it may not be sufficient for the GDPR or the CCPA34.

Opt-in: The website requires the user to explicitly agree to the use of cookies by clicking a button or checking a box. This type of choice is usually compliant with the GDPR and the CCPA, as it ensures that the user gives informed and affirmative consent34.

Opt-out: The website allows the user to reject the use of cookies by clicking a link or changing their browser settings. This type of choice is also compliant with the GDPR and the CCPA, as it gives the user the right to withdraw their consent at any time34.

Based on the description of the cookie notice in the question, the type of legal choice that the notice provides is implied consent, as the website does not explicitly ask for the user's agreement, but rather assumes that the user accepts the use of cookies by using the site. The notice also provides a link for the user to opt out of cookies by setting their browser to refuse them.

Reference: 1: Cookie 2: Cookie Notice 3: INSIGHT: Website Cookies and Privacy—GDPR, CCPA, and Evolving Standards for Online Consent 4: Do You Need A Cookie Notice

Question: 8

SCENARIO

Please use the following to answer the next QUESTION:

Cheryl is the sole owner of Fitness Coach, Inc., a medium-sized company that helps individuals realize their physical fitness goals through classes, individual instruction, and access to an extensive indoor gym. She has owned the company for ten years and has always been concerned about protecting customer's privacy while maintaining the highest level of service. She is proud that she has built long-lasting customer relationships.

Although Cheryl and her staff have tried to make privacy protection a priority, the company has no formal privacy policy. So Cheryl hired Janice, a privacy professional, to help her develop one.

After an initial assessment, Janice created a first of a new policy. Cheryl read through the draft and was concerned about the many changes the policy would bring throughout the company. For example, the draft policy stipulates that a customer's personal information can only be held for one year after paying for a service such as a session with personal trainer. It also promises that customer information will not be shared with third parties without the written consent of the customer. The wording of these rules worry Cheryl since stored personal information often helps her company to serve her customers, even if there are long pauses between their visits. In addition, there are some third parties that provide crucial services, such as aerobics instructors who teach classes on a contract basis. Having access to customer files and understanding the fitness levels of their students helps instructors to organize their classes.

Janice understood Cheryl's concerns and was already formulating some ideas for revision. She tried to put Cheryl at ease by pointing out that customer data can still be kept, but that it should be classified according to levels of sensitivity. However, Cheryl was skeptical. It seemed that classifying data and treating each type differently would cause undue difficulties in the company's day-to-day operations. Cheryl

wants one simple data storage and access system that any employee can access if needed.

Even though the privacy policy was only a draft, she was beginning to see that changes within her company were going to be necessary. She told Janice that she would be more comfortable with implementing the new policy gradually over a period of several months, one department at a time. She was also interested in a layered approach by creating documents listing applicable parts of the new policy for each department.

What is the best reason for Cheryl to follow Janice's suggestion about classifying customer data?

A. It will help employees stay better organized
B. It will help the company meet a federal mandate
C. It will increase the security of customers' personal information (PI)
D. It will prevent the company from collecting too much personal information (PI)

Answer: C

Explanation:
Data classification systematically categorizes information based on sensitivity and importance to determine its level of confidentiality. This process helps apply appropriate security and compliance measures to ensure each category receives proper protection1. This process also helps to identify

which personal data is subject to specific GDPR requirements, such as obtaining explicit consent from data subjects, or notifying data subjects in the event of a data breach2. By classifying data, Cheryl can also make more informed decisions about where to store the information on her computer system and the nature of controls that are required based on classification3. This way, she can protect her customers' privacy while maintaining the highest level of service. Reference: Data Classification for GDPR Explained
A guide to data classification: confidential data vs. sensitive data vs. public information Why Is Data Classification Important?

Question: 9

SCENARIO
Please use the following to answer the next QUESTION:

Cheryl is the sole owner of Fitness Coach, Inc., a medium-sized company that helps individuals realize their physical fitness goals through classes, individual instruction, and access to an extensive indoor gym. She has owned the company for ten years and has always been concerned about protecting customer's privacy while maintaining the highest level of service. She is proud that she has built long-lasting customer relationships.

Although Cheryl and her staff have tried to make privacy protection a priority, the company has no formal privacy policy. So Cheryl hired Janice, a privacy professional, to help her develop one.

After an initial assessment, Janice created a first of a new policy. Cheryl read through the draft and was concerned about the many changes the policy would bring throughout the company. For example, the draft policy stipulates that a customer's personal information can only be held for one year after paying for a service such as a session with personal trainer. It also promises that customer information will not be shared with third

parties without the written consent of the customer. The wording of these rules worry Cheryl since stored personal information often helps her company to serve her customers, even if there are long pauses between their visits. In addition, there are some third parties that provide crucial services, such as aerobics instructors who teach classes on a contract basis. Having access to customer files and understanding the fitness levels of their students helps instructors to organize their classes.

Janice understood Cheryl's concerns and was already formulating some ideas for revision. She tried to put Cheryl at ease by pointing out that customer data can still be kept, but that it should be classified according to levels of sensitivity. However, Cheryl was skeptical. It seemed that classifying data and treating each type differently would cause undue difficulties in the company's day-to-day operations. Cheryl wants one simple data storage and access system that any employee can access if needed.

Even though the privacy policy was only a draft, she was beginning to see that changes within her company were going to be necessary. She told Janice that she would be more comfortable with implementing the new policy gradually over a period of several months, one department at a time. She was also interested in a layered approach by creating documents listing applicable parts of the new policy for each department.

What is the most likely risk of Fitness Coach, Inc. adopting Janice's first draft of the privacy policy?

A. Leaving the company susceptible to violations by setting unrealistic goals B. Failing to meet the needs of customers who are concerned about privacy C. Showing a lack of trust in the organization's privacy practices D. Not being in standard compliance with applicable laws

Answer: A

Explanation:

Janice's first draft of the privacy policy may be too restrictive and impractical for Fitness Coach, Inc. to follow, given the nature of its business and the expectations of its customers. By limiting the retention of personal information to one year and requiring written consent for any third-party sharing, the policy may create operational challenges and customer dissatisfaction. For example, customers may want to resume their fitness programs after a long hiatus and expect the company to have their previous records and preferences. Similarly, third-party contractors may need access to customer information to provide better services and tailor their classes. If the company fails to adhere to its own privacy policy, it may face legal consequences, reputational damage, and loss of trust from its customers. Therefore, the company should adopt a more realistic and flexible privacy policy that balances its business needs and its customers' privacy rights. Reference: Privacy Policy for Health Coaches Privacy Policies for Online Coaches Privacy Policy - Coaching.com

Question: 10

SCENARIO
Please use the following to answer the next QUESTION:

Cheryl is the sole owner of Fitness Coach, Inc., a medium-sized company that helps individuals realize their physical fitness goals through classes, individual instruction, and access to an extensive indoor gym. She has owned the company for ten years and has always been concerned about protecting customer's privacy while

maintaining the highest level of service. She is proud that she has built long-lasting customer relationships.

Although Cheryl and her staff have tried to make privacy protection a priority, the company has no formal privacy policy. So Cheryl hired Janice, a privacy professional, to help her develop one.

After an initial assessment, Janice created a first of a new policy. Cheryl read through the draft and was concerned about the many changes the policy would bring throughout the company. For example, the draft policy stipulates that a customer's personal information can only be held for one year after paying for a service such as a session with personal trainer. It also promises that customer information will not be shared with third parties without the written consent of the customer. The wording of these rules worry Cheryl since stored personal information often helps her company to serve her customers, even if there are long pauses between their visits. In addition, there are some third parties that provide crucial services, such as aerobics instructors who teach classes on a

contract basis. Having access to customer files and understanding the fitness levels of their students helps instructors to organize their classes.

Janice understood Cheryl's concerns and was already formulating some ideas for revision. She tried to put Cheryl at ease by pointing out that customer data can still be kept, but that it should be classified according to levels of sensitivity. However, Cheryl was skeptical. It seemed that classifying data and treating each type differently would cause undue difficulties in the company's day-to-day operations. Cheryl wants one simple data storage and access system that any employee can access if needed.

Even though the privacy policy was only a draft, she was beginning to see that changes within her company were going to be necessary. She told Janice that she would be more comfortable with implementing the new policy gradually over a period of several months, one department at a time. She was also interested in a layered approach by creating documents listing applicable parts of the new policy for each department.

What is the main problem with Cheryl's suggested method of communicating the new privacy policy?

A. The policy would not be considered valid if not communicated in full.
B. The policy might not be implemented consistency across departments.
C. Employees would not be comfortable with a policy that is put into action over time.
D. Employees might not understand how the documents relate to the policy as a whole.

Answer: B

Explanation:
Cheryl's suggested method of communicating the new privacy policy by creating documents listing applicable parts of the new policy for each department and implementing it gradually over several months may create confusion and inconsistency among employees and customers. Different departments may have different interpretations and expectations of the policy, and customers may not be aware of the changes or their rights under the policy. This may lead to errors, complaints, and violations of the policy and the applicable laws. A better approach would be to communicate the policy in full to all employees and customers at once, and provide training and guidance on how to comply with it. The policy should also be easily accessible and

updated on the company's website and other channels. Reference:

Privacy Policy for Health Coaches Privacy Policies for Online Coaches Privacy Policy - Coaching.com

Question: 11

SCENARIO

Please use the following to answer the next QUESTION:

Cheryl is the sole owner of Fitness Coach, Inc., a medium-sized company that helps individuals realize their physical fitness goals through classes, individual instruction, and access to an extensive indoor gym. She has owned the company for ten years and has always been concerned about protecting customer's privacy while maintaining the highest level of service. She is proud that she has built long-lasting customer relationships.

Although Cheryl and her staff have tried to make privacy protection a priority, the company has no formal privacy policy. So Cheryl hired Janice, a privacy professional, to help her develop one.

After an initial assessment, Janice created a first of a new policy. Cheryl read through the draft and was concerned about the many changes the policy would bring throughout the company. For example, the draft policy stipulates that a customer's personal information can only be held for one year after paying for a service such as a session with personal trainer. It also promises that customer information will not be shared with third parties without the written consent of the customer. The wording of these rules worry Cheryl since stored personal information often helps her company to serve her customers, even if there are long pauses between their visits. In addition, there are some third parties that provide crucial services, such as aerobics instructors who teach classes on a contract basis. Having access to customer files and understanding the fitness levels of their students helps instructors to organize their classes.

Janice understood Cheryl's concerns and was already formulating some ideas for revision. She tried to put Cheryl at ease by pointing out that customer data can still be kept, but that it should be classified according to levels of sensitivity. However, Cheryl was skeptical. It seemed that classifying data and treating each type differently would cause undue difficulties in the company's day-to-day operations. Cheryl wants one simple data storage and access system that any employee can access if needed.

Even though the privacy policy was only a draft, she was beginning to see that changes within her company were going to be necessary. She told Janice that she would be more comfortable with implementing the new policy gradually over a period of several months, one department at a time. She was also interested in a layered approach by creating documents listing applicable parts of the new policy for each department.

Based on the scenario, which of the following would have helped Janice to better meet the company's needs?

A. Creating a more comprehensive plan for implementing a new policy
B. Spending more time understanding the company's information goals
C. Explaining the importance of transparency in implementing a new policy

D. Removing the financial burden of the company's employee training program

Answer: B

Explanation:

According to the Wiley study guide, one of the steps in developing a privacy policy is to conduct a privacy assessment, which involves identifying the organization's information goals and needs, as well as the legal and regulatory requirements that apply to its data collection and use practices3. By spending more time understanding the company's information goals, Janice would have been able to tailor the privacy policy to fit the company's business model and customer expectations, while still complying with the relevant privacy laws and standards. This would have also helped Janice to address Cheryl's concerns about the impact of the policy on the company's operations and customer relationships, and to propose solutions that balance privacy protection and service delivery. Reference:

1: https://iapp.org/certify/cippus/

2: https://iapp.org/certify/get-certified/cippus/

3: https://www.wiley.com/en-be/IAPP+CIPP+US+Certified+Information+Privacy+Professional+Study+Guide-p-9781119755517

4: https://www.techtarget.com/searchsecurity/quiz/10-CIPP-US-practice-questions-to-test-your- privacy-knowledge

5: https://www.study4exam.com/iapp/free-cipp-us-questions : https://www.passitcertify.com/iapp/cipp-us-questions.html

Question: 12

According to the FTC Report of 2012, what is the main goal of Privacy by Design?

A. Obtaining consumer consent when collecting sensitive data for certain purposes
B. Establishing a system of self-regulatory codes for mobile-related services
C. Incorporating privacy protections throughout the development process
D. Implementing a system of standardization for privacy notices

Answer: C

Explanation:

Privacy by Design is a concept that the FTC endorsed in its 2012 report on protecting consumer privacy1. It seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice2. It asserts that data held by an organization ultimately belongs to the consumer and organizations should ensure that data subjects are properly informed about how their data is collected and used3. Privacy by Design requires companies to build in consumers' privacy protections at every stage in developing their products, including reasonable security for consumer data, limited collection and retention of such data, and reasonable procedures to promote data accuracy1. Reference: 1: FTC Report of 2012, p. 22-23; 2: Global Data Review3; 3: Termly4.

Question: 13

What is the main reason some supporters of the European approach to privacy are skeptical about self-regulation of privacy practices?

A. A large amount of money may have to be sent on improved technology and security

B. Industries may not be strict enough in the creation and enforcement of rules
C. A new business owner may not understand the regulations
D. Human rights may be disregarded for the sake of privacy

Answer: B

Explanation:
The European approach to privacy is based on the recognition of privacy as a fundamental human right that requires strong legal protection and oversight. The EU has adopted comprehensive and binding privacy laws, such as the General Data Protection Regulation (GDPR) and the ePrivacy Directive, that apply to all sectors and activities involving personal data. The EU also has independent data protection authorities (DPAs) that monitor and enforce compliance with the privacy laws, and a European Data Protection Board (EDPB) that issues guidance and opinions on privacy matters. The EU also requires adequate levels of privacy protection for personal data transferred to third countries or international organizations.
In contrast, the U.S. approach to privacy is based on a sectoral and self-regulatory model that relies on a combination of federal and state laws, industry codes of conduct, consumer education, and market forces. The U.S. does not have a single, comprehensive, and enforceable federal privacy law that covers all sectors and activities involving personal data. Instead, the U.S. has a patchwork of federal and state laws that address specific issues or sectors, such as health, financial, children's, and electronic communications privacy. The U.S. also has various federal and state agencies that share jurisdiction over privacy matters, such as the Federal Trade Commission (FTC), the Federal Communications Commission (FCC), and the Department of Health and Human Services (HHS). The U.S. also relies on self-regulation by industries that develop and adhere to voluntary codes of conduct, standards, and best practices for privacy. The U.S. also allows personal data to be transferred to third countries or international organizations without requiring adequate levels of privacy protection, as long as the data subjects have given their consent or the transfer is covered by a mechanism such as the Privacy Shield or the Standard Contractual Clauses.
Some supporters of the European approach to privacy are skeptical about self-regulation of privacy practices because they believe that self-regulation is not effective, consistent, or accountable enough to protect the rights and interests of data subjects. They argue that self-regulation may not provide sufficient incentives or sanctions for industries to comply with privacy rules, or to adopt privacyenhancing technologies and practices. They also contend that self-regulation may not reflect the views and expectations of data subjects, or address the emerging and complex privacy challenges posed by new technologies and business models. They also question the transparency and legitimacy of self-regulation, and the ability of data subjects to exercise their rights and seek redress for privacy violations. Reference:
IAPP CIPP/US Study Guide, Chapter 1: Introduction to the U.S. Privacy Environment, pp. 9-10, 16-17 IAPP website, CIPP/US Certification
NICCS website, Certified Information Privacy Professional/United States (CIPP/US) Training

Question: 14

What is the main purpose of the Global Privacy Enforcement Network?

A. To promote universal cooperation among privacy authorities

B. To investigate allegations of privacy violations internationally

C. To protect the interests of privacy consumer groups worldwide

D. To arbitrate disputes between countries over jurisdiction for privacy laws

Answer: A

Explanation:

The Global Privacy Enforcement Network (GPEN) is a network for privacy enforcement authorities (PEAs) to share knowledge, experience and best practices on the practical aspects of privacy enforcement and cooperation. GPEN was created in response to the OECD Recommendation on Cross-border Cooperation in the Enforcement of Laws Protecting Privacy, which called for member countries to foster the establishment of an informal network of PEAs. GPEN's main purpose is to facilitate cross-border cooperation and coordination among PEAs, especially in cases involving multiple jurisdictions or regions. GPEN also aims to enhance information sharing, promote awareness and education, and support capacity building among PEAs.

Reference:

Home (public) | Global Privacy Enforcement Network

Global Privacy Enforcement Network - International Association of Privacy Professionals International Partnerships - Office of the Privacy Commissioner of Canada

Specialised networks – Global Privacy Assembly

Action Plan for the Global Privacy Enforcement Network (GPEN)

[IAPP CIPP/US Certified Information Privacy Professional Study Guide], Chapter 6, page 213.

Question: 15

In 2014, Google was alleged to have violated the Family Educational Rights and Privacy Act (FERPA) through its Apps for Education suite of tools. For what specific practice did students sue the company?

A. Scanning emails sent to and received by students

B. Making student education records publicly available

C. Relying on verbal consent for a disclosure of education records

D. Disclosing education records without obtaining required consent

Answer: A

Explanation:

The lawsuit, filed in 2014, claimed that Google violated the federal and state wiretap and privacy laws by scanning and indexing the emails of millions of students who used its Apps for Education suite, which included

Gmail as a key feature12. The plaintiffs alleged that Google used the information from the scans to build profiles of students that could be used for targeted advertising or other commercial purposes, without their consent or knowledge12. The lawsuit also challenged Google's argument that the students consented to the scans when they first logged in to their accounts, saying that such consent was not valid under FERPA, which requires written consent for
any disclosure of education records12. Google denied the allegations and argued that the scans were necessary for providing security, spam protection, and other functionality to the users12. The case was settled in 2016, with Google agreeing to change some of its practices and policies regarding the scanning of student emails3. Reference: 1: Lawsuit Alleges That Google Has Crossed A 'Creepy Line' With Student Data, Huffington Post, 1. 2: Google faces lawsuit over email scanning and student data, The Guardian, 2. 3: Google data case to be heard in Supreme Court, BBC, 3.

Question: 16

Which venture would be subject to the requirements of Section 5 of the Federal Trade Commission Act?

A. A local nonprofit charity's fundraiser
B. An online merchant's free shipping offer
C. A national bank's no-fee checking promotion
D. A city bus system's frequent rider program

Answer: B

Explanation:
Section 5 of the Federal Trade Commission Act (FTC Act) prohibits "unfair or deceptive acts or practices in or affecting commerce."1 This prohibition applies to all persons engaged in commerce, including banks, but also exempts some entities, such as nonprofit organizations and common carriers, from FTC jurisdiction.2
Therefore, among the four options, only an online merchant's free shipping offer would be subject to the requirements of Section 5, as it involves a commercial activity that could potentially mislead or harm consumers. For example, if the online merchant fails to disclose the terms and conditions of the offer, or charges hidden fees, or delivers the products late or damaged, it could violate Section 5 by engaging in a deceptive practice.3 Reference: 1: Section 5 | Federal Trade Commission 2: Federal Trade Commission Act Section 5: Unfair or Deceptive Acts or Practices, page 13: IAPP CIPP/US Certified Information Privacy Professional Study Guide, page 23.

Question: 17

An organization self-certified under Privacy Shield must, upon request by an individual, do what?

A. Suspend the use of all personal information collected by the organization to fulfill its original purpose.
B. Provide the identities of third parties with whom the organization shares personal information.
C. Provide the identities of third and fourth parties that may potentially receive personal information.
D. Identify all personal information disclosed during a criminal investigation.

Answer: B

Explanation:

According to the Privacy Shield Principles, an organization that self-certifies under the Privacy Shield Framework must provide individuals with the choice to opt out of the disclosure of their personal information to a third party or the use of their personal information for a purpose that is materially different from the purpose for which it was originally collected or subsequently authorized by the individual. To facilitate this choice, the organization must inform the individual of the type or identity of the third parties to which it discloses personal information and the purposes for which it does so. The organization must also provide a readily available and affordable independent recourse mechanism to investigate and resolve complaints and disputes regarding its compliance with the Privacy Shield Principles. If the organization transfers personal information to a third party acting as an agent, it must ensure that the agent provides at least the same level of privacy protection as is required by the Privacy Shield Principles and that it takes reasonable and appropriate steps to ensure that the agent effectively processes the personal information transferred in a manner consistent with the organization's obligations under the Privacy Shield Principles. Reference:
Privacy Shield Principles, section II. Choice Principle and section III. Accountability for Onward Transfer Principle
[IAPP CIPP/US Study Guide], p. 67-68, section 3.2.1 and p. 69-70, section 3.2.2
[IAPP CIPP/US Body of Knowledge], p. 15-16, section C.1.b and p. 16-17, section C.1.c

Question: 18

Which of the following federal agencies does NOT enforce the Disposal Rule under the Fair and Accurate Credit Transactions Act (FACTA)?

A. The Office of the Comptroller of the Currency
B. The Consumer Financial Protection Bureau
C. The Department of Health and Human Services
D. The Federal Trade Commission

Answer: C

Explanation:

The Disposal Rule under the Fair and Accurate Credit Transactions Act (FACTA) is a federal regulation that requires any person or entity that maintains or possesses consumer information derived from consumer reports to dispose of such information in a secure and proper manner1.
The Disposal Rule aims to protect consumers from identity theft and fraud by preventing unauthorized access to or use of their personal information1.
The Disposal Rule is enforced by several federal agencies, depending on the type and sector of the entity that is subject to the rule1. These agencies include:
The Federal Trade Commission (FTC), which has general authority over most entities that are not specifically regulated by other agencies2.
The Consumer Financial Protection Bureau (CFPB), which has authority over consumer financial products and services, such as banks, credit unions, lenders, debt collectors, and credit reporting

agencies3.
The Office of the Comptroller of the Currency (OCC), which has authority over national banks and federal savings associations4.
The Federal Deposit Insurance Corporation (FDIC), which has authority over state-chartered banks that are not members of the Federal Reserve System and state-chartered savings associations5. The Board of Governors of the Federal Reserve System (FRB), which has authority over state- chartered banks that are members of the Federal Reserve System, bank holding companies, and certain nonbank subsidiaries of bank holding companies.
The National Credit Union Administration (NCUA), which has authority over federally insured credit unions.
The Securities and Exchange Commission (SEC), which has authority over brokers, dealers, investment companies, and investment advisers.
The Commodity Futures Trading Commission (CFTC), which has authority over commodity futures and options markets and intermediaries.
The Department of Health and Human Services (HHS) is NOT one of the federal agencies that enforces the Disposal Rule under FACTA. HHS has authority over health information privacy and security under the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH), but not under FACTA. Reference: 1: Disposing of Consumer Report Information? Rule Tells How 2: FTC Enforcement 3: CFPB Enforcement 4: OCC Enforcement 5: FDIC Enforcement : [FRB Enforcement] : [NCUA Enforcement] : [SEC Enforcement] : [CFTC Enforcement] : [HHS Enforcement]

Question: 19

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.

At this stage of the investigation, what should the data privacy leader review first?

A. Available data flow diagrams
B. The text of the original complaint
C. The company's data privacy policies

D. Prevailing regulation on this subject

Answer: A

Explanation:

Data flow diagrams are graphical representations of how data moves within an organization or between different entities. They can help identify the sources, destinations, and processing of personal data, as well as the legal basis, retention periods, and security measures for each data flow. Reviewing the available data flow diagrams can help the data privacy leader to quickly and accurately respond to the urgent request from the EU-based retail partner, as well as to assess the potential risks and compliance gaps in the data transfer process. Data flow diagrams are also a key component of data protection impact assessments (DPIAs), which are required by the GDPR for high-risk processing activities. Reference:
IAPP CIPP/US Body of Knowledge, Section II, A, 2 [IAPP CIPP/US Study Guide, Chapter 2, Section 2.3]
[GDPR, Article 35]

Question: 20

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?

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: 21

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.

Under the General Data Protection Regulation (GDPR), how would the U.S.-based startup company most likely be classified?

A. As a data supervisor B. As a data processor C. As a data controller D. As a data manager

Answer: B

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: 22

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.

Under the GDPR, the complainant's request regarding her personal information is known as what?

A. Right of Access
B. Right of Removal
C. Right of Rectification
D. Right to Be Forgotten

Answer: D

Explanation:
Under the GDPR, the complainant's request regarding her personal information is known as the right to be forgotten, also known as the right to erasure. This right allows individuals to ask organizations to delete their personal data in certain circumstances, such as when the data is no longer necessary, the consent is withdrawn, or the processing is unlawful. The right to be forgotten is not absolute and may not apply if the processing is necessary for legal, public interest, or legitimate purposes. The right to be forgotten also requires organizations to inform any recipients of the data about the erasure request, unless it is impossible or involves disproportionate effort. Reference:

Everything you need to know about the "Right to be forgotten"

Right to erasure | ICO

Art. 17 GDPR – Right to erasure ('right to be forgotten') - General ...

[IAPP CIPP/US Certified Information Privacy Professional Study Guide], Chapter 6, page 213.

Question: 23

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

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: 24

What is the main challenge financial institutions face when managing user preferences?

A. Ensuring they are in compliance with numerous complex state and federal privacy laws B. Developing a mechanism for opting out that is easy for their consumers to navigate C. Ensuring that preferences are applied consistently across channels and platforms
D. Determining the legal requirements for sharing preferences with their affiliates

Answer: C

Explanation:

Financial institutions (FIs) collect and process a large amount of personal data from their customers, such as name, address, account number, transaction history, credit score, etc. Customers may have different preferences regarding how their data is used, shared, or protected by the FIs. For example, some customers may want to receive marketing offers from the FIs or their affiliates, while others may opt out of such communications. Some customers may prefer to access their accounts online, while others may use mobile apps, phone calls, or physical branches. Some customers may want to enable biometric authentication, while others may rely on passwords or PINs.

Managing these diverse and dynamic user preferences is a challenge for FIs, as they need to ensure that they respect and honor the choices of their customers across all the channels and platforms they use. This requires FIs to have a robust and integrated system that can capture, store, update, and apply user preferences consistently and accurately. Failing to do so may result in customer dissatisfaction, loss of trust, regulatory fines, or legal disputes.12

Reference: 1: The Top Three Digital Challenges Faced By Financial Institutions And How To Overcome Them3, paragraph 42: IAPP CIPP/US Certified Information Privacy Professional Study Guide, page 127.

Question: 25

A large online bookseller decides to contract with a vendor to manage Personal Information (PI). What is the
least important factor for the company to consider when selecting the vendor?

A. The vendor's reputation
B. The vendor's financial health
C. The vendor's employee retention rates
D. The vendor's employee training program

Answer: C

Explanation:

When selecting a vendor to manage personal information, the company should consider various criteria, such as the vendor's reputation, financial health, employee training program, privacy policies, security practices, compliance record, contractual terms, and service quality. However, the vendor's employee retention rates may not be as important as the other factors, as they do not directly affect the vendor's ability to protect and process the personal information entrusted to them. While high employee turnover may indicate some issues with the vendor's management or culture, it may not necessarily impact the vendor's performance or reliability, as long as the vendor has adequate measures to ensure continuity, accountability, and confidentiality of the personal information they handle. Reference:

Vendor Selection Process: a Step-by-Step Guide, section "Step 2: Define the vendor selection criteria" [IAPP CIPP/US Study Guide], p. 81-82, section 3.4.1 [IAPP CIPP/US Body of Knowledge], p. 18-19, section C.2.a

Question: 26

In which situation is a company operating under the assumption of implied consent?

A. An employer contacts the professional references provided on an applicant's resume
B. An online retailer subscribes new customers to an e-mail list by default
C. A landlord uses the information on a completed rental application to run a credit report
D. A retail clerk asks a customer to provide a zip code at the check-out counter

Answer: A

Explanation:

Implied consent is a form of consent that is inferred from the actions or inactions of the data subject, rather than explicitly expressed by the data subject1.

Implied consent is generally considered a valid basis for processing personal data under certain circumstances, such as when the processing is necessary for the performance of a contract, the legitimate interests of the data controller, or the reasonable expectations of the data subject2. However, implied consent may not be sufficient for processing sensitive personal data, such as health, biometric, or genetic data, or for sending marketing communications, depending on the applicable laws and regulations2.

In the U.S., there is no comprehensive federal privacy law that regulates the use of implied consent for data processing, but there are sector-specific laws and state laws that may impose different requirements and limitations3.

Based on the scenarios given in the question, the situation that is most likely to involve a company operating under the assumption of implied consent is A. An employer contacts the professional references provided on an applicant's resume.

This is because the employer may reasonably infer that the applicant has consented to the contact of the references by voluntarily providing their information on the resume, and that the contact is necessary for the legitimate interest of the employer to verify the applicant's qualifications and suitability for the job4.

The other situations may not involve implied consent, but rather require explicit consent or provide opt-out options for the data subjects, depending on the type and purpose of the data processing and the relevant laws and regulations5 . For example:

B . An online retailer subscribes new customers to an e-mail list by default. This may violate the CANSPAM Act, which requires online marketers to obtain affirmative consent from the recipients before sending commercial e-mail messages, and to provide a clear and conspicuous opt-out mechanism in every message5.

C . A landlord uses the information on a completed rental application to run a credit report. This may violate the Fair Credit Reporting Act, which requires landlords to obtain written authorization from the applicants before obtaining their consumer reports, and to provide them with a copy of the report and a summary of their rights if they take any adverse action based on the report.

D . A retail clerk asks a customer to provide a zip code at the check-out counter. This may violate the California Song-Beverly Credit Card Act, which prohibits retailers from requesting and recording personal identification information from customers who pay with a credit card, unless the information is necessary for a special purpose, such as shipping or fraud prevention.

Reference: 1: Implied Consent 2: Consent 3: U.S. Private-Sector Privacy (CIPP/US) 4: [Reference Checks: Tips for Job Applicants and Employers] 5: [CAN-SPAM Act: A Compliance Guide for Business] : [Using Consumer Reports: What Landlords Need to Know] : [California Song-Beverly Credit Card Act] : [Reference Checks: Tips

for Job Applicants and Employers] : [CAN-SPAM Act: A Compliance Guide for Business] : [Using Consumer Reports: What Landlords Need to Know] : [California Song- Beverly Credit Card Act]

Question: 27

All of the following are tasks in the "Discover" phase of building an information management program EXCEPT?

A. Facilitating participation across departments and levels
B. Developing a process for review and update of privacy policies
C. Deciding how aggressive to be in the use of personal information
D. Understanding the laws that regulate a company's collection of information

Answer: B

Explanation:

The "Discover" phase of building an information management program is the first step in the process of creating a privacy framework. It involves identifying the types, sources, and flows of personal information within an organization, as well as the legal, regulatory, and contractual obligations that apply to it. The tasks in this phase include:

Conducting a data inventory and mapping exercise to document what personal information is collected, used, shared, and stored by the organization, and how it is protected.

Assessing the current state of privacy compliance and risk by reviewing existing policies, procedures, and practices, and identifying any gaps or weaknesses.

Understanding the laws that regulate a company's collection of information, such as the Fair Credit Reporting Act (FCRA), the Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA), and the California Consumer Privacy Act (CCPA).

Facilitating participation across departments and levels to ensure that all stakeholders are involved and informed of the privacy goals and objectives, and to foster a culture of privacy awareness and accountability.

Developing a process for review and update of privacy policies is not a task in the "Discover" phase, but rather in the "Implement" phase, which is the third step in the process of creating a privacy framework. It involves putting the privacy policies and procedures into action, and ensuring that they are effective and compliant. The tasks in this phase include:

Developing a process for review and update of privacy policies to reflect changes in the business environment, legal requirements, and best practices, and to incorporate feedback from internal and external audits and assessments.

Implementing privacy training and awareness programs to educate employees and other relevant parties on their roles and responsibilities regarding privacy, and to promote a privacy-by-design approach.

Establishing privacy governance and oversight mechanisms to monitor and measure the performance and outcomes of the privacy program, and to ensure accountability and transparency. Developing a process for responding to privacy incidents and requests from data subjects, regulators, and other parties, and to mitigate and remediate any privacy risks or harms.

Reference:

IAPP CIPP/US Body of Knowledge, Domain I: Information Management from a U.S. Perspective, Section A:

Building a Privacy Program

IAPP CIPP/US Certified Information Privacy Professional Study Guide, Chapter 1: Information Management from a U.S. Perspective, Section 1.1: Building a Privacy Program

Practice Exam - International Association of Privacy Professionals

Question: 28

Which of the following describes the most likely risk for a company developing a privacy policy with standards that are much higher than its competitors?

A. Being more closely scrutinized for any breaches of policy
B. Getting accused of discriminatory practices
C. Attracting skepticism from auditors
D. Having a security system failure

Answer: A

Explanation:

A company that develops a privacy policy with standards that are much higher than its competitors may face the risk of being more closely scrutinized for any breaches of policy by regulators, customers, media, or other stakeholders. This is because the company sets a higher expectation for its privacy practices and may be held to a higher standard of accountability and transparency. If the company fails to comply with its own policy or experiences a data breach, it may face more severe consequences, such as reputational damage, loss of trust, legal liability, or regulatory sanctions. Reference:

IAPP CIPP/US Body of Knowledge, Section I, B, 2

[IAPP CIPP/US Study Guide, Chapter 1, Section 1.4]

Question: 29

If an organization certified under Privacy Shield wants to transfer personal data to a third party acting as an agent, the organization must ensure the third party does all of the following EXCEPT?

A. Uses the transferred data for limited purposes
B. Provides the same level of privacy protection as the organization
C. Notifies the organization if it can no longer meet its requirements for proper data handling
D. Enters a contract with the organization that states the third party will process data according to the consent agreement

Answer: D

Explanation:

According to the Privacy Shield Framework, an organization that transfers personal data to a third party acting as an agent must ensure that the agent does all of the following1:

Uses the transferred data only for limited and specified purposes;

Provides the same level of privacy protection as is required by the Privacy Shield Principles;

Takes reasonable and appropriate steps to ensure that the agent effectively processes the personal information transferred in a manner consistent with the organization's obligations under the Principles;

Requires the agent to notify the organization if it makes a determination that it can no longer meet its obligation to provide the same level of protection as is required by the Principles;

Upon notice, takes reasonable and appropriate steps to stop and remediate unauthorized processing; and

Provides a summary or a representative copy of the relevant privacy provisions of its contract with that agent to the Department of Commerce upon request.

Therefore, the only option that is not required by the Privacy Shield Framework is D. Enters a contract with the organization that states the third party will process data according to the consent agreement. While the organization must obtain the individual's consent for certain types of data transfers, such as those involving sensitive data or onward transfers to controllers, the organization does not have to include the consent agreement in the contract with the agent. The contract must, however, ensure that the agent will process the data in accordance with the individual's choices and expectations, as well as the Privacy Shield Principles2.

Reference: 1: Privacy Shield Framework3, Section 3 (b); 2: Privacy Shield Framework3, Section 2 (b) and ©; 3: Privacy Shield Framework.

Question: 30

What was the original purpose of the Federal Trade Commission Act?

A. To ensure privacy rights of U.S. citizens
B. To protect consumers
C. To enforce antitrust laws
D. To negotiate consent decrees with companies violating personal privacy

Answer: C

Explanation:

The Federal Trade Commission Act (FTCA) was adopted in 1914 as part of the Progressive Era reforms that aimed to curb the power and influence of monopolies and trusts in the U.S. economy. The FTCA created the Federal Trade Commission (FTC) as an independent agency to investigate and prevent unfair methods of competition and unfair or deceptive acts or practices in or affecting commerce. The FTCA also gave the FTC the authority to issue cease and desist orders, seek injunctions, and impose civil penalties for violations of the law. The FTCA was intended to complement and supplement the existing antitrust laws, such as the Sherman Act and the Clayton Act, that prohibited restraints of trade, price-fixing, mergers, and other anticompetitive conduct.

The other options are not correct, because:

The FTCA did not explicitly address privacy rights of U.S. citizens, although the FTC later used its authority under the FTCA to enforce against unfair or deceptive privacy practices, such as making false or misleading claims, failing to disclose material information, or violating consumers' choices or expectations regarding their personal data.

The FTCA did not specifically focus on consumer protection, although the FTC later expanded its scope to

include consumer protection issues, such as advertising and marketing, credit and finance, privacy and security, and consumer education. The FTC also enforced other consumer protection laws, such as the Truth in Lending Act, the Fair Credit Reporting Act, the Children's Online Privacy Protection Act, and the CAN-SPAM Act.

The FTCA did not authorize the FTC to negotiate consent decrees with companies violating personal privacy, although the FTC later used consent decrees as a common tool to settle privacy cases and impose remedial measures, such as audits, reports, and compliance programs. Consent decrees are agreements between the FTC and the parties involved in a case that resolve the FTC's charges without admitting liability or wrongdoing.

Reference:

FTC website, Federal Trade Commission Act

Britannica website, Federal Trade Commission Act (FTCA)

IAPP CIPP/US Study Guide, Chapter 1: Introduction to the U.S. Privacy Environment, pp. 11-12 IAPP website, Federal Trade Commission Act, Section 5 of

Question: 31

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 network?" 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 Questions 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.

Based on the incident, the FTC's enforcement actions against the marketer would most likely include what violation?

A. Intruding upon the privacy of a family with young children.

B. Collecting information from a child under the age of thirteen.

C. Failing to notify of a breach of children's private information.

D. Disregarding the privacy policy of the children's marketing industry.

Answer: B

Explanation:

Based on the incident, the FTC's enforcement actions against the marketer would most likely include the violation of collecting information from a child under the age of thirteen without obtaining verifiable parental consent, as required by the Children's Online Privacy Protection Act (COPPA) Rule. The COPPA Rule applies to operators of commercial websites and online services (including mobile apps) that collect, use, or disclose personal information from children under 13, and operators of general audience websites or online services that have actual knowledge that they are collecting, using, or disclosing personal information from children under 13. The COPPA Rule also applies to

websites or online services that are directed to children under 13 and that collect personal information from users of any age. The COPPA Rule defines personal information to include full name, address, phone number, email address, date of birth, and other identifiers that permit the physical or online contacting of a specific individual. The COPPA Rule requires operators to post a clear and comprehensive online privacy policy describing their information practices for personal information collected online from children; provide direct notice to parents and obtain verifiable parental consent, with limited exceptions, before collecting personal information online from children; give parents the choice of consenting to the operator's collection and internal use of a child's information, but prohibiting the operator from disclosing that information to third parties (unless disclosure is integral to the site or service, in which case, this must be made clear to parents); provide parents access to their child's personal information to review and/or have the information deleted; give parents the opportunity to prevent further use or online collection of a child's personal information; maintain the confidentiality, security, and integrity of information they collect from children, including by taking reasonable steps to release such information only to parties capable of maintaining its confidentiality and security; and retain personal information collected online from a child for only as long as is necessary to fulfill the purpose for which it was collected and delete the information using reasonable measures to protect against its unauthorized access or use. The FTC has the authority to seek civil penalties and injunctive relief for violations of the COPPA Rule. The FTC has brought numerous enforcement actions against operators for violating the COPPA Rule, resulting in millions of dollars in penalties and orders to delete illegally collected data. Reference:

Children's Privacy | Federal Trade Commission

Kids' Privacy (COPPA) | Federal Trade Commission

FTC Is Escalating Scrutiny of Dark Patterns, Children's Privacy

FTC to Crack Down on Companies that Illegally Surveil Children Learning Online

FTC Takes Action Against Company for Collecting Children's Personal Information Without Parental Permission

[IAPP CIPP/US Certified Information Privacy Professional Study Guide], Chapter 5, pages 165-168.

Question: 32

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 network?" 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 Questions 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.

How does Matt come to the decision to report the marketer's activities?

A. The marketer failed to make an adequate attempt to provide Matt with information
B. The marketer did not provide evidence that the prize books were appropriate for children
C. The marketer seems to have distributed his son's information without Matt's permission
D. The marketer failed to identify himself and indicate the purpose of the messages

Answer: C

Explanation:
Matt's decision to report the marketer's activities is based on his suspicion that the marketer violated the Children's Online Privacy Protection Act (COPPA), which is a federal law that regulates the online collection, use, and disclosure of personal information from children under 13 years of age1. According to COPPA, operators of websites or online services that are directed to children or knowingly collect personal information from children must:
Provide notice to parents about their information practices and obtain verifiable parental consent before collecting, using, or disclosing personal information from children12.
Give parents the choice of consenting to the operator's collection and internal use of a child's information, but prohibiting the operator from disclosing that information to third parties (unless disclosure is integral to the site or service, in which case, this must be made clear to parents)12. Provide parents access to their child's personal information to review and/or have the information deleted and give parents the opportunity to prevent further use or online collection of a child's personal information12.
Maintain the confidentiality, security, and integrity of information they collect from children, including by

taking reasonable steps to release such information only to parties capable of maintaining its confidentiality and security12.
Retain personal information collected online from a child for only as long as is necessary to fulfill the purpose for which it was collected and delete the information using reasonable measures to protect against its unauthorized access or use12.
Establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children12.
In Matt's case, he did not receive any notice from the marketer about the survey or the contest, nor did he give his consent for the collection or disclosure of his son's personal information. He also did not have any access or control over his son's information or the ability to prevent further use or collection. Moreover, he noticed that his son's information seemed to have been shared with other marketers, as evidenced by the commercial emails in his son's inbox. These actions indicate that the marketer did not comply with COPPA's requirements and may have exposed his son's information to unauthorized or inappropriate parties. Therefore, Matt decided to report the marketer's activities to the proper authorities, such as the Federal Trade Commission (FTC), which enforces COPPA and can impose civil penalties for violations13. Reference: 1: Children's Online Privacy Protection Act | Federal Trade Commission, 1. 2: 16 CFR Part 312 – Children's Online Privacy Protection Rule, 3. 3: Children's Online Privacy Protection Act - Wikipedia, 2.

Question: 33

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 network?" 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 Questions 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.

How could the marketer have best changed its privacy management program to meet COPPA "Safe Harbor" requirements?

A. By receiving FTC approval for the content of its emails
B. By making a COPPA privacy notice available on website
C. By participating in an approved self-regulatory program
D. By regularly assessing the security risks to consumer privacy

Answer: C

Explanation:

The Children's Online Privacy Protection Act (COPPA) is a federal law that protects the privacy of children under 13 who use online sites and services. COPPA requires operators of such sites and services to obtain verifiable parental consent before collecting, using, or disclosing personal information from children, and to provide notice of their information practices to parents and the public. COPPA also gives parents the right to access, review, and delete their children's personal information, and to limit further collection or use of such information.1

One way for operators to comply with COPPA is to participate in an approved self-regulatory program, also known as a "safe harbor" program. These are programs that are run by industry groups or other organizations that set and enforce standards for privacy protection that meet or exceed the requirements of COPPA. Operators that join a safe harbor program and follow its guidelines are deemed to be in compliance with COPPA and are subject to the review and disciplinary procedures of the program instead of FTC enforcement actions. The FTC has approved several safe harbor programs, such as CARU, ESRB, iKeepSafe, kidSAFE, PRIVO, and TRUSTe.2

By participating in an approved self-regulatory program, the marketer in the scenario could have best changed its privacy management program to meet COPPA "Safe Harbor" requirements. This would mean that the marketer would have to adhere to the guidelines of the program, which would likely include obtaining verifiable parental consent before collecting personal information from children, providing clear and prominent privacy notices on its website and emails, honoring parents' choices and requests regarding their children's data, and ensuring the security and confidentiality of the data collected. The marketer would also benefit from the oversight and assistance of the program in ensuring compliance and resolving any complaints or disputes.3 Reference: 1: Complying with COPPA: Frequently Asked Questions4, Section A2: COPPA Safe Harbor Program3: IAPP CIPP/US Certified Information Privacy Professional Study Guide, page 143.

Question: 34

What important action should a health care provider take if the she wants to qualify for funds under the Health Information Technology for Economic and Clinical Health Act (HITECH)?

A. Make electronic health records (EHRs) part of regular care
B. Bill the majority of patients electronically for their health care
C. Send health information and appointment reminders to patients electronically
D. Keep electronic updates about the Health Insurance Portability and Accountability Act

Answer: A

Explanation:

The HITECH Act was enacted as part of the American Recovery and Reinvestment Act of 2009 to promote the adoption and use of health information technology, especially electronic health records (EHRs), in the United States. The HITECH Act established the Medicare and Medicaid EHR Incentive Programs, which provide financial incentives to eligible health care providers who demonstrate meaningful use of certified EHR technology. Meaningful use is defined as using EHRs to improve quality, safety, efficiency, and coordination of care, as well as to engage patients and protect their

privacy and security. To qualify for the incentive payments, health care providers must meet certain objectives and measures that demonstrate meaningful use of EHRs as part of their regular care.

Some of these objectives and measures include:

Protect electronic protected health information (ePHI)

Generate prescriptions electronically

Implement clinical decision support (CDS)

Use computerized provider order entry (CPOE) for medication, laboratory, and diagnostic imaging orders

Timely patient access to electronic files

Exchange health information with other providers and public health agencies

Report clinical quality measures and public health data

Therefore, the correct answer is A. Making EHRs part of regular care is an important action that a health care provider must take if she wants to qualify for funds under the HITECH Act. Reference: What is the HITECH Act? 2024 Update, section "The Meaningful Use Program"

The HITECH Act explained: Definition, compliance, and violations, section "HITECH Act definition and summary" and "Why was the HITECH Act created and why is it important?"

Proposed Rulemaking to Implement HITECH Act Modifications, section "The Health Information Technology for Economic and Clinical Health (HITECH) Act"

Health Information Technology for Economic and Clinical Health (HITECH) Audits, section "The American Recovery & Reinvestment Act of 2009 (ARRA, or Recovery Act)"

What is HITECH Compliance? Understanding and Meeting HITECH Requirements, section "HITECH Compliance Requirements"

Question: 35

All of the following organizations are specified as covered entities under the Health Insurance Portability and Accountability Act (HIPAA) EXCEPT?

A. Healthcare information clearinghouses

B. Pharmaceutical companies

C. Healthcare providers

D. Health plans

Answer: C

Explanation:

The Privacy Act of 1974 is a federal law that regulates the collection, use, and disclosure of personal

information by federal agencies.

The Privacy Act of 1974 applies to records that are maintained in a system of records, which is defined as a group of records under the control of an agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifier assigned to the individual.

The Privacy Act of 1974 grants individuals the right to access and amend their records, and requires agencies to provide notice of their systems of records, establish safeguards for the protection of the records, and limit the disclosure of the records to certain authorized purposes.

The Privacy Act of 1974 also establishes civil and criminal penalties for violations of the law, such as unauthorized disclosure, failure to publish a notice, or refusal to grant access or amendment. The Privacy Act of 1974 does NOT require agencies to obtain the consent of the individual before collecting their personal information. However, the Privacy Act of 1974 does require agencies to inform the individual of the authority for the collection, the purpose and use of the collection, and the effects of not providing the information.

Reference: : [Overview of the Privacy Act of 1974]

Question: 36

A covered entity suffers a ransomware attack that affects the personal health information (PHI) of more than 500 individuals. According to Federal law under HIPAA, which of the following would the covered entity NOT have to report the breach to?

A. Department of Health and Human Services
B. The affected individuals
C. The local media
D. Medical providers

Answer: D

Explanation:

According to the Health Insurance Portability and Accountability Act (HIPAA), a covered entity is a health plan, a health care clearinghouse, or a health care provider that transmits any health information in electronic form in connection with a transaction covered by HIPAA. A covered entity must report a breach of unsecured protected health information (PHI) to the following parties: The Department of Health and Human Services (HHS), which is the federal agency responsible for enforcing HIPAA and issuing regulations and guidance on privacy and security issues. A covered entity must notify HHS of a breach affecting 500 or more individuals without unreasonable delay and in no case later than 60 days after discovery of the breach. A covered entity must also notify HHS of breaches affecting fewer than 500 individuals within 60 days of the end of the calendar year in which the breaches occurred.

The affected individuals, who are the individuals whose PHI has been, or is reasonably believed to have been, accessed, acquired, used, or disclosed as a result of the breach. A covered entity must notify the affected individuals without unreasonable delay and in no case later than 60 days after discovery of the breach. The notification must be in writing by first-class mail or, if the individual agrees, by electronic mail. The notification must include a brief description of the breach, the types of information involved, the steps the individual should take to protect themselves, the steps the covered entity is taking to investigate and mitigate the breach, and the contact information of the covered entity.

The local media, if the breach affects more than 500 residents of a state or jurisdiction. A covered entity must

notify prominent media outlets serving the state or jurisdiction without unreasonable delay and in no case later than 60 days after discovery of the breach. The notification must include the same information as the notification to the affected individuals.

A covered entity does not have to report the breach to medical providers, unless they are also affected individuals or business associates of the covered entity. A business associate is a person or entity that performs certain functions or activities on behalf of, or provides certain services to, a

covered entity that involve the use or disclosure of PHI. A covered entity must have a written contract or agreement with its business associates that requires them to protect the privacy and security of PHI and report any breaches to the covered entity.

Reference:

IAPP CIPP/US Body of Knowledge, Domain II: Limits on Private-sector Collection and Use of Data, Section C: Sector-specific Requirements for Health Information

IAPP CIPP/US Certified Information Privacy Professional Study Guide, Chapter 2: Limits on Privatesector Collection and Use of Data, Section 2.3: Sector-specific Requirements for Health Information Practice Exam - International Association of Privacy Professionals

Question: 37

What consumer protection did the Fair and Accurate Credit Transactions Act (FACTA) require?

A. The ability for the consumer to correct inaccurate credit report information
B. The truncation of account numbers on credit card receipts
C. The right to request removal from e-mail lists
D. Consumer notice when third-party data is used to make an adverse decision

Answer: B

Explanation:

The Fair and Accurate Credit Transactions Act (FACTA) is an amendment to the Fair Credit Reporting Act (FCRA) that was enacted in 2003. FACTA aims to enhance consumer protection against identity theft and fraud by requiring various measures, such as free annual credit reports, fraud alerts, and identity theft prevention programs. One of the consumer protections that FACTA requires is the truncation of account numbers on credit card receipts. This means that only the last four or five digits of the account number can be printed on the receipt, while the rest must be masked or deleted. This reduces the risk of unauthorized access or use of the account number by third parties who may obtain the receipt. Reference:

IAPP CIPP/US Body of Knowledge, Section III, B, 1 [IAPP CIPP/US Study Guide, Chapter 3, Section 3.2] [FACTA, Section 113]

Question: 38

Who has rulemaking authority for the Fair Credit Reporting Act (FCRA) and the Fair and Accurate Credit Transactions Act (FACTA)?

A. State Attorneys General

B. The Federal Trade Commission
C. The Department of Commerce
D. The Consumer Financial Protection Bureau

Answer: D

Explanation:
The Consumer Financial Protection Bureau (CFPB) has rulemaking authority for the Fair Credit Reporting Act (FCRA) and the Fair and Accurate Credit Transactions Act (FACTA), as well as other consumer financial laws. The Dodd-Frank Act, enacted in 2010, transferred most of the rulemaking responsibilities added to the FCRA by the FACTA and the Credit CARD Act from the Federal Trade Commission (FTC) to the CFPB. However, the FTC retains its enforcement authority for the FCRA and the FACTA, along with other federal and state agencies1. The CFPB also shares rulemaking authority for some provisions of the FACTA with the FTC, such as the identity theft red flags and address discrepancy rules2. The Department of Commerce and the State Attorneys General do not have rulemaking authority for the FCRA or the FACTA. Reference: 1: FTC3, Fair Credit Reporting Act; 2: CFPB4, Fair Credit Reporting Act; 3: FTC; 4: CFPB.

Question: 39

Under the Fair and Accurate Credit Transactions Act (FACTA), what is the most appropriate action for a car dealer holding a paper folder of customer credit reports?

A. To follow the Disposal Rule by having the reports shredded
B. To follow the Red Flags Rule by mailing the reports to customers
C. To follow the Privacy Rule by notifying customers that the reports are being stored D. To follow the Safeguards Rule by transferring the reports to a secure electronic file

Answer: A

Explanation:
The Disposal Rule is a provision of the Fair and Accurate Credit Transactions Act (FACTA) that requires businesses and individuals to take appropriate measures to dispose of sensitive information about consumers, such as credit reports, that are derived from consumer reports. The Disposal Rule is intended to reduce the risk of identity theft and fraud by preventing unauthorized access to or use of the information. According to the Disposal Rule, reasonable steps for disposal include burning, pulverizing, or shredding papers that contain consumer report information so that they cannot be read or reconstructed.
In this scenario, the most appropriate action for a car dealer holding a paper folder of customer credit reports is to follow the Disposal Rule by having the reports shredded. This would ensure that the car dealer complies with the FACTA and protects the privacy and security of the customers' personal data. The other options are not correct, because:
The Red Flags Rule is another provision of the FACTA that requires financial institutions and creditors to implement a written identity theft prevention program that identifies and responds to the warning signs or red flags of identity theft in their operations. The Red Flags Rule does not apply to the disposal of consumer report information, nor does it require mailing the reports to customers, which could expose the information to interception or theft.
The Privacy Rule is a provision of the Gramm-Leach-Bliley Act (GLBA) that requires financial

institutions to provide notice to customers about their privacy policies and practices, and to allow customers to opt out of sharing their personal information with certain third parties. The Privacy Rule does not apply to the disposal of consumer report information, nor does it require notifying customers that the reports are being stored, which could alert potential identity thieves to the existence of the information.

The Safeguards Rule is another provision of the GLBA that requires financial institutions to develop, implement, and maintain a comprehensive information security program that protects the security, confidentiality, and integrity of customer information. The Safeguards Rule does not apply to the disposal of consumer report information, nor does it require transferring the reports to a secure electronic file, which could still be vulnerable to hacking or unauthorized access.

Reference:

FTC website, FACTA Disposal Rule Goes into Effect June 1

Shred Nations website, What Is the FACTA Disposal Rule?

Seam Services website, The FACTA Disposal Rule: What Does It Mean for Your Business?

IAPP CIPP/US Study Guide, Chapter 2: Limits on Private-sector Collection and Use of Data, pp. 49-50 IAPP website, Red Flags Rule

IAPP website, Fair and Accurate Credit Transactions Act (FACTA)

Question: 40

When may a financial institution share consumer information with non-affiliated third parties for marketing purposes?

A. After disclosing information-sharing practices to customers and after giving them an opportunity to opt in.

B. After disclosing marketing practices to customers and after giving them an opportunity to opt in.

C. After disclosing information-sharing practices to customers and after giving them an opportunity to opt out.

D. After disclosing marketing practices to customers and after giving them an opportunity to opt out.

Answer: C

Explanation:

According to the Gramm-Leach-Bliley Act (GLBA) and its implementing Regulation P, a financial institution may share consumer information with non-affiliated third parties for marketing purposes only after disclosing its information-sharing practices to customers and after giving them an opportunity to opt out of such sharing.

The GLBA defines a customer as a consumer who has a continuing relationship with a financial institution that provides one or more financial products or services to be used primarily for personal, family, or household purposes. A consumer is an individual who obtains or has obtained a financial product or service from a financial institution that is to be used primarily for personal, family, or household purposes, or that individual's legal representative. A non-affiliated third party is any person except a financial institution's affiliate or a person employed jointly by a financial institution and a company that is not the financial institution's affiliate. An affiliate is any company that controls, is controlled by, or is under common control with another company.

The GLBA requires that a financial institution provide a privacy notice to customers: (i) at the time of establishing the customer relationship; (ii) annually during the continuation of the customer relationship; and (iii) before disclosing any nonpublic personal information (NPI) about the customer to any non-affiliated third

party, unless an exception applies. The privacy notice must describe the categories of NPI that the financial institution collects and discloses; the categories of affiliates and non-affiliated third parties to whom the financial institution discloses NPI; the categories of NPI disclosed to service providers and joint marketers; the policies and practices with respect to protecting the confidentiality and security of NPI; and the disclosures of NPI to which the customer has a right to opt out. The financial institution must also provide a reasonable means for the customer to opt out of the disclosure of NPI to non-affiliated third parties, such as a check-off box, a reply form, or a toll-free telephone number. The opt-out notice must be clear and conspicuous, and must state that the customer can opt out at any time. The opt-out notice must also explain how the customer can opt out, and the effect of opting out. The financial institution must honor the customer's opt-out direction as soon as reasonably practicable after receiving it, and must not disclose any NPI to which the opt-out applies, unless an exception applies.

The GLBA provides several exceptions to the opt-out requirement, such as when the disclosure of NPI is necessary to effect, administer, or enforce a transaction requested or authorized by the customer; when the disclosure of NPI is required or permitted by law; when the disclosure of NPI is to a consumer reporting agency in accordance with the Fair Credit Reporting Act; or when the disclosure of NPI is to a person that performs marketing services on behalf of the financial institution or on behalf of the financial institution and another financial institution under a joint marketing agreement. A joint marketing agreement is a formal written contract between a financial institution and any other person under which the parties agree to offer, endorse, or sponsor a financial product or service. The joint marketing agreement must prohibit the other person from using or disclosing the NPI for any purpose other than offering, endorsing, or sponsoring the financial product or service covered by the agreement.

The GLBA also requires that a financial institution provide a privacy notice to consumers who are not customers before disclosing any NPI about the consumer to any non-affiliated third party, unless an exception applies. The financial institution does not need to provide an opt-out notice to consumers who are not customers, unless it has a customer relationship with them. However, if the financial institution establishes a customer relationship with a consumer who was previously not a customer, it must provide a privacy notice and an opt-out notice to the customer as described above. Reference:

Guide to the Gramm–Leach–Bliley Act

GLBA or FCRA? Data Sharing Between Affiliates and Non-Affiliates Existing Privacy Laws Already Regulate Information Sharing Why Do Banks Share Your Financial Information and Are They Allowed To?

[IAPP CIPP/US Certified Information Privacy Professional Study Guide], Chapter 5, pages 161-165.

Question: 41

What are banks required to do under the Gramm-Leach-Bliley Act (GLBA)?

A. Conduct annual consumer surveys regarding satisfaction with user preferences
B. Process requests for changes to user preferences within a designated time frame
C. Provide consumers with the opportunity to opt out of receiving telemarketing phone calls
D. Offer an Opt-Out before transferring PI to an unaffiliated third party for the latter's own use

Answer: D

Explanation:

The Gramm-Leach-Bliley Act (GLBA) is a federal law that regulates the privacy and security of consumer

financial information collected, used, and disclosed by financial institutions, such as banks, credit unions, securities firms, insurance companies, and others12. Under the GLBA, financial institutions must comply with two main rules: the Privacy Rule and the Safeguards Rule12. The Privacy Rule requires financial institutions to provide notice to their customers about their information-sharing practices and to obtain verifiable parental consent before collecting, using, or disclosing personal information from children12. The Privacy Rule also gives customers the right to opt out of having their personal information shared with certain nonaffiliated third parties, unless an exception applies12. The Safeguards Rule requires financial institutions to develop, implement, and maintain a comprehensive information security program that protects the confidentiality, security, and integrity of customer information12.

Therefore, banks and other financial institutions are required to offer an opt-out before transferring personal information (PI) to an unaffiliated third party for the latter's own use, unless an exception applies, such as when the disclosure is necessary to complete a transaction requested or authorized by the customer, or when the disclosure is to a service provider or joint marketer that agrees to protect the information and use it only for the purposes for which it was disclosed12. This requirement is intended to give customers more control over how their personal information is used and shared by financial institutions and to protect their privacy rights12.

Reference: 1: Gramm-Leach-Bliley Act | Federal Trade Commission, 1. 2: How To Comply with the Privacy of Consumer Financial Information Rule of the Gramm-Leach-Bliley Act | Federal Trade Commission, 2.

Question: 42

SCENARIO

Please use the following to answer the next QUESTION:

Declan has just started a job as a nursing assistant in a radiology department at Woodland Hospital. He has also started a program to become a registered nurse.

Before taking this career path, Declan was vaguely familiar with the Health Insurance Portability and Accountability Act (HIPAA). He now knows that he must help ensure the security of his patients' Protected Health Information (PHI). Therefore, he is thinking carefully about privacy issues.

On the morning of his first day, Declan noticed that the newly hired receptionist handed each patient a HIPAA privacy notice. He wondered if it was necessary to give these privacy notices to returning patients, and if the radiology department could reduce paper waste through a system of one-time distribution.

He was also curious about the hospital's use of a billing company. He questioned whether the hospital was doing all it could to protect the privacy of its patients if the billing company had details about patients' care.

On his first day Declan became familiar with all areas of the hospital's large radiology department. As he was organizing equipment left in the halfway, he overheard a conversation between two hospital administrators. He was surprised to hear that a portable hard drive containing non-encrypted patient information was missing. The administrators expressed relief that the hospital would be able to avoid liability. Declan was surprised, and wondered whether the hospital had plans to properly report what had happened.

Despite Declan's concern about this issue, he was amazed by the hospital's effort to integrate Electronic Health Records (EHRs) into the everyday care of patients. He thought about the potential for streamlining care even more if they were accessible to all medical facilities nationwide.

Declan had many positive interactions with patients. At the end of his first day, he spoke to one patient, John, whose father had just been diagnosed with a degenerative muscular disease. John was about to get blood work done, and he feared that the blood work could reveal a genetic predisposition to the disease that could affect his ability to obtain insurance coverage. Declan told John that he did not think that was possible, but the patient was wheeled away before he could explain why. John plans to ask a colleague about this.

In one month, Declan has a paper due for one his classes on a health topic of his choice. By then, he will have had many interactions with patients he can use as examples. He will be pleased to give credit to John by name for inspiring him to think more carefully about genetic testing.

Although Declan's day ended with many Questions, he was pleased about his new position.

What is the most likely way that Declan might directly violate the Health Insurance Portability and Accountability Act (HIPAA)?

A. By being present when patients are checking in
B. By speaking to a patient without prior authorization
C. By ignoring the conversation about a potential breach
D. By following through with his plans for his upcoming paper

Answer: D

Explanation:
Declan might directly violate the HIPAA Privacy Rule by using John's name and personal health information (PHI) in his paper without his written authorization. The Privacy Rule protects the confidentiality of PHI that is created, received, maintained, or transmitted by a covered entity or its business associate. PHI includes any information that relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual1. Declan, as a nursing assistant, is part of the covered entity's workforce and must comply with the Privacy Rule. He cannot disclose John's PHI to anyone, including his classmates or instructors, without John's authorization or a valid exception under the Privacy Rule. Even if he does

not use John's full name, he may still reveal enough information to make John identifiable, such as his diagnosis, his father's condition, or his location. This would be an impermissible use and disclosure of PHI, and a potential HIPAA violation. Declan should either obtain John's written authorization to use his PHI in his paper, or de-identify the information according to the Privacy Rule's standards2. Reference:
Summary of the HIPAA Privacy Rule
Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule

Question: 43

SCENARIO

Please use the following to answer the next QUESTION:

Declan has just started a job as a nursing assistant in a radiology department at Woodland Hospital. He has also started a program to become a registered nurse.

Before taking this career path, Declan was vaguely familiar with the Health Insurance Portability and Accountability Act (HIPAA). He now knows that he must help ensure the security of his patients' Protected Health Information (PHI). Therefore, he is thinking carefully about privacy issues.

On the morning of his first day, Declan noticed that the newly hired receptionist handed each patient a HIPAA privacy notice. He wondered if it was necessary to give these privacy notices to returning patients, and if the radiology department could reduce paper waste through a system of one-time distribution.

He was also curious about the hospital's use of a billing company. He Questioned whether the hospital was doing all it could to protect the privacy of its patients if the billing company had details about patients' care.

On his first day Declan became familiar with all areas of the hospital's large radiology department. As he was organizing equipment left in the halfway, he overheard a conversation between two hospital administrators. He was surprised to hear that a portable hard drive containing non-encrypted patient information was missing. The administrators expressed relief that the hospital would be able to avoid liability. Declan was surprised, and wondered whether the hospital had plans to properly report what had happened.

Despite Declan's concern about this issue, he was amazed by the hospital's effort to integrate Electronic Health Records (EHRs) into the everyday care of patients. He thought about the potential for streamlining care even more if they were accessible to all medical facilities nationwide.

Declan had many positive interactions with patients. At the end of his first day, he spoke to one patient, John, whose father had just been diagnosed with a degenerative muscular disease. John was about to get blood work done, and he feared that the blood work could reveal a genetic predisposition to the disease that could affect his ability to obtain insurance coverage. Declan told John that he did not think that was possible, but the patient was wheeled away before he could explain why. John plans to ask a colleague about this.

In one month, Declan has a paper due for one his classes on a health topic of his choice. By then, he will have had many interactions with patients he can use as examples. He will be pleased to give credit to John by name for inspiring him to think more carefully about genetic testing.

Although Declan's day ended with many Questions, he was pleased about his new position.

How can the radiology department address Declan's concern about paper waste and still comply with the Health Insurance Portability and Accountability Act (HIPAA)?

A. State the privacy policy to the patient verbally
B. Post the privacy notice in a prominent location instead
C. Direct patients to the correct area of the hospital website
D. Confirm that patients are given the privacy notice on their first visit

Answer: D

Explanation:

HIPAA requires covered entities to provide a notice of privacy practices (NPP) to individuals who receive health care services from the covered entity. The NPP must describe how the covered entity may use and disclose protected health information (PHI), the individual's rights with respect to their PHI, and the covered entity's obligations to protect the privacy of PHI. The NPP must be provided to the individual no later than the date of the first service delivery, either in person or electronically. The covered entity must also make the NPP available on request and post it on its website if it has one. The covered entity must also make a good faith effort to obtain a written acknowledgment from the individual that they received the NPP. If the individual refuses to sign the acknowledgment, the covered entity must document the attempt and the reason for the refusal.

The other options are not sufficient to comply with HIPAA. Stating the privacy policy verbally (option A) does not provide the individual with a written or electronic copy of the NPP that they can keep for future reference. Posting the privacy notice in a prominent location (option B) does not ensure that the individual receives the NPP or has an opportunity to review it before receiving services. Directing patients to the correct area of the hospital website (option C) does not provide the individual with the NPP at the time of service delivery, unless the individual agrees to receive the NPP electronically and has access to the website at that time.

Reference:

Notice of Privacy Practices for Protected Health Information

Model Notices of Privacy Practices

Sample Notice: Availability of Notice of Privacy Practices

Notice of Privacy Practices

Notice of Privacy Practices (NPP) Distribution and Acknowledgement

Question: 44

SCENARIO

Please use the following to answer the next QUESTION:

Declan has just started a job as a nursing assistant in a radiology department at Woodland Hospital. He has also started a program to become a registered nurse.

Before taking this career path, Declan was vaguely familiar with the Health Insurance Portability and Accountability Act (HIPAA). He now knows that he must help ensure the security of his patients' Protected Health Information (PHI). Therefore, he is thinking carefully about privacy issues.

On the morning of his first day, Declan noticed that the newly hired receptionist handed each patient a HIPAA privacy notice. He wondered if it was necessary to give these privacy notices to returning patients, and if the radiology department could reduce paper waste through a system of one-time distribution.

He was also curious about the hospital's use of a billing company. He Questioned whether the hospital was doing all it could to protect the privacy of its patients if the billing company had details about patients' care.

On his first day Declan became familiar with all areas of the hospital's large radiology department. As he was

organizing equipment left in the halfway, he overheard a conversation between two hospital administrators. He was surprised to hear that a portable hard drive containing non-encrypted patient information was missing. The administrators expressed relief that the hospital would be able to avoid liability. Declan was surprised, and wondered whether the hospital had plans to properly report what had happened.

Despite Declan's concern about this issue, he was amazed by the hospital's effort to integrate Electronic Health Records (EHRs) into the everyday care of patients. He thought about the potential for streamlining care even more if they were accessible to all medical facilities nationwide.

Declan had many positive interactions with patients. At the end of his first day, he spoke to one patient, John, whose father had just been diagnosed with a degenerative muscular disease. John was about to get blood work done, and he feared that the blood work could reveal a genetic predisposition to the disease that could affect his ability to obtain insurance coverage. Declan told John that he did not think that was possible, but the patient was wheeled away before he could explain why. John plans to ask a colleague about this.

In one month, Declan has a paper due for one his classes on a health topic of his choice. By then, he will have had many interactions with patients he can use as examples. He will be pleased to give credit to John by name for inspiring him to think more carefully about genetic testing.

Although Declan's day ended with many Questions, he was pleased about his new position.

Based on the scenario, what is the most likely way Declan's supervisor would answer his question about the hospital's use of a billing company?

A. By suggesting that Declan look at the hospital's publicly posted privacy policy
B. By assuring Declan that third parties are prevented from seeing Private Health Information (PHI) C. By pointing out that contracts are in place to help ensure the observance of minimum security standards

D. By describing how the billing system is integrated into the hospital's electronic health records (EHR) system

Answer: C

Explanation:

HIPAA requires covered entities, such as hospitals, to enter into contracts with their business associates, such as billing companies, that access, use, or disclose protected health information (PHI). These contracts, known as business associate agreements (BAAs), must specify the permitted and required uses and disclosures of PHI by the business associate, as well as the safeguards, reporting, and termination procedures that the business associate must follow to protect the privacy and security of PHI. By having these contracts in place, the hospital can ensure that the billing company is complying with HIPAA and observing the minimum security standards required by law. Reference:

HIPAA Rules for Medical Billing - Compliancy Group
HIPAA Compliance for Billing Companies: Easy Guide - iFax

Question: 45

Which entities must comply with the Telemarketing Sales Rule?

A. For-profit organizations and for-profit telefunders regarding charitable solicitations
B. Nonprofit organizations calling on their own behalf
C. For-profit organizations calling businesses when a binding contract exists between them
D. For-profit and not-for-profit organizations when selling additional services to establish customers

Answer: A

Explanation:

The Telemarketing Sales Rule (TSR) is a federal regulation that applies to telemarketing calls, which are defined as "a plan, program, or campaign which is conducted to induce the purchase of goods or services or a charitable contribution, by use of one or more telephones and which involves more than one interstate telephone call."1 The TSR requires telemarketers to make specific disclosures, prohibit misrepresentations, limit the times and number of calls, and set payment restrictions for the sale of certain goods and services. The TSR also gives consumers the right to opt out of receiving telemarketing calls by registering their phone numbers on the National Do Not Call Registry.2 The TSR applies to both for-profit and not-for-profit organizations, but there are some exemptions and partial exemptions for certain types of entities, calls, and transactions. For example, the TSR does not apply to nonprofit organizations calling on their own behalf, as they are not considered to be engaged in telemarketing. However, if a nonprofit organization hires a for-profit telemarketer or telefunder to solicit charitable contributions on its behalf, the for-profit entity must comply with the TSR, as it is engaged in telemarketing. Similarly, the TSR does not apply to for-profit organizations

calling businesses when a binding contract exists between them, as they are not considered to be inducing the purchase of goods or services. However, if a for-profit organization calls businesses to sell additional services to established customers, the TSR applies, as it is considered to be inducing the purchase of goods or services.3

Therefore, among the four options, only for-profit organizations and for-profit telefunders regarding charitable solicitations must comply with the TSR, as they are engaged in telemarketing and do not fall under any of the exemptions or partial exemptions. Reference: 1: eCFR :: 16 CFR Part 310 – Telemarketing Sales Rule3, Section 310.22: Telemarketing Sales Rule | Federal Trade Commission1, Rule Summary3: Complying with the Telemarketing Sales Rule - Federal Trade Commission2, Exemptions to the TSR.

Question: 46

Under the Telemarketing Sales Rule, what characteristics of consent must be in place for an organization to acquire an exception to the Do-Not-Call rules for a particular consumer?

A. The consent must be in writing, must state the times when calls can be made to the consumer and must be signed
B. The consent must be in writing, must contain the number to which calls can be made and must have an

end date

C. The consent must be in writing, must contain the number to which calls can be made and must be signed
D. The consent must be in writing, must have an end data and must state the times when calls can be made

Answer: C

Explanation:
The Telemarketing Sales Rule (TSR) is a federal regulation that applies to telemarketing calls, which are defined as "a plan, program, or campaign which is conducted to induce the purchase of goods or services or a charitable contribution, by use of one or more telephones and which involves more than one interstate telephone call."1 The TSR requires telemarketers to make specific disclosures, prohibit misrepresentations, limit the times and number of calls, and set payment restrictions for the sale of certain goods and services. The TSR also gives consumers the right to opt out of receiving telemarketing calls by registering their phone numbers on the National Do Not Call Registry.2 The TSR applies to both for-profit and not-for-profit organizations, but there are some exemptions and partial exemptions for certain types of entities, calls, and transactions. For example, the TSR does not apply to nonprofit organizations calling on their own behalf, as they are not considered to be engaged in telemarketing. However, if a nonprofit organization hires a for-profit telemarketer or telefunder to solicit charitable contributions on its behalf, the for-profit entity must comply with the TSR, as it is engaged in telemarketing. Similarly, the TSR does not apply to for-profit organizations calling businesses when a binding contract exists between them, as they are not considered to be inducing the purchase of goods or services. However, if a for-profit organization calls businesses to sell additional services to established customers, the TSR applies, as it is considered to be inducing the purchase of goods or services.3
Therefore, among the four options, only for-profit organizations and for-profit telefunders regarding

charitable solicitations must comply with the TSR, as they are engaged in telemarketing and do not fall under any of the exemptions or partial exemptions. Reference: 1: eCFR :: 16 CFR Part 310 – Telemarketing Sales Rule3, Section 310.22: Telemarketing Sales Rule | Federal Trade Commission1, Rule Summary3: Complying with the Telemarketing Sales Rule - Federal Trade Commission2, Exemptions to the TSR.

Question: 47

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

Answer: A

Explanation:
The Telemarketing Sales Rule (TSR) is a federal regulation that implements the Telemarketing and Consumer Fraud and Abuse Prevention Act of 1994. The TSR aims to protect consumers from deceptive or abusive

telemarketing practices, such as unwanted calls, false or misleading claims, unauthorized billing, and privacy violations1.

The TSR requires telemarketers and sellers to comply with the National Do Not Call Registry, which is a list of phone numbers of consumers who have indicated that they do not want to receive telemarketing calls2.

The TSR also requires telemarketers and sellers to honor the do-not-call requests of individual consumers, regardless of whether their numbers are on the National Do Not Call Registry or not2. A do-not-call request is a statement made by a consumer, either orally or in writing, that they do not wish to receive any more calls from a specific telemarketer or seller2.

The TSR requires an entity to share a do-not-call request across its organization when the operational structures of its divisions are not transparent to consumers3. This means that the entity must treat the do-not-call request as if it applies to all of its affiliates and subsidiaries that engage in telemarketing, unless the consumer would reasonably expect them to be separate and distinct entities based on their names, products, or services3.

The TSR does not require an entity to share a do-not-call request across its organization in the following situations:

When the goods and services sold by its divisions are very similar. This is not a relevant factor for determining whether the entity must share a do-not-call request across its organization. The key factor is whether the consumers can distinguish between the different divisions based on their operational structures3.

When a call is not the result of an error or other unforeseen cause. This is not an exception to the requirement to honor a do-not-call request. The TSR prohibits telemarketers and sellers from calling a consumer who has made a do-not-call request, unless the call falls under one of the specific exemptions, such as calls from or on behalf of tax-exempt nonprofit organizations, calls to consumers with whom the seller has an established business relationship, or calls to consumers who have given prior express written consent2.

When the entity manages user preferences through multiple platforms. This is not an excuse for not sharing a do-not-call request across its organization. The TSR requires telemarketers and sellers to maintain an internal do-not-call list of consumers who have asked them not to call again, and to update the list at least once every 31 days2. The entity must ensure that the do-not-call request is recorded and communicated across all of its platforms that are used for telemarketing purposes3. Reference: 1: Telemarketing Sales Rule 2: Q&A for Telemarketers & Sellers About DNC Provisions in TSR 3: Federal Register :: Telemarketing Sales Rule

Question: 48

Within what time period must a commercial message sender remove a recipient's address once they have asked to stop receiving future e-mail?

A. 7 days
B. 10 days
C. 15 days
D. 21 days

Answer: B

Explanation:

According to the CAN-SPAM Act of 2003, a federal law that regulates commercial email messages, a commercial message sender must honor a recipient's opt-out request within 10 business days. The sender must provide a clear and conspicuous way for the recipient to opt out of receiving future emails, such as a link or an email address. The sender must not charge a fee, require the recipient to provide any personal information, or make the recipient take any steps other than sending a reply email or visiting a single web page to opt out. The sender must also not sell, exchange, or transfer the email address of the recipient who has opted out, unless it is necessary to comply with the law or prevent fraud.

Reference:

IAPP CIPP/US Body of Knowledge, Domain II: Limits on Private-sector Collection and Use of Data, Section B: Communications and Marketing

IAPP CIPP/US Certified Information Privacy Professional Study Guide, Chapter 2: Limits on Privatesector Collection and Use of Data, Section 2.2: Communications and Marketing Practice Exam - International Association of Privacy Professionals

Question: 49

A student has left high school and is attending a public postsecondary institution. Under what condition may a school legally disclose educational records to the parents of the student without consent?

A. If the student has not yet turned 18 years of age
B. If the student is in danger of academic suspension
C. If the student is still a dependent for tax purposes
D. If the student has applied to transfer to another institution

Answer: C

Explanation:

The Family Educational Rights and Privacy Act (FERPA) is a federal law that protects the privacy of students' educational records. FERPA generally requires schools to obtain written consent from students before disclosing their records to third parties, such as parents. However, FERPA allows some exceptions to this rule, such as when the disclosure is for health or safety emergencies, or when the student is still a dependent for tax purposes. According to FERPA, a school may disclose educational records to the parents of a student who is claimed as a dependent on the parents' most recent federal income tax return, without the student's consent. This exception applies regardless of the student's age or enrollment status at a postsecondary institution.

Reference: IAPP CIPP/US Body of Knowledge, Section III, C, 2 [IAPP CIPP/US Study Guide, Chapter 3, Section 3.5] [FERPA, 34 CFR § 99.31(a)(8)]

Question: 50

In what way does the "Red Flags Rule" under the Fair and Accurate Credit Transactions Act (FACTA) relate to the owner of a grocery store who uses a money wire service?

A. It mandates the use of updated technology for securing credit records
B. It requires the owner to implement an identity theft warning system
C. It is not usually enforced in the case of a small financial institution
D. It does not apply because the owner is not a creditor

Answer: D

Explanation:

The Red Flags Rule is a regulation that requires financial institutions and creditors to implement a written identity theft prevention program that is designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account1. A creditor is any person who regularly extends, renews, or continues credit; any person who regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who participates in the decision to extend, renew, or continue credit2. A covered account is an account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a credit card account, mortgage loan, automobile loan, margin account, cell phone account, utility account, checking account, or savings account2. A money wire service is a service that allows customers to send or receive money electronically3. The owner of a grocery store who uses a money

wire service is not a creditor because he or she does not regularly extend, renew, or continue credit to customers. Therefore, the Red Flags Rule does not apply to the owner of a grocery store who uses a money wire service. Reference:

1: FTC, Red Flags Rule, https://www.ftc.gov/business-guidance/privacy-security/red-flags-rule

2: FTC, Fighting Identity Theft with the Red Flags Rule: A How-To Guide for Business, https://www.ftc.gov/tips-advice/business-center/guidance/fighting-identity-theft-red-flags-rule- how-guide-business

3: Alessa, Wire Transfer Red Flags: Understanding Money Laundering and Fraud Risks, https://alessa.com/webinars/wire-transfer-red-flags-and-fraud-risks/

Question: 51

Which of the following is an important implication of the Dodd-Frank Wall Street Reform and Consumer Protection Act?

A. Financial institutions must avoid collecting a customer's sensitive personal information
B. Financial institutions must help ensure a customer's understanding of products and services
C. Financial institutions must use a prescribed level of encryption for most types of customer records D. Financial institutions must cease sending e-mails and other forms of advertising to customers who opt out of direct marketing

Answer: B

Explanation:

The Dodd-Frank Act created the Consumer Financial Protection Bureau (CFPB) as an independent agency within the Federal Reserve System. The CFPB has the authority to regulate consumer financial products and services, such as mortgages, credit cards, student loans, and payday loans. One of the main objectives of the CFPB is to promote transparency, fairness, and consumer choice in the financial marketplace. The CFPB has issued rules and guidance to require financial institutions to provide clear and accurate information to consumers about the costs, risks, and benefits of their products and services. The CFPB also has the power to enforce consumer protection laws and prohibit unfair, deceptive, or abusive acts or practices by

financial institutions123 Reference: 1: Dodd-Frank Wall Street Reform and Consumer Protection Act, Title X, Subtitle A, Section 1011. 2: Consumer Financial Protection Bureau, Wikipedia. 3: Dodd-Frank Act: What It Does, Major Components, and Criticisms, Investopedia.

Question: 52

Which act violates the Family Educational Rights and Privacy Act of 1974 (FERPA)?

A. A K-12 assessment vendor obtains a student's signed essay about her hometown from her school to use as an exemplar for public release

B. A university posts a public student directory that includes names, hometowns, e-mail addresses, and majors

C. A newspaper prints the names, grade levels, and hometowns of students who made the quarterly honor roll

D. University police provide an arrest report to a student's hometown police, who suspect him of a similar crime

Answer: A

Explanation:

The Family Educational Rights and Privacy Act of 1974 (FERPA) is a federal law that protects the privacy of student education records. FERPA grants parents or eligible students the right to access, amend, and control the disclosure of their education records, with some exceptions. Schools must obtain written consent from the parent or eligible student before disclosing any personally identifiable information from the education records, unless an exception applies123

Option A violates FERPA because it involves the disclosure of a student's personally identifiable information (PII) from the education records without consent. A student's signed essay about her hometown is considered an education record under FERPA, as it is directly related to the student and maintained by the school12 A K-12 assessment vendor is not a school official with a legitimate educational interest, nor does it fall under any of the exceptions that allow disclosure without consent12 Therefore, the school must obtain the student's (or the parent's, if the student is a minor) written consent before providing the essay to the vendor for public release.

Option B does not violate FERPA because it involves the disclosure of directory information, which is not considered PII under FERPA. Directory information is information that would not generally be considered harmful or an invasion of privacy if disclosed, such as name, address, phone number, email address, major, etc12 Schools may disclose directory information without consent, unless the parent or eligible student has opted out of such disclosure12 However, schools must notify parents and eligible students of the types of directory information they designate and their right to opt out annually12

Option C does not violate FERPA because it involves the disclosure of information that is not part of the education records. FERPA only applies to education records that are directly related to a student and maintained by the school or a party acting for the school12 A newspaper's publication of the names, grade levels, and hometowns of students who made the quarterly honor roll is not based on the education records, but on the newspaper's own sources and reporting. Therefore, FERPA does not prohibit such disclosure.

Option D does not violate FERPA because it involves the disclosure of information under an exception that allows disclosure without consent. FERPA permits schools to disclose education records, or PII from education records, without consent to comply with a judicial order or lawfully issued subpoena, or to appropriate officials

in connection with a health or safety emergency123 If the university police provide an arrest report to the student's hometown police in response to a subpoena or to prevent a serious threat to the student or others, they are not violating FERPA.

Reference: 1: Family Educational Rights and Privacy Act - Wikipedia 2: Family Educational Rights and Privacy Act (FERPA) | CDC 3: What is FERPA? | Protecting Student Privacy - ed

Question: 53

According to FERPA, when can a school disclose records without a student's consent?

A. If the disclosure is not to be conducted through email to the third party
B. If the disclosure would not reveal a student's student identification number
C. If the disclosure is to practitioners who are involved in a student's health care
D. If the disclosure is to provide transcripts to a school where a student intends to enroll

Answer: D

Explanation:

According to FERPA, a school may disclose personally identifiable information (PII) from an eligible student's education records without consent if the disclosure meets one of the exceptions in 34 CFR § 99.31. One of these exceptions is for disclosures to other schools to which a student seeks or intends to enroll, or is already enrolled if the disclosure is for purposes related to the student's enrollment or transfer (34 CFR § 99.31(a)(2)). This exception allows schools to disclose transcripts, recommendations, or other information that may facilitate the student's admission or enrollment at another school. However, the school must make a reasonable attempt to notify the student of the disclosure, unless the student initiated the disclosure, and must provide the student with a copy of the records that were disclosed upon request (34 CFR § 99.34(a)(1)). Reference: https://studentprivacy.ed.gov/ferpa https://studentprivacy.ed.gov/ferpa

Question: 54

What is the main purpose of the CAN-SPAM Act?

A. To diminish the use of electronic messages to send sexually explicit materials
B. To authorize the states to enforce federal privacy laws for electronic marketing
C. To empower the FTC to create rules for messages containing sexually explicit content
D. To ensure that organizations respect individual rights when using electronic advertising

Answer: D

Explanation:

The CAN-SPAM Act is a federal law that sets the rules for commercial email, establishes requirements for commercial messages, gives recipients the right to have you stop emailing them, and spells out tough penalties for violations1. The main purpose of the act is to protect consumers from unwanted and deceptive email messages and to give them more control over their online privacy2. The act applies to all commercial messages, which are defined as "any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service"1. The act does not apply to transactional or

relationship messages, which are messages that facilitate an agreed-upon transaction or update a customer about an existing business relationship1. The act also does not apply to non-commercial messages, such as political or charitable solicitations3. Reference: 1: CAN-SPAM Act: A Compliance Guide for Business2: What is the CAN-SPAM Act? | Proton3: What is the CAN-SPAM Act? | Cloudflare

Question: 55

The Video Privacy Protection Act of 1988 restricted which of the following?

A. Which purchase records of audio visual materials may be disclosed B. When downloading of copyrighted audio visual materials is allowed C. When a user's viewing of online video content can be monitored D. Who advertisements for videos and video games may target

Answer: A

Explanation:
The VPPA was enacted to prevent the wrongful disclosure of personally identifiable information (PII) concerning any consumer of a video tape service provider. PII includes information that identifies a person as having requested or obtained specific video materials or services from a video tape service provider. The VPPA prohibits such disclosure, except in certain limited circumstances, such as with the consumer's informed, written consent, or pursuant to a law enforcement warrant, subpoena, or court order. The VPPA also allows the disclosure of the names and addresses of consumers, but not the title, description, or subject matter of any video tapes or other audio visual material, for the exclusive use of marketing goods and services directly to the consumer, unless the consumer has opted out of such disclosure. The other options (B, C, and D) are not restricted by the VPPA. Reference:
Video Privacy Protection Act - Wikipedia
18 U.S. Code § 2710 - Wrongful disclosure of video tape rental or sale records | U.S. Code | US Law | LII / Legal Information Institute
IAPP CIPP/US Certified Information Privacy Professional Study Guide, Chapter 3: Federal Privacy Laws and Regulations, Section 3.5: Video Privacy Protection Act (VPPA)

Question: 56

The Cable Communications Policy Act of 1984 requires which activity?

A. Delivery of an annual notice detailing how subscriber information is to be used
B. Destruction of personal information a maximum of six months after it is no longer needed
C. Notice to subscribers of any investigation involving unauthorized reception of cable services
D. Obtaining subscriber consent for disseminating any personal information necessary to render cable services

Answer: A

Explanation:
The Cable Communications Policy Act of 1984 (CCPA) is a federal law that regulates the cable television industry and protects the privacy of cable subscribers. One of the provisions of the CCPA is that cable operators must provide their subscribers with an annual notice that clearly and conspicuously informs them of the following information12:

The nature of personally identifiable information collected or to be collected with respect to the subscriber and the nature of the use of such information

The nature, frequency, and purpose of any disclosure of such information, including an identification of the types of persons to whom the disclosure may be made

The period during which such information will be maintained by the cable operator

The times and place at which the subscriber may have access to such information

The limitations provided by the CCPA with respect to the collection and disclosure of information by a cable operator and the right of the subscriber under the CCPA to enforce such limitations

The annual notice must also state that the subscriber has the right to prevent disclosure of personally identifiable information to third parties, except as required by law or court order, and that the subscriber may sue for damages, attorney's fees, and other relief for violations of the CCPA12. Reference: 1: Cable Communications Policy Act of 1984, Section 631 2: [IAPP CIPP/US Study Guide], Chapter 8, Section 8.3.2

Question: 57

What is the main purpose of requiring marketers to use the Wireless Domain Registry?

A. To access a current list of wireless domain names
B. To prevent unauthorized emails to mobile devices
C. To acquire authorization to send emails to mobile devices
D. To ensure their emails are sent to actual wireless subscribers

Answer: B

Explanation:
The Wireless Domain Registry is a list of domain names that are used to transmit electronic messages to wireless devices, such as cell phones and pagers. The purpose of the registry is to protect wireless consumers from unwanted commercial electronic mail messages, by identifying the domain names for those who send such messages. Marketers are required to use the registry to avoid sending unsolicited emails to wireless devices, which may incur costs or inconvenience for the recipients. Sending such emails without the express prior authorization of the recipient is a violation of the CAN-SPAM Act of 2003. Reference: https://www.fcc.gov/cgb/policy/domain-name-input https://www.prnewswire.com/in/news-releases/the-wireless-registry-launches-worlds-first-global- registry-for-wireless-names-240222521.html

Question: 58

SCENARIO
Please use the following to answer the next QUESTION:

You are the chief privacy officer at HealthCo, a major hospital in a large U.S. city in state A. HealthCo is a HIPAA-covered entity that provides healthcare services to more than 100,000 patients. A third-party cloud computing service provider, CloudHealth, stores and manages the electronic protected health information (ePHI) of these individuals on behalf of HealthCo. CloudHealth stores the data in state B. As part of HealthCo's business associate agreement (BAA) with CloudHealth, HealthCo requires CloudHealth to implement security

measures, including industry standard encryption practices, to adequately protect the data. However, HealthCo did not perform due diligence on CloudHealth before entering the contract, and has not conducted audits of CloudHealth's security measures.

A CloudHealth employee has recently become the victim of a phishing attack. When the employee unintentionally clicked on a link from a suspicious email, the PHI of more than 10,000 HealthCo patients was compromised. It has since been published online. The HealthCo cybersecurity team quickly identifies the perpetrator as a known hacker who has launched similar attacks on other hospitals – ones that exposed the PHI of public figures including celebrities and politicians.

During the course of its investigation, HealthCo discovers that CloudHealth has not encrypted the PHI in accordance with the terms of its contract. In addition, CloudHealth has not provided privacy or security training to its employees. Law enforcement has requested that HealthCo provide its investigative report of the breach and a copy of the PHI of the individuals affected.

A patient affected by the breach then sues HealthCo, claiming that the company did not adequately protect the individual's ePHI, and that he has suffered substantial harm as a result of the exposed data. The patient's attorney has submitted a discovery request for the ePHI exposed in the breach.

What is the most significant reason that the U.S. Department of Health and Human Services (HHS) might impose a penalty on HealthCo?

A. Because HealthCo did not require CloudHealth to implement appropriate physical and administrative measures to safeguard the ePHI
B. Because HealthCo did not conduct due diligence to verify or monitor CloudHealth's security measures
C. Because HIPAA requires the imposition of a fine if a data breach of this magnitude has occurred D. Because CloudHealth violated its contract with HealthCo by not encrypting the ePHI

Answer: B

Explanation:
According to the HIPAA Security Rule, covered entities are responsible for ensuring that their business associates comply with the security standards and safeguards required by the rule. This includes conducting due diligence to assess the business associate's security capabilities and practices, and monitoring their performance and compliance. Failure to do so may result in a violation of the rule and a penalty by the HHS. In this scenario, HealthCo did not perform due diligence on CloudHealth before entering the contract, and did not conduct audits of CloudHealth's security measures. This is the most significant reason why HHS might impose a penalty on HealthCo, as it indicates a lack of oversight and accountability for the protection of ePHI. Reference: HIPAA Security Rule

Question: 59

SCENARIO
Please use the following to answer the next QUESTION:

You are the chief privacy officer at HealthCo, a major hospital in a large U.S. city in state A. HealthCo is a HIPAA-covered entity that provides healthcare services to more than 100,000 patients. A third-party cloud computing service provider, CloudHealth, stores and manages the electronic protected health information (ePHI) of these individuals on behalf of HealthCo. CloudHealth stores the data in state B. As part of HealthCo's business associate agreement (BAA) with CloudHealth, HealthCo requires CloudHealth to implement security measures, including industry standard encryption practices, to adequately protect the data. However, HealthCo did not perform due diligence on CloudHealth before entering the contract, and has not conducted audits of CloudHealth's security measures.

A CloudHealth employee has recently become the victim of a phishing attack. When the employee unintentionally clicked on a link from a suspicious email, the PHI of more than 10,000 HealthCo patients was compromised. It has since been published online. The HealthCo cybersecurity team quickly identifies the perpetrator as a known hacker who has launched similar attacks on other hospitals – ones that exposed the PHI of public figures including celebrities and politicians.

During the course of its investigation, HealthCo discovers that CloudHealth has not encrypted the PHI in accordance with the terms of its contract. In addition, CloudHealth has not provided privacy or security training to its employees. Law enforcement has requested that HealthCo provide its investigative report of the breach

and a copy of the PHI of the individuals affected.

A patient affected by the breach then sues HealthCo, claiming that the company did not adequately protect the individual's ePHI, and that he has suffered substantial harm as a result of the exposed data. The patient's attorney has submitted a discovery request for the ePHI exposed in the breach.

What is the most effective kind of training CloudHealth could have given its employees to help prevent this type of data breach?

A. Training on techniques for identifying phishing attempts
B. Training on the terms of the contractual agreement with HealthCo
C. Training on the difference between confidential and non-public information
D. Training on CloudHealth's HR policy regarding the role of employees involved data breaches

Answer: A

Explanation:

Phishing is a form of social engineering that involves sending fraudulent emails or other messages that appear to come from a legitimate source, but are designed to trick recipients into revealing sensitive information, such

as passwords, account numbers, or personal identifiers1. Phishing is one of the most common and effective methods of cyberattacks, and it can lead to data breaches, identity theft, ransomware infections, or other serious consequences2. Therefore, training on how to recognize and avoid phishing attempts is crucial for any organization that handles sensitive data, especially ePHI, which is subject to strict regulations under HIPAA3. Training on techniques for identifying phishing attempts can help employees to spot the signs of a phishing email, such as: Sender's address or domain name that does not match the expected source or contains spelling errors4

Generic salutations or impersonal tone that do not address the recipient by name or use proper grammar4 Urgent or threatening language that creates a sense of pressure or fear and asks the recipient to take immediate action, such as clicking on a link, opening an attachment, or providing information4 Suspicious links or attachments that may contain malware or lead to fake websites that mimic the appearance of a legitimate site, but have a different URL or request login credentials or other data4 Requests for sensitive information that are unusual or out of context, such as asking for passwords, account numbers, or personal identifiers that the sender should already have or should not need4 Training on techniques for identifying phishing attempts can also help employees to learn how to respond to a phishing email, such as:

Not clicking on any links or opening any attachments in the email4 Not replying to the email or providing any information to the sender4 Reporting the email to the IT department or security team and deleting it from the inbox4 Verifying the legitimacy of the email by contacting the sender directly using a different channel, such as phone or another email address4

Updating the antivirus software and scanning the device for any malware infection4

Training on techniques for identifying phishing attempts is the most effective kind of training that CloudHealth could have given its employees to help prevent this type of data breach, because it would have enabled them to recognize the phishing email that compromised the PHI of more than 10,000 HealthCo patients, and to avoid falling victim to it. Training on the terms of the contractual agreement with HealthCo, the difference between confidential and non-public information, or CloudHealth's HR policy regarding the role of employees involved in data breaches, while important, would not have been as effective in preventing this specific type of data breach, because they would not have addressed the root cause of the breach, which was the phishing email.

Reference:

1: IAPP, Phishing, https://iapp.org/resources/glossary/phishing/

2: SpinOne, The Top 5 Phishing Awareness Training Providers 2023, https://spinbackup.com/blog/phishing-awareness-training-best-providers/

3: IAPP, HIPAA, https://iapp.org/resources/glossary/hipaa/

4: Expert Insights, The Top 11 Phishing Awareness Training and Simulation Solutions, https://expertinsights.com/insights/the-top-11-phishing-awareness-training-and-simulation- solutions/

Question: 60

SCENARIO

Please use the following to answer the next QUESTION:

You are the chief privacy officer at HealthCo, a major hospital in a large U.S. city in state A. HealthCo is a HIPAA-covered entity that provides healthcare services to more than 100,000 patients. A third-party cloud computing service provider, CloudHealth, stores and manages the electronic protected health information (ePHI) of these individuals on behalf of HealthCo. CloudHealth stores the data in state B. As part of HealthCo's business associate agreement (BAA) with CloudHealth, HealthCo requires CloudHealth to implement security measures, including industry standard encryption practices, to adequately protect the data. However, HealthCo did not perform due diligence on CloudHealth before entering the contract, and has not conducted audits of CloudHealth's security measures.

A CloudHealth employee has recently become the victim of a phishing attack. When the employee unintentionally clicked on a link from a suspicious email, the PHI of more than 10,000 HealthCo patients was compromised. It has since been published online. The HealthCo cybersecurity team quickly identifies the perpetrator as a known hacker who has launched similar attacks on other hospitals – ones that exposed the PHI of public figures including celebrities and politicians.

During the course of its investigation, HealthCo discovers that CloudHealth has not encrypted the PHI in accordance with the terms of its contract. In addition, CloudHealth has not provided privacy or security training to its employees. Law enforcement has requested that HealthCo provide its investigative report of the breach and a copy of the PHI of the individuals affected.

A patient affected by the breach then sues HealthCo, claiming that the company did not adequately protect the individual's ePHI, and that he has suffered substantial harm as a result of the exposed data. The patient's attorney has submitted a discovery request for the ePHI exposed in the breach.

Of the safeguards required by the HIPAA Security Rule, which of the following is NOT at issue due to HealthCo's actions?

A. Administrative Safeguards
B. Technical Safeguards
C. Physical Safeguards
D. Security Safeguards

Answer: D

Explanation:

The HIPAA Security Rule requires covered entities and their business associates to implement three types of safeguards to protect the confidentiality, integrity, and availability of electronic protected health information (ePHI): administrative, physical, and technical1. Security safeguards is not a separate category of safeguards, but rather a general term that encompasses all three types. Therefore, it is not a correct answer to the question.

Administrative safeguards are the policies and procedures that govern the conduct of the workforce and the security measures put in place to protect ePHI. They include risk analysis and management, training, contingency planning, incident response, and evaluation12.

Physical safeguards are the locks, doors, cameras, and other physical measures that prevent unauthorized access to ePHI. They include workstation and device security, locks and keys, and disposal of media12.

Technical safeguards are the software and hardware tools that protect ePHI from unauthorized access, alteration, or destruction. They include access control, encryption, audit controls, integrity controls, and transmission security12.

In the scenario, HealthCo's actions have potentially violated all three types of safeguards. For example: HealthCo did not perform due diligence on CloudHealth before entering the contract, and has not conducted audits of CloudHealth's security measures. This could be a breach of the administrative safeguard of risk analysis and management12.

HealthCo discovers that CloudHealth has not encrypted the PHI in accordance with the terms of its contract.

This could be a breach of the technical safeguard of encryption12.
HealthCo provides its investigative report of the breach and a copy of the PHI of the individuals affected to law enforcement. This could be a breach of the physical safeguard of disposal of media, if HealthCo did not ensure that the media was properly erased or destroyed after the transfer12. Reference: 1: Summary of the HIPAA Security Rule, HHS.gov. 2: What is the HIPAA Security Rule? Safeguards ... - Secureframe, Secureframe.com.

Question: 61

SCENARIO
Please use the following to answer the next QUESTION:

You are the chief privacy officer at HealthCo, a major hospital in a large U.S. city in state A. HealthCo is a HIPAA-covered entity that provides healthcare services to more than 100,000 patients. A third-party cloud computing service provider, CloudHealth, stores and manages the electronic protected health information (ePHI) of these individuals on behalf of HealthCo. CloudHealth stores the data in state B. As part of HealthCo's business associate agreement (BAA) with CloudHealth, HealthCo requires CloudHealth to implement security measures, including industry standard encryption practices, to adequately protect the data. However, HealthCo did not perform due diligence on CloudHealth before entering the contract, and has not conducted audits of CloudHealth's security measures.

A CloudHealth employee has recently become the victim of a phishing attack. When the employee unintentionally clicked on a link from a suspicious email, the PHI of more than 10,000 HealthCo patients was compromised. It has since been published online. The HealthCo cybersecurity team quickly identifies the perpetrator as a known hacker who has launched similar attacks on other hospitals – ones that exposed the PHI of public figures including celebrities and politicians.

During the course of its investigation, HealthCo discovers that CloudHealth has not encrypted the PHI in accordance with the terms of its contract. In addition, CloudHealth has not provided privacy or security training to its employees. Law enforcement has requested that HealthCo provide its investigative report of the breach and a copy of the PHI of the individuals affected.

A patient affected by the breach then sues HealthCo, claiming that the company did not adequately protect the individual's ePHI, and that he has suffered substantial harm as a result of the exposed data. The patient's attorney has submitted a discovery request for the ePHI exposed in the breach.

Which of the following would be HealthCo's best response to the attorney's discovery request?

A. Reject the request because the HIPAA privacy rule only permits disclosure for payment, treatment or healthcare operations
B. Respond with a request for satisfactory assurances such as a qualified protective order
C. Turn over all of the compromised patient records to the plaintiff's attorney
D. Respond with a redacted document only relative to the plaintiff

Answer: B

Explanation:
The HIPAA privacy rule establishes national standards to protect individuals' medical records and other

individually identifiable health information (collectively defined as “protected health information”) and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically (collectively defined as “covered entities”)1 The rule requires appropriate safeguards to protect the privacy of protected health information and sets limits and conditions on the uses and disclosures that may be made of such information without an individual’s authorization1 The rule also gives individuals rights over their protected health information, including rights to examine and obtain a copy of their health records, to direct a covered entity to transmit to a third party an electronic copy of their protected health information in an electronic health record, and to request corrections1

The HIPAA privacy rule permits a covered entity to disclose protected health information for the litigation in response to a court order, subpoena, discovery request, or other lawful process, provided the applicable requirements of 45 CFR 164.512 (e) for disclosures for judicial and administrative proceedings are met2

These requirements include:

In response to a court order or administrative tribunal order, the covered entity may disclose only the protected health information expressly authorized by such order2

In response to a subpoena, discovery request, or other lawful process that is not accompanied by a court order or administrative tribunal order, the covered entity must receive satisfactory assurances that the party seeking the information has made reasonable efforts to ensure that the individual who is the subject of the information has been given notice of the request, or that the party seeking the information has made reasonable efforts to secure a qualified protective order2

A qualified protective order is an order of a court or administrative tribunal or a stipulation by the parties to the litigation or administrative proceeding that prohibits the parties from using or disclosing the protected health information for any purpose other than the litigation or proceeding for which such information was requested and requires the return to the covered entity or destruction of the protected health information (including all copies made) at the end of the litigation or proceeding2

Option A is incorrect because the HIPAA privacy rule does not only permit disclosure for payment, treatment or healthcare operations. The rule also allows disclosure for other purposes, such as public health, research, law enforcement, judicial and administrative proceedings, as long as the applicable conditions and limitations are met1

Option B is correct because it is consistent with the HIPAA privacy rule’s requirement for disclosures for judicial and administrative proceedings. By responding with a request for satisfactory assurances such as a qualified protective order, HealthCo is ensuring that the protected health information will be used only for the litigation and will be returned or destroyed afterwards2

Option C is incorrect because it is not consistent with the HIPAA privacy rule’s requirement for disclosures for judicial and administrative proceedings. By turning over all of the compromised patient records to the plaintiff’s attorney, HealthCo is disclosing more information than necessary and may violate the privacy rights of other individuals who are not parties to the lawsuit2 Option D is incorrect because it is not consistent with the HIPAA privacy rule’s requirement for disclosures for judicial and administrative proceedings. By responding with a redacted document only relative to the plaintiff, HealthCo is not providing satisfactory assurances that the protected health information will be used only for the litigation and will be returned or destroyed afterwards2 Reference: 1: Summary of the HIPAA Privacy Rule | HHS.gov 2: May a covered entity use or disclose protected health information for litigation? | HHS.gov

Question: 62

Which of the following types of information would an organization generally NOT be required to disclose to law enforcement?

A. Information about medication errors under the Food, Drug and Cosmetic Act
B. Money laundering information under the Bank Secrecy Act of 1970
C. Information about workspace injuries under OSHA requirements
D. Personal health information under the HIPAA Privacy Rule

Answer: D

Explanation:
The HIPAA Privacy Rule generally prohibits covered entities and business associates from disclosing protected health information (PHI) to law enforcement without the individual's authorization, unless one of the exceptions in 45 CFR § 164.512 applies. These exceptions include disclosures required by law, disclosures for law enforcement purposes, disclosures about victims of abuse, neglect or domestic violence, disclosures for health oversight activities, disclosures for judicial and administrative proceedings, disclosures for research purposes, disclosures to avert a serious threat to health or safety, disclosures for specialized government functions, disclosures for workers' compensation, and disclosures to coroners and medical examiners. None of these exceptions apply to the type of information in option D, which is personal health information that is not related to any of the above purposes. Therefore, an organization would generally not be required to disclose such information to law enforcement under the HIPAA Privacy Rule. Reference: https://www.justice.gov/opcl/overview-privacy-act-1974-2020-edition/disclosures-third-parties https://bing.com/search?q=information+disclosure+to+law+enforcement https://hipaatrek.com/law-enforcement-hipaa-disclosing-phi/

Question: 63

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. 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 the Communications 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: 64

What practice do courts commonly require in order to protect certain personal information on documents, whether paper or electronic, that is involved in litigation?

A. Redaction
B. Encryption
C. Deletion
D. Hashing

Answer: A

Explanation:

Redaction is the permanent removal of sensitive data—the digital equivalent of "blacking out" text in printed material. Redaction can be accomplished by simply deleting characters from a file or database record, or by replacing characters with asterisks or other placeholders. Redaction is often

used to protect personal information, such as names, addresses, social security numbers, or financial data, on documents that are disclosed in litigation, such as pleadings, exhibits, or discovery responses. Redaction is required by courts to comply with privacy laws and rules, such as the Federal Rules of Civil Procedure (FRCP), which mandate that parties must redact certain types of personal information from documents filed with the court or produced to the other party. Redaction is also a best practice to minimize the risk of unauthorized access, identity theft, or reputational harm that may result from exposing personal information in litigation. Reference:

When to redact, or not, disclosable documents in litigation - Stewarts

The approach to redaction – High Court guidance - Lexology

IAPP CIPP/US Certified Information Privacy Professional Study Guide, Chapter 3: Federal Privacy Laws and Regulations, Section 3.2: Federal Rules of Civil Procedure (FRCP).

Question: 65

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

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.

Reference: 1: Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510-2523 2: [IAPP CIPP/US Study Guide], Chapter 8, Section 8.2.1. 3: [Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations], pp. 77-78.

Question: 66

What was the original purpose of the Foreign Intelligence Surveillance Act?

A. To further define what information can reasonably be under surveillance in public places under the USA PATRIOT Act, such as Internet access in public libraries.
B. To further clarify a reasonable expectation of privacy stemming from the Katz v. United States decision.
C. To further define a framework for authorizing wiretaps by the executive branch for national security purposes under Article II of the Constitution.
D. To further clarify when a warrant is not required for a wiretap performed internally by the telephone company outside the suspect's home, stemming from the Olmstead v. United States decision.

Answer: C

Explanation:

The Foreign Intelligence Surveillance Act (FISA) was enacted in 1978 in response to revelations of widespread privacy violations by the federal government under President Nixon. It established procedures for requesting judicial authorization for electronic surveillance and physical search of persons engaged in espionage or

international terrorism against the United States on behalf of a foreign power1 The original purpose of FISA was to further define a framework for authorizing wiretaps by the executive branch for national security purposes under Article II of the Constitution, which grants the president the power to conduct foreign affairs and defend the nation23 FISA was intended to balance the need for collecting foreign intelligence information with the protection of privacy and civil liberties of U.S. persons4 Reference: https://www.intelligence.gov/foreign- intelligence-surveillance-act
https://www.intelligence.gov/foreign-intelligence-surveillance-act/1234-categories-of-fisa

Question: 67

What practice does the USA FREEDOM Act NOT authorize?

A. Emergency exceptions that allows the government to target roamers B. An increase in the maximum penalty for material support to terrorism C. An extension of the expiration for roving wiretaps
E. The bulk collection of telephone data and internet metadata

Answer: D

Explanation:
The USA FREEDOM Act is a law that was enacted in 2015 to reform the surveillance practices of the

U.S. government. The law was a response to the revelations by Edward Snowden about the mass collection of phone records and internet data by the National Security Agency (NSA) under the authority of Section 215 of the USA PATRIOT Act. The USA FREEDOM Act ended the bulk collection of telephone data and internet metadata by the NSA, and instead required the government to obtain a specific order from the Foreign Intelligence Surveillance Court (FISC) to access such data from the telecommunication providers. The law also authorized the following practices:
Emergency exceptions that allow the government to target roamers: The law allows the government to temporarily target a non-U.S. person who is using a phone number or identifier of a U.S. person, without a court order, if there is an emergency situation that involves a threat of death or serious bodily harm. The government must obtain a court order within seven days to continue the surveillance.
An increase in the maximum penalty for material support to terrorism: The law increases the maximum prison term for providing material support or resources to a foreign terrorist organization from 15 years to 20 years.
An extension of the expiration for roving wiretaps: The law extends the sunset date for the roving wiretap provision of the USA PATRIOT Act, which allows the government to obtain a single order from the FISC to conduct surveillance on a target who switches devices or locations, without specifying the device or location. The law extends the expiration date from June 1, 2015 to December 15, 2019. Reference:
USA FREEDOM Act
USA FREEDOM Act Summary
USA FREEDOM Act FAQs

Question: 68

Why was the Privacy Protection Act of 1980 drafted?

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

Question: 69

The rules for "e-discovery" mainly prevent which of the following?

A. A conflict between business practice and technological safeguards
B. The loss of information due to poor data retention practices
C. The practice of employees using personal devices for work
D. A breach of an organization's data retention program

Answer: A

Explanation:
E-discovery is the process by which parties share, review, and collect electronically stored information (ESI) to use as evidence in a legal matter1. The rules for e-discovery mainly prevent a conflict between business practice and technological safeguards, because they establish the standards and procedures for preserving, collecting, reviewing, and producing ESI in a way that balances the needs of litigation with the realities of technology2. For example, the Federal Rules of Civil Procedure (FRCP) provide guidance on the scope, timing, format, and methods of e-discovery, as well as the sanctions for failing to comply with e-discovery obligations3. The rules also encourage cooperation and communication among parties and courts to resolve e-discovery issues efficiently and effectively4. By following the rules for e-discovery, parties can avoid disputes, delays, and costs that may arise from incompatible or inconsistent business and technological practices.

The other options are not the main purpose of the rules for e-discovery, although they may be related or affected by them. The rules for e-discovery do not directly prevent the loss of information due to poor data retention practices, although they do impose a duty to preserve relevant ESI when litigation is reasonably anticipated5. The rules for e-discovery do not directly prevent the practice of employees using personal devices for work, although they do require parties to identify and disclose the sources of ESI that may be subject to discovery, including personal devices6. The rules for ediscovery do not directly prevent a breach of an organization's data retention program, although they do require parties to produce ESI in a reasonably usable form and to protect privileged or confidential information7.

Reference: 1: Everything You Need to Know About E-Discovery, The National Law Review. 2: EDiscovery: The Basics of E-Discovery Guide - Exterro, Exterro.com. 3: Federal Court and Government Agency E-Discovery Rules and Guidelines, Crowell & Moring LLP. 4: FRCP Rule 1, Cornell Law School. 5: FRCP Rule 37, Cornell Law School. 6: FRCP Rule 26, Cornell Law School. 7: FRCP Rule 34, Cornell Law School.

Question: 70

What do the Civil Rights Act, Pregnancy Discrimination Act, Americans with Disabilities Act, Age Discrimination Act, and Equal Pay Act all have in common?

A. They require employers not to discriminate against certain classes when employees use personal information
B. They require that employers provide reasonable accommodations to certain classes of employees
C. They afford certain classes of employees' privacy protection by limiting inquiries concerning their personal information
D. They permit employers to use or disclose personal information specifically about employees who are members of certain classes

Answer: C

Explanation:

The Civil Rights Act, Pregnancy Discrimination Act, Americans with Disabilities Act, Age Discrimination Act, and Equal Pay Act are all federal laws that prohibit employment discrimination based on certain protected characteristics, such as race, sex, disability, age, and pay1234 These laws also afford certain classes of employees' privacy protection by limiting inquiries concerning their personal information that may reveal their protected status or be used for discriminatory purposes. For example:

The Civil Rights Act of 1964 prohibits employers from making pre-employment inquiries that express a preference, limitation, or specification based on race, color, religion, sex, or national origin, unless they are bona fide occupational qualifications.

The Pregnancy Discrimination Act of 1978, which amended the Civil Rights Act of 1964, prohibits employers from making pre-employment inquiries about whether an applicant is pregnant or intends to become pregnant, unless they are related to the ability to perform the job.

The Americans with Disabilities Act of 1990 prohibits employers from making pre-employment inquiries about whether an applicant has a disability or the nature or severity of a disability, unless they are related to the ability to perform the essential functions of the job with or without reasonable accommodation.

The Age Discrimination in Employment Act of 1967 prohibits employers from making preemployment inquiries

about an applicant's age, unless they are related to a bona fide occupational qualification or a lawful affirmative action plan.

The Equal Pay Act of 1963 prohibits employers from making pre-employment inquiries about an applicant's salary history, unless they are made for a lawful purpose other than determining the applicant's pay.

Option A is incorrect because these laws do not require employers not to discriminate against certain classes when employees use personal information. Rather, they require employers not to discriminate against certain classes in any aspect of employment, such as hiring, firing, pay, promotion, training, benefits, etc1234 The use of personal information by employees is not directly addressed by these laws, although it may be subject to other privacy laws or policies.

Option B is incorrect because these laws do not require that employers provide reasonable accommodations to certain classes of employees. Rather, only the Americans with Disabilities Act and the Pregnancy Discrimination Act require employers to provide reasonable accommodations to qualified individuals with disabilities and workers with limitations related to pregnancy, childbirth, or related medical conditions, respectively, unless doing so would cause an undue hardship to the employer. The other laws do not have a similar requirement, although they may prohibit employers
from denying equal opportunities to certain classes of employees.

Option C is correct because these laws afford certain classes of employees' privacy protection by limiting inquiries concerning their personal information that may reveal their protected status or be used for discriminatory purposes, as explained above.

Option D is incorrect because these laws do not permit employers to use or disclose personal information specifically about employees who are members of certain classes. Rather, these laws generally prohibit employers from using or disclosing personal information that is protected by these laws for any unlawful or discriminatory purpose, unless an exception applies. For example, employers may use or disclose such information for legitimate business reasons, such as complying with reporting requirements, administering benefits, or conducting investigations.

Reference: 1: Facts About Equal Pay and Compensation Discrimination 2: Pregnancy Discrimination and Pregnancy-Related Disability Discrimination | U.S. Equal Employment Opportunity Commission 3: Regulations, Guidance and Policy | Equal Opportunity Guidance | OEEOWE 4: Age Discrimination | U.S. Equal Employment Opportunity Commission : Pre-Employment Inquiries and Medical Questions & Examinations | U.S. Equal Employment Opportunity Commission : Employee Medical Information | U.S. Equal Employment Opportunity Commission : Employee Privacy Rights | U.S. Department of Labor : Title VII of the Civil Rights Act of 1964 | U.S. Equal Employment Opportunity Commission : Fact Sheet: Pregnancy Discrimination | U.S. Equal Employment Opportunity Commission : The Americans with Disabilities Act: A Primer for Small Business : Age Discrimination in Employment Act of 1967 | U.S. Equal Employment Opportunity Commission : Equal Pay Act of 1963 | U.S. Equal Employment Opportunity Commission

Question: 71

Which is an exception to the general prohibitions on telephone monitoring that exist under the U.S. Wiretap Act?

A. Call center exception
B. Inter-company communications exception
C. Ordinary course of business exception
D. Internet calls exception

Answer: C

Explanation:
The U.S. Wiretap Act prohibits the interception and disclosure of wire, oral, or electronic communications, unless one of the statutory exceptions applies. One of these exceptions is the ordinary course of business exception, which allows an employer or service provider to intercept communications that are made in the ordinary course of its business, such as for quality control, training, or security purposes. This exception does not apply to communications that are not related to the business, such as personal calls or emails, or to communications that are intercepted for other reasons, such as harassment, discrimination, or retaliation. The scope and applicability of this exception may vary depending on the context, the consent of the parties, and the state law. The other options are not valid exceptions under the Wiretap Act. Reference: 1, 2, 3, 4

Question: 72

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 medi a. 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

Answer: A

Explanation:
Larry has a misconception about the applicability of federal law to private-sector employee rights. He believes that the U.S. Constitution protects American workers from various forms of discrimination, harassment, and invasion of privacy by their employers. However, the U.S. Constitution only applies to government actions, not private actions, unless there is a specific federal statute that extends constitutional protections to the private sector1. For example, the Civil Rights Act of 1964 prohibits discrimination on the basis of race, color, religion, sex, or national origin by private employers2. The Electronic Communications Privacy Act of 1986 regulates the interception and disclosure of electronic communications by private parties3. The CAN-SPAM Act of 2003 sets the rules for commercial email and gives recipients the right to opt out of receiving unwanted messages4.
These are examples of federal laws that apply to private-sector employees, but they do not cover all the situations that Larry faces at SunriseLynx. For instance, there is no federal law that protects privatesector employees from political discrimination or from having their personal mail opened by their employers. Larry may have to rely on state laws or common law torts to seek redress for these violations of his rights.
Reference: 1: Private Sector vs. Public Sector Employee Rights2: [Civil Rights Act of 1964 - Wikipedia] 3: [Electronic Communications Privacy Act - Wikipedia] 4: CAN-SPAM Act: A Compliance Guide for Business : IAPP CIPP/US Certified Information Privacy Professional Study Guide, Chapter 5: Federal Trade Commission and Consumer Privacy, p. 141-142

Question: 73

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 medi
a. 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.

Based on the way he uses social media, Evan is susceptible to a lawsuit based on?

A. Defamation
B. Discrimination
C. Intrusion upon seclusion
D. Publicity given to private life

Answer: B

Explanation:
Discrimination is the unfair or prejudicial treatment of people based on certain characteristics, such as race, gender, age, religion, or political affiliation. Discrimination can occur in various contexts, such as employment, education, housing, or public accommodations. Discrimination can violate federal, state, or local laws that prohibit discrimination on the basis of protected categories. In the scenario, Evan is susceptible to a lawsuit based on discrimination because he uses social media to favor employees who share his political views and deny promotions to those who do not. This could constitute political discrimination, which is prohibited by some state and local laws, such as the District of Columbia Human Rights Act and the New York City Human Rights Law. Additionally, Evan's use of social media could reveal other protected characteristics of his employees, such as their race, gender, age, religion, or sexual orientation, and expose him to claims of discrimination based on those grounds as well. For example, if Evan posts derogatory comments about a certain race or religion, and then denies a promotion to an employee of that race or religion, that employee could sue Evan for discrimination under federal laws, such as Title VII of the Civil Rights Act of 1964 or the Civil Rights Act of 1991. Reference:
Political Discrimination in the Workplace | Nolo
Social Media and Employment Law Summary of Key Cases and Legal Issues
IAPP CIPP/US Certified Information Privacy Professional Study Guide, Chapter 4: State Privacy Laws and Regulations, Section 4.1: State Anti-Discrimination Laws.

Question: 74

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 medi a. 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.

Which act would authorize Evan's undercover investigation?

A. The Whistleblower Protection Act
B. The Stored Communications Act (SCA)
C. The National Labor Relations Act (NLRA)
D. The Fair and Accurate Credit Transactions Act (FACTA)

Answer: B

Explanation:
The Stored Communications Act (SCA) is a federal law that regulates the privacy of electronic communications that are stored by third-party service providers, such as email providers, cloud storage providers, or social media platforms. The SCA prohibits unauthorized access to or disclosure

of such communications, unless authorized by law or by the consent of the user or the service provider . The SCA also provides exceptions for certain types of access or disclosure, such as those made for law enforcement purposes, for the protection of the service provider's rights or property, or for the consent of the

subscriber or customer .

One of the exceptions to the SCA is where the service provider gives consent to the access or disclosure of the stored communications. This means that if a third-party service provider agrees to cooperate with an investigation or a request for information, the access or disclosure is lawful under the SCA. Consent can be express or implied, depending on the circumstances and the terms of service of the provider. For example, if a service provider has a policy that allows it to disclose user information to third parties for legitimate purposes, the provider has impliedly consented to the access or disclosure of the stored communications. However, if a service provider has a policy that prohibits such disclosure, the provider has not consented to the access or disclosure of the stored communications.

In the scenario, Evan's undercover investigation may have been authorized by the SCA if he obtained the consent of the third-party service provider that stored the electronic communications of the employee who was suspected of misconduct. For instance, if the employee used a company email account or a cloud storage service that had a policy that allowed the service provider to disclose user information to the employer or to law enforcement, Evan may have been able to access or disclose the stored communications with the consent of the service provider. However, if the employee used a personal email account or a cloud storage service that had a policy that protected user privacy and prohibited such disclosure, Evan may have violated the SCA by accessing or disclosing the stored communications without the consent of the service provider.

Reference: : [Stored Communications Act], 18 U.S.C. §§ 2701-2712 : [IAPP CIPP/US Study Guide], Chapter 8, Section 8.2.2. : [The Stored Communications Act: An Old Statute for Modern Problems], pp. 10-11.

Question: 75

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 medi a. 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 regard to telemarketing practices, Evan the supervisor has a misconception regarding?

A. The conditions under which recipients can opt out
B. The wishes of recipients who request callbacks
C. The right to monitor calls for quality assurance
D. The relationship of state law to federal law

Answer: B

Explanation:

Question: 76

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 backlash123 Reference: https://www.jibble.io/article/us-employee-monitoringhttps://www.worktime.com/most-asked-questions-on-us-employee-monitoring-laws

Question: 77

Which of the following is most likely to provide privacy protection to private-sector employees in the United States?

A. State law, contract law, and tort law
B. The Federal Trade Commission Act (FTC Act)
C. Amendments one, four, and five of the U.S. Constitution
D. The U.S. Department of Health and Human Services (HHS)

Answer: A

Explanation:

Unlike many other countries, the United States does not have a comprehensive federal law that regulates the privacy of private-sector employees. Instead, the privacy protection of employees depends largely on state law, contract law, and tort law. State law may provide specific rights and remedies for employees regarding issues such as drug testing, background checks, electronic monitoring, social media access, and genetic information. Contract law may create obligations and expectations for employers and employees based on written or implied agreements, such as employment contracts, employee handbooks, or collective bargaining agreements. Tort law may allow employees to sue their employers for invasion of privacy, such as intrusion upon seclusion, public disclosure of private facts, false light, or appropriation of name or likeness. The other options are less likely to provide privacy protection to private-sector employees in the United States. The FTC Act primarily regulates the privacy practices of businesses that collect and use consumer data, not employee data. The U.S. Constitution only protects individuals from unreasonable searches and seizures by the government, not by private employers. The HHS only enforces the HIPAA Privacy Rule, which applies to covered entities and business associates that handle protected health information, not to all private-sector employers. Reference:

IAPP CIPP/US Study Guide, Chapter 6: Workplace Privacy

Privacy Rights of Employees Using Workplace Computers in the United States Employee Privacy Laws

Question: 78

What role does the U.S. Constitution play in the area of workplace privacy?

A. It provides enforcement resources to large employers, but not to small businesses
B. It provides legal precedent for physical information security, but not for electronic security
C. It provides contractual protections to members of labor unions, but not to employees at will
D. It provides significant protections to federal and state governments, but not to private-sector employment

Answer: D

Explanation:

The U.S. Constitution plays a limited role in the area of workplace privacy, because it mainly applies to the

actions of the government, not private employers. The Fourth Amendment protects the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures1. The Supreme Court has interpreted this right to include a reasonable expectation of privacy in certain situations, such as in one's home, car, or personal belongings2. However, this right does not extend to private-sector employees, who are not protected by the Constitution from the actions of their employers, unless the employer is acting as an agent of the government3. Private-sector employees may have some privacy rights under state laws, common law, or contractual agreements, but these vary depending on the jurisdiction and the circumstances4.

Public-sector employees, on the other hand, are protected by the Constitution from unreasonable searches and seizures by their employers, who are considered part of the government. Public-sector employees have a reasonable expectation of privacy in their workplace, unless there is a legitimate work-related reason for the search or seizure, such as to ensure safety, security, or efficiency. Publicsector employers must also comply with the due process and equal protection clauses of the Fifth and Fourteenth Amendments, which prohibit the government from depriving any person of life, liberty, or property without due process of law, or from denying any person the equal protection of the laws. These clauses protect public-sector employees from arbitrary or discriminatory actions by their employers that affect their employment status or benefits.

Therefore, the U.S. Constitution plays a significant role in the area of workplace privacy for federal and state governments, but not for private-sector employment, because it only regulates the actions of the government, not private actors. Reference:

1: Cornell Law School, Fourth Amendment, https://www.law.cornell.edu/constitution/fourth_amendment

2: FindLaw, What Is a Reasonable Expectation of Privacy?, https://www.findlaw.com/criminal/criminal-rights/what-is-a-reasonable-expectation-of-privacy.html 3: FindLaw, Workplace Privacy, https://www.findlaw.com/smallbusiness/employment-law-and- human-resources/workplace-privacy.html

4: Nolo, Privacy Rights of Employees, https://www.nolo.com/legal-encyclopedia/privacy-rights- employees-29849.html

: OPM, Employee Relations, https://www.opm.gov/policy-data-oversight/employee- relations/reference-materials/employee-privacy/

: Cornell Law School, Fifth Amendment, https://www.law.cornell.edu/constitution/fifth_amendment : FindLaw, Public Employees and the Constitution, https://www.findlaw.com/employment/employment-rights/public-employees-and-the- constitution.html

Question: 79

Which action is prohibited under the Electronic Communications Privacy Act of 1986?

A. Intercepting electronic communications and unauthorized access to stored communications
B. Monitoring all employee telephone calls
C. Accessing stored communications with the consent of the sender or recipient of the message
D. Monitoring employee telephone calls of a personal nature

Answer: A

Explanation:

The Electronic Communications Privacy Act of 1986 (ECPA) is a federal law that protects the privacy of wire, oral, and electronic communications while they are being made, in transit, or stored on computers1. The ECPA has three titles: Title I prohibits the intentional interception, use, or disclosure of wire, oral, or electronic communications, except for certain exceptions, such as consent, provider protection, or law enforcement purposes2. Title II, also known as the Stored Communications Act (SCA), prohibits the unauthorized access to or disclosure of stored wire or electronic communications, such as email, voicemail, or online messages, except for certain exceptions, such as consent, provider protection, or law enforcement purposes3. Title III regulates the installation and use of pen register and trap and trace devices, which record the numbers dialed to or from a telephone line, but not the content of the communications4.

Therefore, the action that is prohibited under the ECPA is intercepting electronic communications and unauthorized access to stored communications, which are covered by Title I and Title II of the Act, respectively. The other actions are not prohibited by the ECPA, as long as they comply with the exceptions and requirements of the Act. For example, monitoring all employee telephone calls or monitoring employee telephone calls of a personal nature may be allowed if the employer has a legitimate business purpose, has obtained the consent of the employees, or has a court order5. Accessing stored communications with the consent of the sender or recipient of the message is also allowed under the ECPA, as consent is one of the exceptions to the prohibition of unauthorized access3.

Reference: 1: Electronic Communications Privacy Act of 1986 (ECPA), Bureau of Justice Assistance. 2: 18 U.S. Code Chapter 119 - WIRE AND ELECTRONIC COMMUNICATIONS INTERCEPTION AND INTERCEPTION OF ORAL COMMUNICATIONS, Legal Information Institute. 3: 18 U.S. Code Chapter 121 - STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORDS ACCESS, Legal Information Institute. 4: 18 U.S. Code Chapter 206 - PEN REGISTERS AND TRAP AND TRACE DEVICES, Legal Information Institute. 5: Monitoring Employees' Phone Calls and E-Mail, FindLaw.

Question: 80

Which of the following does Title VII of the Civil Rights Act prohibit an employer from asking a job applicant?

A. Questions about age
B. Questions about a disability
C. Questions about a national origin
D. Questions about intended pregnancy

Answer: D

Explanation:

Title VII of the Civil Rights Act of 1964 is a federal law that prohibits employment discrimination based on race, color, religion, sex, and national origin1 It also prohibits retaliation against individuals who assert their rights under the law or participate in an EEOC investigation1 Title VII applies to employers with 15 or more employees, as well as to employment agencies, labor organizations, and joint labor-management committees1

Title VII prohibits employers from making pre-employment inquiries that express a preference, limitation, or specification based on any of the protected characteristics, unless they are bona fide occupational qualifications (BFOQs)2 BFOQs are rare and narrowly construed exceptions that allow employers to consider a protected characteristic when it is reasonably necessary to the normal operation of the business2 For example, a religious organization may require its employees to share its faith, or a women's shelter may hire only female counselors2 Option A is incorrect because questions about age are not prohibited by Title VII,

but by the Age Discrimination in Employment Act of 1967 (ADEA), which protects individuals who are 40 years of age or older from employment discrimination based on age3 The ADEA generally prohibits employers from asking applicants about their age or date of birth, unless age is a BFOQ or the inquiry is part of a lawful affirmative action plan3

Option B is incorrect because questions about a disability are not prohibited by Title VII, but by the Americans with Disabilities Act of 1990 (ADA), which protects qualified individuals with disabilities from employment discrimination based on disability4 The ADA generally prohibits employers from asking applicants about whether they have a disability or the nature or severity of a disability, unless the inquiry is related to the ability to perform the essential functions of the job with or without reasonable accommodation4

Option C is incorrect because questions about a national origin are prohibited by Title VII, but not in all circumstances. Title VII prohibits employers from asking applicants about their national origin, ancestry, birthplace, native language, or accent, unless they are BFOQs or the inquiry is related to a legitimate business purpose, such as verifying eligibility to work in the United States or assessing language proficiency for a job that requires communication skills25 Option D is correct because questions about intended pregnancy are prohibited by Title VII, as amended by the Pregnancy Discrimination Act of 1978 (PDA), which protects women from employment discrimination based on pregnancy, childbirth, or related medical conditions. The PDA prohibits employers from asking applicants about whether they are pregnant or intend to become pregnant, unless they are related to the ability to perform the job. Such questions may indicate an intent to discriminate based on sex or pregnancy, or may deter women from applying for certain jobs.

Reference: 1: Title VII of the Civil Rights Act of 1964 | U.S. Equal Employment Opportunity Commission 2: Questions and Answers about Race and Color Discrimination in Employment | U.S. Equal Employment Opportunity Commission 3: Age Discrimination | U.S. Equal Employment Opportunity Commission 4: Disability Discrimination | U.S. Equal Employment Opportunity Commission 5: National Origin Discrimination | U.S. Equal Employment Opportunity Commission : Pregnancy Discrimination | U.S. Equal Employment Opportunity Commission

Question: 81

How did the Fair and Accurate Credit Transactions Act (FACTA) amend the Fair Credit Reporting Act (FCRA)?

A. It expanded the definition of "consumer reports" to include communications relating to employee investigations

B. It increased the obligation of organizations to dispose of consumer data in ways that prevent unauthorized access

C. It stipulated the purpose of obtaining a consumer report can only be for a review of the employee's credit worthiness

D. It required employers to get an employee's consent in advance of requesting a consumer report for internal investigation purposes

Answer: B

Explanation:

FACTA added a new section to the FCRA that requires any person who maintains or otherwise possesses consumer information, or any compilation of consumer information, derived from consumer reports for a business purpose, to properly dispose of any such information or compilation. The purpose of this provision is to reduce the risk of identity theft and other consumer harm resulting from improper disposal of consumer

information. The FTC and other federal agencies have issued rules implementing this provision, which specify the reasonable measures that covered entities must take to ensure secure disposal of consumer information, such as burning, pulverizing, shredding, erasing, or otherwise modifying the information to make it unreadable or indecipherable (16 CFR § 682.3). Reference: 1, 2, 3

Question: 82

Which federal act does NOT contain provisions for preempting stricter state laws?

A. The CAN-SPAM Act
B. The Children's Online Privacy Protection Act (COPPA)
C. The Fair and Accurate Credit Transactions Act (FACTA)
D. The Telemarketing Consumer Protection and Fraud Prevention Act

Answer: D

Explanation:

The federal act that does NOT contain provisions for preempting stricter state laws is the Telemarketing Consumer Protection and Fraud Prevention Act1. This act authorizes the Federal Trade Commission (FTC) to establish and enforce rules for telemarketing practices, such as the Do Not Call Registry, the prohibition of robocalls, and the disclosure of material information2. However, the act also explicitly states that it does not "annul, alter, or affect, or exempt any person subject to the provisions of this section from complying with, the laws of any State with respect to telemarketing practices, except to the extent that those laws are inconsistent with any provision of this section, and then only to the extent of the inconsistency"1. This means that states can enact and enforce their own laws regarding telemarketing, as long as they are not less protective than the federal law. In contrast, the other three acts listed in the question do contain preemption clauses that limit or override the authority of states to regulate certain aspects of electronic communications, online privacy, and credit transactions345. Reference: 1: Telemarketing Consumer Protection and Fraud Prevention Act2: Telemarketing Sales Rule | Federal Trade Commission3: CAN-SPAM Act: A Compliance Guide for Business4: Children's Online Privacy Protection Rule ("COPPA") | Federal Trade Commission5: Fair and Accurate Credit Transactions Act of 2003 - Wikipedia : IAPP CIPP/US Certified Information Privacy Professional Study Guide, Chapter 5: Federal Trade Commission and Consumer Privacy, p. 144-145, 149-150, 154-155

Question: 83

Which of the following is commonly required for an entity to be subject to breach notification requirements under most state laws?

A. The entity must conduct business in the state
B. The entity must have employees in the state
C. The entity must be registered in the state
D. The entity must be an information broker

Answer: A

Explanation:

Most state laws require that a person or business that conducts business in the state and owns or licenses personal information of residents of that state must notify those residents of any breach of the security of the system involving their personal information. This means that the entity does not have to be physically located in the state, have employees in the state, or be registered in the state to be subject to the breach notification requirements, as long as it conducts business in the state and holds personal information of state residents. Conducting business in the state can be interpreted broadly to include any transaction or activity that involves the state or its residents, such as selling goods or services, collecting payments, or maintaining a website accessible by state residents. The other options (B, C, and D) are not commonly required by most state laws, although some states may have additional or specific requirements for certain types of entities, such as information brokers, health care providers, or financial institutions. Reference:

Security Breach Notification Chart | Perkins Coie

Security Breach Notification Laws - National Conference of State Legislatures

IAPP CIPP/US Certified Information Privacy Professional Study Guide, Chapter 4: State Privacy Laws and Regulations, Section 4.2: State Security Breach Notification Laws.

Question: 84

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

Answer: C

Explanation:

The most likely reason that states have adopted their own data breach notification laws is that many types of organizations are not currently subject to federal laws regarding breaches. As explained in the Data Breach Response: A Guide for Business from the Federal Trade Commission (FTC), certain federal laws govern obligations to report data breaches in particular industries, such as health care, financial services, or telecommunications. However, these laws do not cover all types of businesses or all types of personal information that may be compromised in a data breach. Therefore, states have enacted their own data breach notification laws to fill the gaps and protect the privacy and security of their residents. According to the National Conference of State Legislatures, as of January 2022, all 50 states, the District of Columbia, Puerto Rico, and the Virgin Islands have enacted legislation requiring notification of security breaches involving personal information. These state laws vary in terms of the definitions of personal information, the triggers for notification, the methods and timing of notification, the exemptions and exceptions, and the penalties and enforcement mechanisms.

Reference: 1: Data Breach Response: A Guide for Business, Section 2 2: 2022 Security Breach Legislation

Question: 85

Which federal law or regulation preempts state law?

A. Health Insurance Portability and Accountability Act
B. Controlling the Assault of Non-Solicited Pornography and Marketing Act
C. Telemarketing Sales Rule
D. Electronic Communications Privacy Act of 1986

Answer: A

Explanation:

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 is a federal law that regulates the privacy and security of health information in the United States. HIPAA preempts state laws that are contrary to its provisions, unless the state laws provide more stringent protections for health information12 HIPAA establishes a floor of federal standards for health information privacy and security, but allows states to enact laws that are more protective of individuals' rights34 For example, some states may require more specific consent from individuals before disclosing their health information, or impose stricter penalties for violations of health information privacy and security. HIPAA also provides exceptions for certain state laws that serve a compelling public interest, such as public health, safety, or welfare.

Reference: https://www.findlaw.com/litigation/legal-system/the-supremacy-clause-and-the- doctrine-of-preemption.htmlhttps://www.bonalaw.com/insights/legal-resources/when-does-federal-law-preempt-state-law

Question: 86

More than half of U.S. states require telemarketers to?

A. Identify themselves at the beginning of a call
B. Obtain written consent from potential customers
C. Register with the state before conducting business
D. Provide written contracts for customer transactions

Answer: C

Explanation:

According to the IAPP CIPP/US Study Guide, more than half of U.S. states require telemarketers to register with the state before conducting business within the state. This registration requirement may involve paying a fee, posting a bond, or providing information about the telemarketer's identity, location, and business practices. The purpose of this requirement is to protect consumers from fraudulent or deceptive telemarketing calls and to facilitate the enforcement of state laws and regulations. The other options are not required by most states,

although some states may have additional rules or guidelines for telemarketers regarding identification, consent, or contracts. Reference:
IAPP CIPP/US Study Guide, Chapter 7: Marketing and Advertising
State Telemarketing Registration Requirements

Question: 87

What does the Massachusetts Personal Information Security Regulation require as it relates to encryption of personal information?

A. The encryption of all personal information of Massachusetts residents when all equipment is located in Massachusetts.
B. The encryption of all personal information stored in Massachusetts-based companies when all equipment is located in Massachusetts.
C. The encryption of personal information stored in Massachusetts-based companies when stored on portable devices.
D. The encryption of all personal information of Massachusetts residents when stored on portable devices.

Answer: D

Explanation:
The Massachusetts Personal Information Security Regulation (201 CMR 17.00) requires that any person or entity that owns or licenses personal information of Massachusetts residents must implement and maintain a comprehensive written information security program that includes administrative, technical, and physical safeguards to protect such information. One of the technical requirements of the regulation is to encrypt all personal information of Massachusetts residents that is stored on laptops or other portable devices, regardless ofwhere the equipment is located12. The regulation defines personal information as a person's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such person: (a) Social Security number; (b) driver's license number or state-issued identification card number; or © financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account1. The regulation also requires encryption of all transmitted records and files containing personal information that will travel across public networks, and encryption of all data containing personal information to be transmitted wirelessly1. Reference:
Regulation 201 CMR 17.00: Standards for the Protection of Personal Information of MA Residents
Massachusetts Law Raises the Bar for Data Security

Question: 88

California's SB 1386 was the first law of its type in the United States to do what?

A. Require commercial entities to disclose a security data breach concerning personal information about the state's residents

B. Require notification of non-California residents of a breach that occurred in California
C. Require encryption of sensitive information stored on servers that are Internet connected
D. Require state attorney general enforcement of federal regulations against unfair and deceptive trade practices

Answer: A

Explanation:
California's SB 1386, also known as the California Security Breach Information Act, was enacted in 2002 and became effective in 2003. It was the first law of its kind in the United States to require commercial entities that own or license personal information of California residents to notify them in

the event of a security breach that compromises their unencrypted data. The law aims to protect the privacy and security of personal information and to enable individuals to take preventive measures against identity theft and fraud. The law applies to any business or person that conducts business in California and that owns or licenses computerized data that includes personal information, as defined by the law. Personal information includes an individual's first name or first initial and last name in combination with any one or more of the following data elements: Social Security number, driver's license number or California identification card number, account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account, or medical information or health insurance information. The law does not apply to encrypted information, publicly available information, or information that is lawfully obtained from federal, state, or local government records. The law requires the disclosure of a breach of the security of the system to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. The disclosure may be made by written notice, electronic notice, or substitute notice, as specified by the law. The law also requires any person or business that maintains computerized data that includes personal information that the person or business does not own to notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The law also authorizes a civil action for damages by a customer injured by a violation of the law and provides that the rights and remedies available under the law are cumulative to each other and to any other rights and remedies available under law. Reference: California Senate Bill 1386 (2002)
California SB 1386: For the Love of Privacy
What Is the California Security Breach Information Act? California Raises the Bar on Data Security and Privacy

Question: 89

Most states with data breach notification laws indicate that notice to affected individuals must be sent in the "most expeditious time possible without unreasonable delay." By contrast, which of the following states currently imposes a definite limit for notification to affected individuals?

A. Maine
B. Florida

C. New York

D. California

Answer: B

Explanation:

According to the web search results from my predefined tool, Florida is the only state among the four options that currently imposes a definite limit for notification to affected individuals in case of a data

breach. Florida's law requires that notice be provided within 30 days after determination of the breach or reason to believe a breach occurred, unless delayed by law enforcement or measures to determine the scope of the breach and restore the integrity of the system1. The other states have more flexible or vague terms for the notification timeframe, such as "as soon as practicable" (Maine), "in the most expedient time possible and without unreasonable delay" (New York), or "in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement" (California)2. Reference:

Security Breach Notification Chart | Perkins Coie

State Data Breach Notification Chart - International Association of ...

Question: 90

Under state breach notification laws, which is NOT typically included in the definition of personal information?

A. State identification number

B. First and last name

C. Social Security number

D. Medical Information

Answer: B

Explanation:

Under state breach notification laws, personal information is typically defined as an individual's first name or first initial and last name plus one or more other data elements, such as Social Security number, state identification number, account number, medical information, etc. However, first and last name alone are not usually considered personal information, unless they are combined with other data elements that could identify the individual or compromise their security or privacy. Therefore, option B is the correct answer, as it is not typically included in the definition of personal information under state breach notification laws.

Reference:

https://www.ncsl.org/technology-and-communication/security-breach-notification-laws

https://iapp.org/resources/article/state-data-breach-notification-chart/

Question: 91

Which of the following best describes what a “private right of action” is?

A. The right of individuals to keep their information private.
B. The right of individuals to submit a request to access their information.
C. The right of individuals harmed by data processing to have their information deleted.
D. The right of individuals harmed by a violation of a law to file a lawsuit against the violation.

Answer: D

Explanation:

A private right of action is a legal provision that grants individuals the ability to bring a lawsuit against a party that has wronged them and to seek redress for the harm that they have suffered. A private right of action is a fundamental component of the U.S. judicial system and an essential element of enforcing privacy rights. Privacy advocates argue that a private right of action is necessary to hold perpetrators of privacy violations accountable and to address the limitations of the FTC’s enforcement authority. However, businesses are concerned that a private right of action would lead to a proliferation of frivolous lawsuits that would burden responsible data processors and impede innovation. Reference:

U.S. Private-Sector Privacy, Third Edition by Peter P. Swire, DeBrae Kennedy-Mayo, Chapter 2, Section 2.3.3, pp. 35-36.

How to end the deadlock on the private right of action by Paula Bruening, IAPP Privacy Perspectives, Jan 20, 2022.

Private Right of Action (Legal Definition & Examples) by Lawrina, accessed on Jan 25, 2022.

Question: 92

Which of the following is NOT a principle found in the APEC Privacy Framework?

A. Integrity of Personal Information.
B. Access and Correction.
C. Preventing Harm.
D. Privacy by Design.

Answer: D

Explanation:

The APEC Privacy Framework is a set of non-binding principles adopted by the Asia-Pacific Economic Cooperation (APEC) that aim to promote electronic commerce and protect information privacy in the region. The Framework is consistent with the core values of the OECD Guidelines on the Protection of Privacy and Trans-Border Flows of Personal Data, and reaffirms the value of privacy to individuals and to the information society. The Framework consists of nine principles: Preventing Harm, Notice, Collection Limitation, Use of

Personal Information, Choice, Integrity of Personal Information, Security Safeguards, Access and Correction, and Accountability. Privacy by Design is not one of the principles in the APEC Privacy Framework, although it is a concept that is endorsed by the OECD Guidelines and other privacy frameworks. Reference: APEC Privacy Framework (2015), APEC Privacy Principles, IAPP CIPP/US Study Guide, Chapter 4.

Question: 93

What is the most important action an organization can take to comply with the FTC position on retroactive changes to a privacy policy?

A. Describing the policy changes on its website.
B. Obtaining affirmative consent from its customers.
C. Publicizing the policy changes through social media.
D. Reassuring customers of the security of their information.

Answer: B

Explanation:
The FTC has stated that it is a deceptive practice to make retroactive changes to a privacy policy that affect how a company uses or shares previously collected personal information, unless the company obtains affirmative consent from the affected consumers. This means that the company must clearly and conspicuously disclose the changes and obtain the consumers' express agreement to them. Simply describing the policy changes on the website, publicizing them through social media, or reassuring customers of the security of their information are not sufficient to comply with the FTC's position. Reference:
FTC Staff Revises Online Behavioral Advertising Principles, paragraph 3.
Do I really have to obtain consent from all my customers to make a change to my privacy policy?, paragraph 2.
IAPP CIPP/US Study Guide, page 64.

Question: 94

Federal laws establish which of the following requirements for collecting personal information of minors under the age of 13?

A. Implied consent from a minor's parent or guardian, or affirmative consent from the minor.
B. Affirmative consent from a minor's parent or guardian before collecting the minor's personal information online.
C. Implied consent from a minor's parent or guardian before collecting a minor's personal information online, such as when they permit the minor to use the internet.
D. Affirmative consent of a parent or guardian before collecting personal information of a minor ofline (e.g., in person), which also satisfies any requirements for online consent.

Answer: B

Explanation:

The Children's Online Privacy Protection Act (COPPA) is a federal law that regulates the online collection and use of personal information from children under 13 years of age. COPPA requires operators of websites or online services that are directed to children, or that knowingly collect personal information from children, to obtain verifiable parental consent before collecting, using, or disclosing such information. Verifiable parental consent means any reasonable effort (taking into

consideration available technology) to ensure that before personal information is collected from a child, the child's parent receives notice of the operator's information practices and consents to those practices. COPPA also imposes other obligations on operators, such as providing parents with access to their children's information, maintaining reasonable security measures, and limiting data retention. Reference: COPPA, IAPP CIPP/US Study Guide, Chapter 2, Section 2.3.1

Question: 95

If an organization maintains data classified as high sensitivity in the same system as data classified as low sensitivity, which of the following is the most likely outcome?

A. The organization will still be in compliance with most sector-specific privacy and security laws.
B. The impact of an organizational data breach will be more severe than if the data had been segregated.
C. Temporary employees will be able to find the data necessary to fulfill their responsibilities.
D. The organization will be able to address legal discovery requests efficiently without producing more information than necessary.

Answer: B

Explanation:
Data classification is the process of categorizing data based on its sensitivity and importance to determine its level of confidentiality and protection. Data classification helps organizations apply appropriate security and compliance measures to ensure each category receives proper protection1. Data classification also helps organizations identify which data is subject to specific privacy laws and regulations, such as the GDPR, HIPAA, or CCPA, and how to handle data subject requests, data breaches, or legal discovery2. If an organization maintains data classified as high sensitivity, such as personal information, financial information, or health information, in the same system as data classified as low sensitivity, such as public information or internal information, it increases the risk of exposing the high sensitivity data in the event of a data breach. A data breach can result in legal consequences, reputational damage, and loss of trust from customers and stakeholders. Therefore, it is advisable to segregate data based on its classification and apply different levels of encryption, access control, and monitoring to each category3. This way, the organization can minimize the impact of a data breach and protect the privacy and security of its data assets. Reference:
Why Is Data Classification Important?
Data Classification for GDPR Explained
Data classification and privacy considerations

Question: 96

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. An international court ruling on personal information held in the commercial sector.
D. A baseline of marketers' minimum responsibilities for providing opt-out mechanisms.

Answer: C

Explanation:

The APEC principles are part of the APEC Privacy Framework, which is an inter-governmental agreement among the 21 member economies of the Asia-Pacific Economic Cooperation (APEC) to promote information privacy protection and the free flow of information in the region. The APEC Privacy Framework consists of four parts: a preamble, a scope, a set of nine information privacy principles, and an implementation section. The APEC information privacy principles are: Preventing harm: Personal information controllers should take reasonable steps to protect personal information from loss, misuse, unauthorized access, disclosure, alteration, and destruction, and to address the risks and challenges posed by specific technologies and business practices.

Notice: Personal information controllers should provide clear and easily accessible statements about their personal information handling practices, including the types of personal information they collect, the purposes for which they collect it, the types of third parties to which they disclose it, the choices and means they offer individuals for limiting the use and disclosure of their personal information, and how they can contact the personal information controller with inquiries or complaints.

Collection limitation: Personal information controllers should limit the collection of personal information to what is relevant for the purposes of collection and should collect personal information by lawful and fair means and, where appropriate, with notice to, or consent of, the individual concerned.

Use limitation: Personal information controllers should use personal information only for the purposes for which it was collected or for purposes that a reasonable person would consider appropriate in the circumstances, and should retain personal information only as long as necessary to fulfill the stated purposes or as required by law or regulation.

Choice: Personal information controllers should offer individuals choices and means to limit the use and disclosure of their personal information, where appropriate, and should respect the choices made by individuals.

Integrity of personal information: Personal information controllers should take reasonable steps to ensure that personal information is accurate, complete, and up-to-date for the purposes for which it is used.

Security safeguards: Personal information controllers should protect personal information with reasonable security safeguards against risks such as loss, unauthorized access, destruction, misuse, modification, and disclosure.

Access and correction: Personal information controllers should give individuals the ability to access and, where appropriate, correct their personal information that is under their control, subject to reasonable limitations, such as where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy, or where the legitimate rights of persons other than the individual would be violated.

Accountability: Personal information controllers should be accountable for complying with the privacy principles and should have in place mechanisms to ensure their implementation and compliance.

The APEC Privacy Framework is not a binding legal instrument, but rather a voluntary and flexible arrangement that allows each member economy to implement the principles according to its own domestic laws and regulations, applicable international frameworks, and cultural and social values. The APEC Privacy Framework also provides for cross-border cooperation and information sharing among member economies, as well as the development of mechanisms to facilitate the cross-border transfer of personal information, such as the APEC

Cross-Border Privacy Rules (CBPR) System and the APEC Privacy Recognition for Processors (PRP) System. These mechanisms are based on a common set of rules and standards derived from the APEC Privacy Framework, and are intended to enhance the protection of personal information that flows across borders and to increase the interoperability among different privacy regimes in the region and beyond.

Reference: APEC Privacy Framework (2015)
APEC Cross-Border Privacy Rules (CBPR) System
APEC Privacy Recognition for Processors (PRP) System
APEC Privacy Framework: A New Model for Transborder Data Flows

Question: 97

Which of the following became the first state to pass a law specifically regulating the practices of data brokers?

A. Washington.
B. California.
C. New York.
D. Vermont.

Answer: D

Explanation:
According to the web search results from my predefined tool, Vermont became the first state to pass a law specifically regulating the practices of data brokers in 2018. The law defines a data broker as "a business, or unit or units of a business, separately or together, that knowingly collects and sells or licenses to third parties the brokered personal information of a consumer with whom the business does not have a direct relationship." The law requires data brokers to register with the Secretary of State, pay a registration fee, provide information about their data collection and opt-out practices, and implement security measures to protect the personal information they collect and sell. The law also imposes additional obligations on data brokers that possess the personal information of minors. The law aims to increase the transparency and accountability of the data broker industry and to protect the privacy rights of consumers12.

Reference:
Registered Data Brokers in the United States: 2021 | Privacy Rights ... Am I A Data Broker?: A Quick Primer on State Laws Regulating a ... - Taft

Question: 98

Acme Student Loan Company has developed an artificial intelligence algorithm that determines whether an individual is likely to pay their bill or default. A person who is determined by the

algorithm to be more likely to default will receive frequent payment reminder calls, while those who are less likely to default will not receive payment reminders.

Which of the following most accurately reflects the privacy concerns with Acme Student Loan Company using

artificial intelligence in this manner?

A. If the algorithm uses risk factors that impact the automatic decision engine. Acme must ensure that the algorithm does not have a disparate impact on protected classes in the output.
B. If the algorithm makes automated decisions based on risk factors and public information, Acme need not determine if the algorithm has a disparate impact on protected classes.
C. If the algorithm's methodology is disclosed to consumers, then it is acceptable for Acme to have a disparate impact on protected classes.
D. If the algorithm uses information about protected classes to make automated decisions, Acme must ensure that the algorithm does not have a disparate impact on protected classes in the output.

Answer: D

Explanation:
The correct answer is D. If the algorithm uses information about protected classes to make automated decisions, Acme must ensure that the algorithm does not have a disparate impact on protected classes in the output. The Fair Credit Reporting Act (FCRA) protects consumers from unfair, inaccurate, and discriminatory treatment by creditors and other businesses that use credit reports. The FCRA prohibits creditors from using information about protected classes, such as race, color, religion, national origin, sex, marital status, age, or because they receive income from a public assistance program, to make decisions about credit. In the case of Acme Student Loan Company, the algorithm is using information about protected classes to make automated decisions about whether to send payment reminder calls. This could have a disparate impact on protected classes, such as people of color or people with low incomes. For example, people of color may be more likely to be identified as being at risk of default, even if they are just as likely to repay their loans as people of other races. Acme Student Loan Company must ensure that the algorithm does not have a disparate impact on protected classes. This could be done by using a variety of methods, such as:
Testing the algorithm for accuracy, fairness, and bias before and after deployment Providing consumers with notice and consent options for the use of their data Allowing consumers to access, correct, or delete their data
Implementing accountability and oversight mechanisms for the algorithm Ensuring compliance with applicable laws and regulations
Reference: https://economictimes.indiatimes.com/news/how-to/ai-and-privacy-the-privacy- concerns-surrounding-ai-its-potential-impact-on-personal-data/articleshow/99738234.cmshttps://pupuweb.com/iapp-cipp-us-qa-privacy-concerns-acme-student-loan-company-artificial- intelligence/

Question: 99

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.

E. Providing notice to employees that their emails will be scanned by the software and creating automated profiles.

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:

U.S. Private-Sector Privacy, Third Edition by Peter P. Swire, DeBrae Kennedy-Mayo, Chapter 4, Section 4.2.1, pp. 97-98.

U.S. Private-Sector Privacy, Third Edition by Peter P. Swire, DeBrae Kennedy-Mayo, Chapter 5, Section 5.2.1, pp. 125-126.

U.S. Private-Sector Privacy, Third Edition by Peter P. Swire, DeBrae Kennedy-Mayo, Chapter 6, Section 6.2.1, pp. 153-154.

IAPP CIPP/US Certified Information Privacy Professional Study Guide by Mike Chapple and Joe Shelley, Chapter 4, Section 4.1, pp. 113-114.

Question: 100

Which of the following would NOT constitute an exception to the authorization requirement under the HIPAA Privacy Rule?

A. Disclosing health information for public health activities.
B. Disclosing health information to file a child abuse report.
C. Disclosing health information needed to treat a medical emergency.
D. Disclosing health information needed to pay a third party billing administrator.

Answer: D

Explanation:
The HIPAA Privacy Rule requires covered entities to obtain an individual's written authorization for any use or disclosure of protected health information (PHI) that is not for treatment, payment, or health care operations or otherwise permitted or required by the Privacy Rule. However, there are some exceptions to the authorization requirement for certain public interest-related activities, such as disclosing health information for public health activities, reporting child abuse, or treating a medical emergency. These exceptions are intended to balance the privacy interests of individuals with the public interest in protecting health and safety, promoting quality health care, and ensuring compliance with the law. Disclosing health information needed to pay a third party billing administrator is not one of the exceptions to the authorization requirement, as it is considered a payment activity that falls under the general rule of requiring authorization. Therefore, it is the correct answer to the question. Reference: Summary of the HIPAA Privacy Rule, HIPAA Exceptions, Exceptions to HIPAA Privacy Rule, Waiver of Authorization, IAPP CIPP/US Study Guide, Chapter 5.

Question: 101

What type of material is exempt from an individual's right to disclosure under the Privacy Act?

A. Material requires by statute to be maintained and used solely for research purposes.
B. Material reporting investigative efforts to prevent unlawful persecution of an individual.
C. Material used to determine potential collaboration with foreign governments in negotiation of trade deals.
D. Material reporting investigative efforts pertaining to the enforcement of criminal law.

Answer: D

Explanation:
The Privacy Act allows agencies to exempt certain records from some of its provisions, including the right to disclosure, if the records fall within one of the categories specified in subsections (j) or (k) of the Act. One of these categories is records maintained by an agency or component thereof which performs as its principal function any activity pertaining to the enforcement of criminal laws, including police efforts to prevent, control, or reduce crime or to apprehend criminals, and the activities of prosecutors, courts, correctional, probation, pardon, or parole authorities, and which consists of (A) information compiled for the purpose of identifying individual criminal offenders and

alleged offenders and consisting only of identifying data and notations of arrests, the nature and disposition of criminal charges, sentencing, confinement, release, and parole and probation status; (B) information compiled for the purpose of a criminal investigation, including reports of informants and investigators, and associated with an identifiable individual; or © reports identifiable to an individual compiled at any stage of the process of enforcement of the criminal laws from arrest or indictment through release from supervision. 5 U.S.C. § 552a (j) (2). Therefore, material reporting investigative efforts pertaining to the enforcement of criminal law falls within this category and can be exempted from the right to disclosure under the Privacy Act.

Reference: Overview of the Privacy Act: 2020 Edition, Ten Exemptions, subsection (j) (2).
Privacy Act Exemptions, subsection (j) (2).
IAPP CIPP/US Study Guide, page 66.

Question: 102

Which of the following best describes an employer's privacy-related responsibilities to an employee who has left the workplace?

A. An employer has a responsibility to maintain a former employee's access to computer systems and company data needed to support claims against the company such as discrimination.

B. An employer has a responsibility to permanently delete or expunge all sensitive employment records to minimize privacy risks to both the employer and former employee.

C. An employer may consider any privacy-related responsibilities terminated, as the relationship between employer and employee is considered primarily contractual.

D. An employer has a responsibility to maintain the security and privacy of any sensitive employment records retained for a legitimate business purpose.

Answer: D

Explanation:

Employers have a duty to protect the personal information of their current and former employees, as well as applicants, from unauthorized access, use, or disclosure. This duty may arise from federal or state laws, such as the Fair Credit Reporting Act (FCRA), the Health Insurance Portability and Accountability Act (HIPAA), or the California Consumer Privacy Act (CCPA), or from contractual obligations, such as non-disclosure agreements or privacy policies. Employers may retain sensitive employment records, such as performance evaluations, disciplinary actions, medical records, or background checks, for a legitimate business purpose, such as complying with legal requirements, defending against lawsuits, or conducting audits. However, employers must ensure that these records are stored securely, accessed only by authorized personnel, and disposed of properly when no longer needed. Reference: IAPP CIPP/US Study Guide, Chapter 4, Section 4.1.1, IAPP CIPP/US Body of Knowledge, Domain IV, Objective B

Question: 103

All of the following common law torts are relevant to employee privacy under US law EXCEPT?

A. Infliction of emotional distress.

B. Intrusion upon seclusion.

C. Defamation

D. Conversion.

Answer: D

Explanation:

Question: 104

Which law provides employee benefits, but often mandates the collection of medical information?

A. The Occupational Safety and Health Act.
B. The Americans with Disabilities Act.
C. The Employee Medical Security Act.
D. The Family and Medical Leave Act.

Answer: D

Explanation:

The Family and Medical Leave Act (FMLA) is a federal law that provides eligible employees with up to 12 weeks of unpaid, job-protected leave per year for certain family and medical reasons, such as the birth or adoption of a child, the serious health condition of the employee or a family member, or a qualifying exigency arising from the employee's spouse, child, or parent being on covered active duty or call to covered active duty status in the Armed Forces. The FMLA also provides eligible employees with up to 26 weeks of unpaid, job-protected leave per year to care for a covered service member with a serious injury or illness if the employee is the spouse, child, parent, or next of kin of the service member. The FMLA applies to all public agencies, including state, local, and federal employers, and local education agencies (schools), and to private sector employers who employ 50 or more employees for at least 20 workweeks in the current or preceding calendar year.

The FMLA often requires employers to collect medical information from employees who request FMLA leave or from their health care providers to certify the need for leave, the duration of leave, and the employee's ability to return to work. The FMLA regulations specify the type and amount of information that employers may request and require for different types of FMLA leave, such as: Basic medical facts, such as the diagnosis, symptoms, hospitalization, doctor visits, whether medication has been prescribed, and any referrals for evaluation or treatment, for the employee's own serious health condition or that of a family member.

Information on the medical necessity of intermittent leave or reduced schedule leave and the expected frequency and duration of such leave, for the employee's own serious health condition or that of a family member, or for planned medical treatment.

A statement of the facts regarding the qualifying exigency, such as the type of military duty, the dates of the covered active duty, and the contact information of the military member, for leave due to a qualifying exigency arising from the employee's spouse, child, or parent being on covered active duty or call to covered active duty status in the Armed Forces.

Information on the medical condition, treatment, and recovery of the covered service member, such as the date of injury or onset of illness, the current medical status, the prognosis, and the estimated time of treatment, for leave to care for a covered service member with a serious injury or illness.

The FMLA also imposes certain obligations on employers to protect the privacy and security of the medical information they collect from employees or their health care providers. For example, employers must: Maintain records and documents relating to medical certifications, recertifications, or medical histories of employees or employees' family members as confidential medical records in separate files/records from the usual personnel files, and if the Americans with Disabilities Act (ADA) applies, such records must be maintained in conformance with ADA confidentiality requirements.

Ensure that any electronic systems used to maintain such records meet the confidentiality requirements of the FMLA and the ADA, and that only authorized persons have access to such records.
Limit the disclosure of such records to supervisors and managers who need to know about an employee's FMLA leave, first aid and safety personnel when an employee's medical condition might require emergency treatment, and government officials investigating compliance with the FMLA. Comply with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule when requesting medical information from an employee's health care provider, such as obtaining a valid authorization from the employee or using a HIPAA-compliant certification form.
Refrain from requesting more information than allowed by the FMLA regulations, such as asking for an employee's complete medical records or information unrelated to the FMLA leave request.
Respect the employee's right to revoke a medical authorization or challenge a medical certification, and follow the procedures for resolving disputes over the validity or sufficiency of such documents. Reference:
The Family and Medical Leave Act (FMLA)
FMLA Employee Guide
FMLA Employer Guide
FMLA Regulations
FMLA Forms

Question: 105

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 has no right to sue the corporation because the CCPA does not address any data breach rights.
B. John cannot sue the corporation for the data breach because only the state's Attoney 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 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.

Answer: D

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. Reference:
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

Question: 106

Smith Memorial Healthcare (SMH) is a hospital network headquartered in New York and operating in 7 other states. SMH uses an electronic medical record to enter and track information about its patients. Recently, SMH suffered a data breach where a third-party hacker was able to gain access to the SMH internal network. Because it is a HIPPA-covered entity, SMH made a notification to the Office of Civil Rights at the U.S. Department of Health and Human Services about the breach.

Which statement accurately describes SMH's notification responsibilities?

A. If SMH is compliant with HIPAA, it will not have to make a separate notification to individuals in the state of New York.
B. If SMH has more than 500 patients in the state of New York, it will need to make separate notifications to these patients.
C. If SMH must make a notification in any other state in which it operates, it must also make a notification to individuals in New York.
D. If SMH makes credit monitoring available to individuals who inquire, it will not have to make a separate notification to individuals in the state of New York.

Answer: C

Explanation:
The correct answer is C. If SMH must make a notification in any other state in which it operates, it must also make a notification to individuals in New York. Under the Health Insurance Portability and Accountability Act (HIPAA), SMH is required to notify the Office of Civil Rights (OCR) and the affected individuals of a data breach involving unsecured protected health information (PHI) within 60 days of discovery1. However, HIPAA does not preempt state laws that provide greater protection to individuals or impose additional obligations on covered entities2. Therefore, SMH must also comply with the state breach notification laws of the states where it operates, including New York. According to the New York State Information Security Breach and Notification Act, any person or business that owns or licenses computerized data that includes private information of a resident of New York must disclose any breach of the security of the system to such resident in the most expedient time possible and without unreasonable delay, unless the exposure of the private information was inadvertent and unlikely to result in misuse or financial harm3. Private information includes personal information (such as name, number, or other identifier) plus one or more of the following data elements: social security number; driver's license number or non-driver identification card number; account number, credit or debit card number, in combination with any required security code, access code, password or other

information that would permit access to an individual's financial account; biometric information; or a user name or e-mail address in combination with a password or security question and answer that would permit access to an online account3.

Therefore, if SMH's data breach involved any of these data elements of New York residents, SMH must notify them of the breach, regardless of whether SMH is compliant with HIPAA, has more than 500 patients in New York, or offers credit monitoring services. SMH must also notify the New York Attorney General, the Department of State, and the Division of State Police within 10 days of notifying the affected individuals3.

Additionally, SMH must notify the New York Department of Health if the breach involved electronic health records4.

Reference: https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Guide-on- Managing-and-Notifying-Data-Breaches-under-the-PDPA-15-Mar-2021.pdf?la=enhttps://www.pcpd.org.hk/english/resources_centre/publications/files/guidance_note_dbn_e.pdf

Question: 107

Sarah lives in San Francisco, Californi

a. Based on a dramatic increase in unsolicited commercial emails, Sarah believes that a major social media platform with over 50 million users has collected a lot of personal information about her. The company that runs the platform is based in New York and France.

Why is Sarah entitled to ask the social media platform to delete the personal information they have collected about her?

A. Any company with a presence in Europe must comply with the General Data Protection Regulation globally, including in response to data subject deletion requests.

B. Under Section 5 of the FTC Act, the Federal Trade Commission has held that refusing to delete an individual's personal information upon request constitutes an unfair practice.

C. The California Consumer Privacy Act entitles Sarah to request deletion of her personal information.

D. The New York "Stop Hacks and Improve Electronic Data Security" (SHIELD) Act requires that businesses under New York's jurisdiction must delete customers' personal information upon request.

Answer: C

Explanation:

The correct answer is C because the California Consumer Privacy Act (CCPA) is a state privacy law that grants California residents the right to request the deletion of their personal information that a business has collected from them. The CCPA applies to any business that collects personal information from California residents, regardless of where the business is located, as long as the business meets certain thresholds of revenue, data volume, or data sharing. Therefore, the social media platform that Sarah uses is subject to the CCPA and must honor Sarah's deletion request, unless an exception applies. The CCPA also requires businesses to provide notice and choice to consumers about their data collection and use practices, and to respond to consumer requests within 45 days.

The other answers are incorrect because:

A is incorrect because the General Data Protection Regulation (GDPR) is a European Union privacy law that

applies to the processing of personal data of individuals who are in the EU, regardless of where the data controller or processor is located. However, the GDPR does not apply to the processing of personal data of individuals who are outside the EU, unless the processing relates to the offering of goods or services to such individuals or the monitoring of their behavior within the EU. Therefore, the GDPR does not apply to Sarah's personal data, since she is not in the EU and the social media platform is not targeting or tracking her in the EU.

B is incorrect because Section 5 of the FTC Act is a federal law that prohibits unfair or deceptive acts or practices in or affecting commerce. The FTC has used its Section 5 authority to enforce privacy and data security standards against businesses that violate their own privacy policies, misrepresent their data practices, or fail to protect consumer data from unauthorized access or disclosure. However, the FTC has not held that refusing to delete an individual's personal information upon request constitutes an unfair practice per se, unless the refusal is inconsistent with the business's privacy policy or representations, or causes substantial injury to consumers that is not reasonably avoidable or outweighed by countervailing benefits.

D is incorrect because the New York SHIELD Act is a state law that imposes data breach notification and data security requirements on any person or business that owns or licenses computerized data that includes the private information of a New York resident. The SHIELD Act does not grant New York residents the right to request the deletion of their personal information, nor does it apply to businesses that do not collect or hold the private information of New York residents. Therefore, the SHIELD Act does not apply to Sarah's personal data, since she is not a New York resident and the social media platform may not have her private information as defined by the SHIELD Act. Reference: U.S. Private-Sector Privacy, Third Edition by Peter P. Swire, DeBrae Kennedy-Mayo, Chapter 7, Section 7.2.1, pp. 183-186.

IAPP CIPP/US Certified Information Privacy Professional Study Guide by Mike Chapple and Joe Shelley, Chapter 7, Section 7.2, pp. 217-219.

Question: 108

Which of the following is an example of federal preemption?

A. The Payment Card Industry's (PCI) ability to self-regulate and enforce data security standards for payment card data.

B. The U.S. Federal Trade Commission's (FTC) ability to enforce against unfair and deceptive trade practices across sectors and industries.

C. The California Consumer Privacy Act (CCPA) regulating businesses that have no physical brick-and- mortal presence in California, but which do business there.

D. The U.S. Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act prohibiting states from passing laws that impose greater obligations on senders of email marketing.

Answer: D

Explanation:

Federal preemption is a doctrine in law that allows a federal law to take precedence over or to displace a state law in certain matters of national importance (such as interstate commerce). The doctrine is based on the Supremacy Clause of the Constitution, which declares that federal law is the "supreme law of the land" and that state judges are bound by it. There are two types of federal preemption: express and implied. Express preemption occurs when Congress expressly states that a federal law is intended to preempt certain types of state legislation. Implied preemption occurs when a state law conflicts with federal law because it is impossible to comply with both at the same time, or because it interferes with the objectives of

the federal law, or because the federal government has fully occupied the field of regulation.

The U.S. Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act is an example of express preemption. The Act regulates commercial email messages and establishes requirements for senders and penalties for violations. The Act also explicitly preempts any state law that "expressly regulates the use of electronic mail to send commercial messages", except for state laws that prohibit falsity or deception. This means that states cannot pass laws that impose greater obligations on senders of email marketing than the federal law, such as requiring opt-in consent or providing additional opt-out mechanisms. Therefore, the CAN-SPAM Act is the correct answer to the question.

The other options are not examples of federal preemption. The Payment Card Industry's (PCI) ability to self-regulate and enforce data security standards for payment card data is not a federal law, but a private sector initiative. The U.S. Federal Trade Commission's (FTC) ability to enforce against unfair and deceptive trade practices across sectors and industries is not a preemption of state law, but a concurrent power that can coexist with state consumer protection laws. The California Consumer Privacy Act (CCPA) regulating businesses that have no physical brick-and-mortal presence in California, but which do business there, is not preempted by any federal law, but is a state law that applies to entities that meet certain criteria of collecting or selling personal information of California residents. Reference: Federal preemption, What is Federal Preemption?, Federal preemption Definition & Meaning, preemption, Preemption legal definition of Preemption, CAN-SPAM Act, IAPP CIPP/US Study Guide, Chapter 2.

Question: 109

Which of these organizations would be required to provide its customers with an annual privacy notice?

A. The Four Winds Tribal College.
B. The Golden Gavel Auction House.
C. The King County Savings and Loan.
D. The Breezy City Housing Commission.

Answer: C

Explanation:

The annual privacy notice requirement under the Gramm-Leach-Bliley Act (GLBA) applies to financial institutions that collect nonpublic personal information from customers and disclose it to nonaffiliated third parties, unless they qualify for an exception. A financial institution is any entity that engages in activities that are financial in nature or incidental to such activities, as defined by section 4(k) of the Bank Holding Company Act of 1956. The King County Savings and Loan is a financial institution under this definition, as it engages in lending money and accepting deposits. Therefore, it is required to provide its customers with an annual privacy notice, unless it meets the conditions for an exception. The Four Winds Tribal College, the Golden Gavel Auction House, and the Breezy City Housing Commission are not financial institutions under the GLBA, as they do not engage in activities that are financial in nature or incidental to such activities. Therefore, they are not required to provide their customers with an annual privacy notice under the GLBA. Reference: Amendment to the Annual Privacy Notice Requirement Under the Gramm-Leach-Bliley Act, section I. Background, paragraph 2.
17 CFR § 248.5 - Annual privacy notice to customers required., paragraph (a) (1).
IAPP CIPP/US Study Guide, page 65.

Question: 110

Which entity within the Department of Health and Human Services (HHS) is the primary enforcer of the Health Insurance Portability and Accountability Act (HIPAA) "Privacy Rule"?

A. Office for Civil Rights.
B. Office of Social Services.
C. Office of Inspector General.
D. Office of Public Health and Safety.

Answer: A

Explanation:
The Office for Civil Rights (OCR) within the HHS is the primary enforcer of the HIPAA Privacy Rule, which establishes national standards for the protection of individually identifiable health information by covered entities and business associates. The OCR investigates complaints, conducts compliance reviews, and provides technical assistance and guidance to ensure compliance with the Privacy Rule. The OCR can also impose civil monetary penalties for violations of the Privacy Rule, ranging from $100 to $50,000 per violation, up to a maximum of $1.5 million per year for the same violation. Reference: HIPAA Enforcement, IAPP CIPP/US Study Guide, Chapter 3, Section 3.1.1

Question: 111

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

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

Explanation:
Federal anti-discrimination laws, such as Title VII of the Civil Rights Act of 1964, the Equal Pay Act of 1963, the Age Discrimination in Employment Act of 1967, and the Americans with Disabilities Act of 1990, prohibit employers from discriminating against employees or applicants based on certain protected characteristics, such as race, color, religion, sex, national origin, age, disability, and genetic information. These laws also limit the types of information that employers can collect, use, disclose, or retain about employees or applicants, in order to prevent discrimination or invasion of privacy. For example, employers cannot ask about an applicant's medical history, disability status, genetic information, or religious beliefs, unless they are relevant to the job or a bona fide occupational qualification. Employers also cannot use such information to make adverse employment decisions, such as hiring, firing, promotion, or compensation, unless they are justified by a

legitimate business necessity or a reasonable accommodation. Employers must also safeguard the confidentiality of such information and dispose of it properly when it is no longer needed.

Reference:

Federal Laws Prohibiting Job Discrimination Questions And Answers Laws Enforced by EEOC

Employment and Anti-Discrimination Laws in the Workplace

Protections Against Discrimination and Other Prohibited Practices

3. Who is protected from employment discrimination?

Question: 112

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

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: B

Explanation:

The CCPA grants California residents the right to request that a business delete, disclose, or stop selling their personal information, but it does not grant them the right to request that a business correct their personal information. However, the CPRA, which will amend and expand the CCPA in 2023, will grant California residents the right to request that a business correct inaccurate personal information. Reference: CCPA, CPRA, IAPP CIPP/US Study Guide (p. 62)

Question: 113

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

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

Explanation:
The FTC is the primary federal agency responsible for enforcing privacy and data security laws in the United States. The FTC has broad jurisdiction over most commercial entities that collect, use, or share personal information from consumers. The FTC Act prohibits unfair or deceptive acts or practices in or affecting commerce, which includes unfair or deceptive privacy practices. The FTC can bring enforcement actions against companies that violate their own privacy policies, fail to provide adequate notice or choice to consumers, engage in unfair or harmful data practices, or breach consumers' reasonable expectations of privacy. The FTC can also issue rules, guidelines, and reports on privacy and data security issues, as well as conduct investigations, workshops, and educational campaigns. Reference:
IAPP CIPP/US Body of Knowledge, Section I.A.1.a
IAPP CIPP/US Textbook, Chapter 1, pp. 9-12
FTC Privacy and Security Enforcement

Question: 114

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?

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

Explanation:
The scenario describes how the company had no adequate rules about access to customer information and how low-level employees had access to all of the company's customer data, including financial records. This indicates that the company did not implement proper access controls to limit who can access, use, or disclose customer information based on their roles and responsibilities. Access controls are one of the key elements of information security and privacy, as they help prevent unauthorized or inappropriate access to sensitive data. Without access controls,

the company's customer information was vulnerable to mishandling by employees or outsiders who could exploit the weak security measures. Therefore, the most likely cause of the breach was mishandling of information caused by lack of access controls. Reference:
IAPP CIPP/US Certified Information Privacy Professional Study Guide, Chapter 4: Information Management from a U.S. Perspective, Section 4.2: Information Security, p. 113-114
IAPP CIPP/US Body of Knowledge, Domain I: Introduction to the U.S. Privacy Environment, Objective 1 .C: Describe the role of information security in privacy, Subobjective I.C.1: Identify the key elements of information security, p. 8

Question: 115

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.

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

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

Explanation:
The Consumer Privacy Bill of Rights is a set of principles proposed by the Obama administration in 2012 to protect the privacy of consumers online and ofline. The principles are based on the Fair Information Practice Principles, which are widely accepted as the foundation of privacy protection. One of the principles is the right to reasonable limits on the personal data that a company retains, which means that companies should collect and keep only the personal data they need for legitimate purposes, and dispose of it securely when it is no longer needed. This principle would best reform the company's privacy program in the scenario, as it would address the major concerns that Roberta identified in her report, such as the lack of rules and procedures for purging and destroying outdated data, and the excessive access to customer information by low-level employees. By implementing reasonable limits on the personal data that the company retains, the company would reduce the risk of data breaches, enhance customer trust, and comply with state breach notification laws. Reference: Fact Sheet: Plan to Protect Privacy in the Internet Age by Adopting a Consumer Privacy Bill of Rights IAPP CIPP/US Certified Information Privacy Professional Study Guide, Chapter 1: Introduction to U.S. Privacy Law, Section 1.2: The Consumer Privacy Bill of Rights

Question: 116

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.

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.

Answer: A

Explanation:

The scenario suggests that the company lacked adequate rules about access to customer information, which increased the risk of unauthorized access and data breach. Implementing a comprehensive policy for accessing customer information would have helped the company to limit the access to only those who need it for legitimate purposes, and to protect the confidentiality, integrity, and availability of the data. This is also one of the recommendations that Roberta made in her report. Reference:
CIPP/US Practice Questions (Sample Questions), Question 116, Answer A, Explanation A.
IAPP CIPP/US Certified Information Privacy Professional Study Guide, Chapter 5, Section 5.2, p. 143.

Question: 117

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 network?" 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 Questio ns about my opinions."
"Let me see," Matt said, and began reading the list of Questio ns 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.

Based on the incident, the FTC's enforcement actions against the marketer would most likely include what violation?

A. Intruding upon the privacy of a family with young children.
B. Collecting information from a child under the age of thirteen.
C. Failing to notify of a breach of children's private information.
D. Disregarding the privacy policy of the children's marketing industry.

Answer: B

Based on the incident, the FTC's enforcement actions against the marketer would most likely include the violation of collecting information from a child under the age of thirteen without obtaining verifiable parental consent, as required by the Children's Online Privacy Protection Act (COPPA) Rule. The COPPA Rule applies to operators of commercial websites and online services (including mobile apps) that collect, use, or disclose personal information from children under 13, and operators of general audience websites or online services that have actual knowledge that they are collecting, using, or disclosing personal information from children under 13. The COPPA Rule also applies to websites or online services that are directed to children under 13 and that collect personal information from users of any age. The COPPA Rule defines personal information to include full name, address, phone number, email address, date of birth, and other identifiers that permit the physical or online contacting of a specific individual. The COPPA Rule requires operators to post a clear and comprehensive online privacy policy describing their information practices for personal information collected online from children; provide direct notice to parents and obtain verifiable parental consent, with limited exceptions, before collecting personal information online from children; give parents the choice of consenting to the operator's collection and internal use of a child's information, but prohibiting the operator from disclosing that information to third parties (unless disclosure is integral to the site or service, in which case, this must be made clear to parents); provide parents access to their child's personal information to review and/or

have the information deleted; give parents the opportunity to prevent further use or online collection of a child's personal information; maintain the confidentiality, security, and integrity of information they collect from children, including by taking reasonable steps to release such information only to parties capable of maintaining its confidentiality and security; and retain personal information collected online from a child for only as long as is necessary to fulfill the purpose for which it was collected and delete the information using reasonable measures to protect against its unauthorized access or use. The FTC has the authority to seek civil penalties and injunctive relief for violations of the COPPA Rule. The FTC has

brought numerous enforcement actions against operators for violating the COPPA Rule, resulting in millions of dollars in penalties and orders to delete illegally collected data. References:

Children's Privacy | Federal Trade Commission
Kids' Privacy (COPPA) | Federal Trade Commission
FTC Is Escalating Scrutiny of Dark Patterns, Children's Privacy
FTC to Crack Down on Companies that Illegally Surveil Children Learning Online
FTC Takes Action Against Company for Collecting Children's Personal Information Without Parental Permission
[IAPP CIPP/US Certified Information Privacy Professional Study Guide], Chapter 5, pages 165-168.

Question: 118

Under the California Consumer Privacy Act (as amended by the California Pnvacy Rights Act), a consumer may Initiate a civil action against a business for?

A. Any personal information that is subject to unauthorized access or disclosure.
B. A security breach of certain categories of personal information that is nonencrypted and nonredacted
C. Failure to implement and maintain reasonable security procedures and practices to protect the personal information held.
D. Failure to implement and maintain security practices set out in regulations issued by the California Privacy Protection Agency (CPPA).

Answer: B

Explanation:
Under the California Consumer Privacy Act (CCPA), as amended by the California Privacy Rights Act (CPRA), consumers have the right to initiate a civil action if a business fails to adequately protect their personal information and a security breach occurs. This right applies specifically to breaches of certain categories of personal information that are unencrypted and unredacted.
Key Details of CCPA/CPRA Civil Actions:
Security Breaches:
A consumer can sue a business if the breach involves personal information such as Social Security numbers, driver's license numbers, or financial account information, provided that the data was unencrypted and unredacted.
Reasonable Security Practices:
Businesses are required to implement and maintain reasonable security practices to protect personal information. Failure to do so may expose the business to liability in case of a breach.
Categories of Data Covered:

The law specifies that only certain sensitive categories of personal information are actionable under a civil suit.

Explanation of Options:

A . Any personal information that is subject to unauthorized access or disclosure:

This is incorrect. The civil action is limited to specific sensitive data categories, not all personal information.

B . A security breach of certain categories of personal information that is nonencrypted and nonredacted:

This is correct. Civil actions under the CCPA/CPRA apply to breaches involving specific sensitive data that is not encrypted or redacted.

C . Failure to implement and maintain reasonable security procedures and practices to protect the personal information held:

While this is a requirement under the law, it does not by itself provide grounds for a civil action. A security breach must occur for a consumer to sue.

D . Failure to implement and maintain security practices set out in regulations issued by the California Privacy Protection Agency (CPPA):

This is incorrect. Civil actions are tied to breaches of sensitive data, not a failure to meet specific agency guidelines.

Reference from CIPP/US Materials:

CCPA/CPRA (Civil Code § 1798.150): Outlines the private right of action for security breaches involving certain unencrypted and unredacted data.

IAPP CIPP/US Certification Textbook: Discusses the conditions under which consumers may bring civil actions under the CCPA/CPRA.

Question: 119

A California resident has created an account on your company's online food delivery platform and placed several orders in the past month Later she submits a data subject request to access her personal information under the California Privacy Rights Act.

Based on the CPR

A. which of the following data elements would your company NOT have to provide to the requestor once her identity has been verified?

A. Inferences made about the individual for the company s internal purposes
B. The loyalty account number assigned through the individuals use of the services
C. The time stamp for the creation of the individual's account in the platform's database.
D. The email address submitted by the individual as part of the account registration process.

Answer: A

Explanation:

Under the California Privacy Rights Act (CPRA), which amends the California Consumer Privacy Act (CCPA), California residents have the right to request access to their personal information collected by a business. However, the CPRA provides an exception for inferences made about an individual for internal purposes, meaning businesses are not obligated to disclose inferences generated solely for internal use.

Key Points Under the CPRA:

Access to Personal Information:

Businesses must provide consumers with access to personal information they have collected, which includes data submitted by the consumer and other information directly associated with the consumer.

Exception for Inferences:
Inferences made about a consumer, particularly when used for internal purposes (e.g., improving services, analytics, or predicting preferences), are not explicitly required to be disclosed under the CPRA unless they are part of the consumer's profile or used for decision-making purposes that affect the consumer.
Examples of Data to Be Provided:
Information provided by the consumer (e.g., email address, account information).
Automatically collected information (e.g., timestamps, purchase history).
Identifiers (e.g., loyalty account numbers).

Explanation of Options:

A . Inferences made about the individual for the company's internal purposes:
This is correct. Inferences generated for internal use are not considered part of the data set that must be disclosed in response to a CPRA data access request.
B . The loyalty account number assigned through the individual's use of the services: Loyalty account numbers are directly associated with the consumer and must be provided in response to an access request under the CPRA.
C. The time stamp for the creation of the individual's account in the platform's database: This information is part of the consumer's account data and must be disclosed under the CPRA. D . The email address submitted by the individual as part of the account registration process: This is personal information directly provided by the consumer and must be disclosed under the CPRA.
Reference from CIPP/US Materials:
CPRA (Civil Code § 1798.140): Defines personal information and exceptions for internal use, including inferences.
IAPP CIPP/US Certification Textbook: Discusses consumer rights under the CPRA, including access rights and the treatment of inferences.

Question: 120

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?

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

Explanation:
The marketer could be prosecuted for violating the Unfair and Deceptive Acts and Practices (UDAP) laws,

which are enforced by the Federal Trade Commission (FTC) and state attorneys general. UDAP laws prohibit businesses from engaging in unfair or deceptive practices that harm consumers, such as false advertising, misleading claims, or hidden fees. In this scenario, the marketer could be accused of deceiving children into providing personal information and preferences under the guise of a survey and a contest, without obtaining verifiable parental consent or disclosing how the information will be used or shared. This could also violate the Children's Online Privacy Protection Act (COPPA), which is a federal law that regulates the online collection and use of personal information from children under 13 years of age. Reference: [IAPP CIPP/US Study Guide], Chapter 5: Enforcement of Privacy and Security, pp. 177-178.
IAPP CIPP/US Body of Knowledge, Section II: Limits on Private-sector Collection and Use of Data, Subsection A: Government and Court Access to Private-sector Information, Topic 2: Unfair and Deceptive Trade Practices.
IAPP CIPP/US Practice Questions, Question 27.

Question: 121

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

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

Answer: C

Explanation:
An injunction is a court order that requires a party to stop or refrain from doing something. In a case of civil litigation, a defendant who is being sued for distributing an employee's private information might face an injunction that prohibits them from further disclosing or using the employee's private information. An injunction is a form of equitable relief that aims to prevent or remedy harm that cannot be adequately compensated by monetary damages. Probation, criminal fines, and jail sentences are forms of criminal sanctions that are not applicable in civil litigation, unless the defendant is also charged with a criminal offense related to the distribution of the employee's private information. Reference: Standing issues in U.S. privacy class actions, US Private-Sector Privacy (CIPP/US Exam Prep), IAPP CIPP/US

Question: 122

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?

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

Explanation:

The U.S. Supreme Court has recognized an individual's right to privacy over personal issues, such as contraception, by acknowledging a "penumbra" of unenumerated constitutional rights as well as more general protections of due process of law. This means that the right to privacy is not explicitly stated in the Constitution, but it is implied from other rights that are explicitly stated, such as the First Amendment rights of speech and assembly, the Third Amendment right to be free from quartering of soldiers, the Fourth Amendment right to be secure from unreasonable searches and seizures, the Fifth Amendment right to be free from self-incrimination, and the Ninth Amendment right to retain other rights not enumerated in the Constitution. These rights create a "zone of privacy" that protects individuals from undue government interference in their personal affairs. The Supreme Court first articulated this concept of privacy in Griswold v. Connecticut (1965), where it struck down a state law that prohibited the use of contraceptives by married couples. The Court also relied on the due process clause of the Fourteenth Amendment, which prohibits states from depriving any person of life, liberty, or property without due process of law. The Court interpreted this clause to include a substantive component that protects certain fundamental rights from state regulation, unless there is a compelling state interest and the regulation is narrowly tailored to achieve that interest. The Court has applied this due process analysis to other privacy issues, such as abortion, marriage, and sexual orientation. Reference:

Privacy | Wex | US Law | LII / Legal Information Institute

Privacy isn't in the Constitution – but it's everywhere in constitutional law

Privacy Rights and Personal Autonomy Legally Protected by the ... - Justia Right to privacy | Wex | US Law | LII / Legal Information Institute

Question: 123

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?

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:

According to the FTC report, the most important directive for businesses is to adopt a "privacy by design" approach, which means integrating privacy protections throughout the entire product lifecycle, from initial

design to disposal. This includes implementing reasonable security measures, collecting only the data needed for a specific purpose, retaining data only as long as necessary, and safely disposing of data that is no longer needed. The FTC report also recommends that businesses provide clear and transparent privacy notices, offer consumers meaningful choices about how their data is used, and increase their accountability for data practices. Reference: FTC Report, IAPP CIPP/US Study Guide (p. 32-33)

Question: 124

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

a. Which was NOT one of these principles?

A. Simplifying consumer choice.

B. Enhancing security measures.

C. Practicing Privacy by Design.

D. Providing greater transparency.

Answer: B

Explanation:

The FTC's privacy report, titled "Protecting Consumer Privacy in an Era of Rapid Change", proposed a framework for companies that collect and use consumer data. The framework consisted of three core principles: privacy by design, simplified consumer choice, and greater transparency. Privacy by design means that companies should incorporate privacy protections into their everyday business practices, such as data security, reasonable collection limits, sound retention practices, and data accuracy. Simplified consumer choice means that companies should provide consumers with clear and easy-to-understand choices about the collection and use of their data, and respect their preferences. Greater transparency means that companies should increase the visibility and accessibility of their data practices, such as providing clear and concise privacy notices, educating consumers about the commercial data practices, and providing consumers with access to their data. Enhancing security measures is not one of the core principles of the FTC's privacy framework, although it is a component of the privacy by design principle. Reference: IAPP CIPP/US Body of Knowledge, Section I.A.1.a IAPP CIPP/US Textbook, Chapter 1, pp. 13-15 FTC Privacy Report, Executive Summary, pp. i-vii

Question: 125

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

Answer: D

Explanation:

The GLBA prohibits financial institutions from disclosing a consumer's account number or similar form of access number or access code to any nonaffiliated third party for use in telemarketing, direct mail marketing, or other marketing through electronic mail to the consumer. This restriction is intended to prevent unauthorized access to a person's bank account by third parties who may use the account number to initiate fraudulent transactions or identity theft. The GLBA also requires financial institutions to implement safeguards to protect the security, confidentiality, and integrity of customer information, and to notify customers and regulators in the event of a security breach involving such information. Reference:

IAPP CIPP/US Certified Information Privacy Professional Study Guide, Chapter 2: Limits on Private-sector Collection and Use of Data, Section 2.3: Financial Privacy, p. 49-50

IAPP CIPP/US Body of Knowledge, Domain II: Limits on Private-sector Collection and Use of Data, Objective II.C: Identify the privacy requirements for financial institutions, Subobjective II.C.2: Identify the restrictions on disclosure of account numbers, p. 14

IAPP CIPP/US Exam Blueprint, Domain II: Limits on Private-sector Collection and Use of Data, Objective II.C: Identify the privacy requirements for financial institutions, Subobjective II.C.2: Identify the restrictions on disclosure of account numbers, p. 5

Question: 126

In what way is the Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act intended to help consumers?

A. By providing consumers with free spam-filtering software.
B. By requiring a company to receive an opt-in before sending any advertising e-mails.
C. By prohibiting companies from sending objectionable content through unsolicited e-mails.
D. By requiring companies to allow consumers to opt-out of future e-mails.

Answer: D

Explanation:

The Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act is a law passed in 2003 that establishes the first national standards for the sending of commercial e-mail in the United States. The law requires the Federal Trade Commission (FTC) to enforce its provisions. The

law applies to any commercial e-mail message, which is defined as any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service. The law does not apply to transactional or relationship messages, which are messages that facilitate an agreed-upon transaction or update a customer about an existing business

relationship. The law also does not apply to non-commercial messages, such as political or charitable solicitations12

The CAN-SPAM Act is intended to help consumers by giving them more control over the commercial e-mails they receive. The law does not require companies to obtain prior consent (opt-in) from consumers before sending them commercial e-mails, but it does require companies to honor consumers' requests to stop

receiving such e-mails (opt-out). The law specifies that each commercial e-mail message must include a clear and conspicuous notice of the opportunity to decline to receive further messages from the sender, and a valid physical postal address of the sender. The sender must provide a functioning return e-mail address or other Internet-based mechanism that allows the recipient to submit an opt-out request. The sender must honor the opt-out request within 10 business days and must not sell, exchange, or transfer the e-mail address of the opt-out requester to another entity, unless the other entity is acting as an agent of the sender12

By requiring companies to allow consumers to opt-out of future e-mails, the CAN-SPAM Act aims to reduce the amount of unwanted and unsolicited commercial e-mail that consumers receive, and to protect their privacy and preferences. The law also imposes other requirements on companies that send commercial e-mails, such as banning false or misleading header information and deceptive subject lines, requiring the identification of the message as an advertisement, and requiring the labeling of sexually explicit content. The law also authorizes the FTC and other federal agencies to enforce the law and impose civil penalties for violations12

Reference:

Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act) IAPP CIPP/US Certified Information Privacy Professional Study Guide, Chapter 4: Federal Privacy Laws, Section 4.4: The CAN-SPAM Act

Question: 127

SCENARIO

Please use the following to answer the next QUESTION

Otto is preparing a report to his Board of Directors at Filtration Station, where he is responsible for the privacy program. Filtration Station is a U.S. company that sells filters and tubing products to pharmaceutical companies for research use. The company is based in Seattle, Washington, with offices throughout the U.S. and Asi

a. It sells to business customers across both the U.S. and the Asia-Pacific region. Filtration Station participates in the Cross-Border Privacy Rules system of the APEC Privacy Framework.

Unfortunately, Filtration Station suffered a data breach in the previous quarter. An unknown third party was able

to gain access to Filtration Station's network and was able to steal data relating to employees in the company's Human Resources database, which is hosted by a third-party cloud provider based in the U.S. The HR data is encrypted. Filtration Station also uses the third-party cloud provider to host its business marketing contact database. The marketing database was not affected by the data breach. It appears that the data breach was caused when a system administrator at the cloud provider stored

the encryption keys with the data itself.

The Board has asked Otto to provide information about the data breach and how updates on new developments in privacy laws and regulations apply to Filtration Station. They are particularly concerned about staying up to date on the various U.S. state laws and regulations that have been in the news, especially the California Consumer Privacy Act (CCPA) and breach notification requirements.

The Board has asked Otto whether the company will need to comply with the new California Consumer Privacy Law (CCPA). What should Otto tell the Board?

A. That CCPA will apply to the company only after the California Attorney General determines that it will enforce the statute.

B. That the company is governed by CCPA, but does not need to take any additional steps because it follows CPBR.

C. That business contact information could be considered personal information governed by CCPA. D. That CCPA only applies to companies based in California, which exempts the company from compliance.

Answer: C

Explanation:

The CCPA applies to any business that collects personal information of California residents, regardless of where the business is located1. The CCPA defines personal information broadly as any information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household2. This could include business contact information, such as name, email address, phone number, or job title, if it is linked to a specific individual3. Therefore, Otto should tell the Board that business contact information could be considered personal information governed by CCPA, and that the company may need to comply with the CCPA requirements, such as providing notice, honoring consumer rights requests, and implementing reasonable security measures4. Reference:
CIPP/US Practice Questions (Sample Questions), Question 124, Answer C, Explanation C.
IAPP CIPP/US Certified Information Privacy Professional Study Guide, Chapter 6, Section 6.2, p. 181182.
California Consumer Privacy Act (CCPA), Section 1798.140, Subsection (o).
CCPA Compliance Checklist for Businesses, Section 2, Subsection (a).

Question: 128

SCENARIO
Please use the following to answer the next QUESTION

Otto is preparing a report to his Board of Directors at Filtration Station, where he is responsible for the privacy program. Filtration Station is a U.S. company that sells filters and tubing products to pharmaceutical companies for research use. The company is based in Seattle, Washington, with offices throughout the U.S. and Asi
a. It sells to business customers across both the U.S. and the Asia-Pacific region. Filtration Station

participates in the Cross-Border Privacy Rules system of the APEC Privacy Framework.

Unfortunately, Filtration Station suffered a data breach in the previous quarter. An unknown third party was able to gain access to Filtration Station's network and was able to steal data relating to employees in the company's Human Resources database, which is hosted by a third-party cloud provider based in the U.S. The HR data is encrypted. Filtration Station also uses the third-party cloud provider to host its business marketing contact database. The marketing database was not affected by the data breach. It appears that the data breach was caused when a system administrator at the cloud provider stored the encryption keys with the data itself.

The Board has asked Otto to provide information about the data breach and how updates on new developments in privacy laws and regulations apply to Filtration Station. They are particularly concerned about staying up to date on the various U.S. state laws and regulations that have been in the news, especially the

California Consumer Privacy Act (CCPA) and breach notification requirements.

What can Otto do to most effectively minimize the privacy risks involved in using a cloud provider for the HR data?

A. Request that the Board sign off in a written document on the choice of cloud provider.

B. Ensure that the cloud provider abides by the contractual requirements by conducting an on-site audit.

C. Obtain express consent from employees for storing the HR data in the cloud and keep a record of the employee consents.

D. Negotiate a Business Associate Agreement with the cloud provider to protect any health-related data employees might share with Filtration Station.

Answer: B

Explanation:

The best way for Otto to minimize the privacy risks involved in using a cloud provider for the HR data is to ensure that the cloud provider abides by the contractual requirements by conducting an on-site audit. This would allow Otto to verify that the cloud provider has implemented adequate security measures, such as encryption, access controls, and backup systems, to protect the HR data from unauthorized access, use, or disclosure. It would also allow Otto to check that the cloud provider is complying with the applicable privacy laws and regulations, such as the CCPA, the APEC Privacy Framework, and the breach notification requirements. By conducting an on-site audit, Otto can identify any gaps or weaknesses in the cloud provider's privacy practices and address them promptly. This would also demonstrate due diligence and accountability on the part of Filtration Station, which could mitigate the legal and reputational consequences of a data breach.
Reference: [IAPP CIPP/US Study Guide], Chapter 3: Data Assessments, pp. 77-78.
IAPP CIPP/US Body of Knowledge, Section III: Government and Court Access to Private-sector Information, Subsection B: Cross-Border Data Transfer, Topic 2: APEC Privacy Framework.
IAPP CIPP/US Practice Questions, Question 125.

Question: 129

Which of the following statements is most accurate in regard to data breach notifications under federal and state laws:

A. You must notify the Federal Trade Commission (FTC) in addition to affected individuals if over 500 individuals are receiving notice.

B. When providing an individual with required notice of a data breach, you must identify what personal information was actually or likely compromised.

C. When you are required to provide an individual with notice of a data breach under any state's law, you must provide the individual with an offer for free credit monitoring.

D. The only obligations to provide data breach notification are under state law because currently there is no federal law or regulation requiring notice for the breach of personal information.

Answer: D

Explanation:

Data breach notification laws in the United States vary by state and territory, and there is no comprehensive federal law that applies to all types of personal information. Some federal laws, such as HIPAA, GLBA, and the FDIC rule, impose data breach notification requirements for specific industries or sectors, but they do not cover all types of personal information or all entities that collect, store, or process such information. Therefore, the only obligations to provide data breach notification for the breach of personal information are under state law, unless a specific federal law applies to the entity or the information involved. The other statements are incorrect because: A . You do not have to notify the FTC in addition to affected individuals if over 500 individuals are receiving notice, unless you are a health care entity subject to HIPAA, in which case you have to notify the Department of Health and Human Services (HHS) within 60 days of the breach.

B . When providing an individual with required notice of a data breach, you do not have to identify what personal information was actually or likely compromised, unless the state law requires you to do so. Some states, such as California, require the notice to include the types of personal information that were or are reasonably believed to have been the subject of the breach, while others, such as Alabama, do not specify the content of the notice.

C . When you are required to provide an individual with notice of a data breach under any state's law, you do not have to provide the individual with an offer for free credit monitoring, unless the state law requires you to do so. Some states, such as Connecticut, require the offer of appropriate identity theft prevention and mitigation services for at least 12 months, while others, such as Arizona, do not impose such a requirement.

Reference: Data Breach Notification in the United States and Territories, Data Breach Notification Laws in the United States: What is Required and How is that Determined?, US State Data Breach Notification Law Matrix, Breach Notification in United States, Data Breach Notification Laws: How to Manufacture a Confident Response

Question: 130

What consumer service was the Fair Credit Reporting Act (FCRA) originally intended to provide?

A. The ability to receive reports from multiple credit reporting agencies.
B. The ability to appeal negative credit-based decisions.
C. The ability to correct inaccurate credit information.
D. The ability to investigate incidents of identity theft.

Answer: C

Explanation:

The Fair Credit Reporting Act (FCRA) was originally intended to provide consumers with the ability to correct inaccurate credit information that could affect their access to credit, employment, insurance, and other benefits. The FCRA gives consumers the right to access their credit reports from the three major credit reporting agencies (Equifax, Experian, and TransUnion) for free once every 12 months, and to dispute any errors or inaccuracies with the credit reporting agencies or the information furnishers (such as lenders, creditors, or debt collectors). The FCRA also requires the credit reporting agencies and the information furnishers to investigate and resolve the disputes within 30 days, and to delete or correct any information that is found to be inaccurate, incomplete, or outdated. The FCRA also provides consumers with the right to place

fraud alerts or security freezes on their credit reports if they are victims or potential victims of identity theft, and to receive notifications from users of their credit reports (such as employers or insurers) if any adverse action is taken based on their credit information. Reference:

Fair Credit Reporting Act - Wikipedia

What is the Fair Credit Reporting Act (FCRA)? | Money

The Fair Credit Reporting Act of 1970 - The Balance

How the Fair Credit Reporting Act (FCRA) Protects Consumer Rights

Question: 131

Privacy Is Hiring Inc., a CA-based company, is an online specialty recruiting firm focusing on placing privacy professionals in roles at major companies. Job candidates create online profiles outlining their experience and credentials, and can pay $19.99/month via credit card to have their profiles promoted to potential employers. Privacy Is Hiring Inc. keeps all customer data at rest encrypted on its servers.

Under what circumstances would Privacy Is Hiring Inc., need to notify affected individuals in the event of a data breach?

A. If law enforcement has completed its investigation and has authorized Privacy Is Hiring Inc. to provide the notification to clients and applicable regulators.

B. If the job candidates' credit card information and the encryption keys were among the information taken.

C. If Privacy Is Hiring Inc., reasonably believes that job candidates will be harmed by the data breach. D. If the personal information stolen included the individuals' names and credit card pin numbers.

Answer: B

Explanation:

Under the California Consumer Privacy Act (CCPA), a business that collects personal information of California residents must notify them of a data breach if their personal information is subject to unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices. However, the CCPA excludes encrypted or redacted personal information from the definition of personal information, unless the encryption key or security credential is also compromised. Therefore, Privacy Is Hiring Inc. would need to notify the affected individuals only if the encryption keys were also taken along with the credit card information, as this would render the encryption ineffective and expose the personal information to unauthorized access. The other options are not relevant to the CCPA notification requirement, although they may be relevant to other laws or best practices. Reference: CCPA (Section 1798.150), IAPP CIPP/US Study Guide (p. 63-64)

Question: 132

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.

Consumers today are most likely protected from situations like the one Noah had buying stock because of which federal action or legislation?

A. The rules under the Fair Debt Collection Practices Act.
B. The creation of the Consumer Financial Protection Bureau.
C. Federal Trade Commission investigations into "unfair and deceptive" acts or practices.
D. Investigations of "abusive" acts and practices under the Dodd-Frank Wall Street Reform and Consumer Protection Act.

Answer: D

Explanation:

The Dodd-Frank Act was established to prevent the risky financial practices that led to the 2007–2008 financial crisis, which included issues similar to Noah's experience with buying stocks without understanding the risks. The act includes provisions for consumer protection in financial services and aims to prevent abusive

practices in the financial industry

Question: 133

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 Privacy Rule under the Gramm-Leach-Bliley Act (GLBA).
B. The Safeguards 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). 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: 134

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

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: 135

Which of the following is NOT one of three broad categories of products offered by data brokers, as identified by the U.S. Federal Trade Commission (FTC)?

A. Research (such as information for understanding consumer trends).
B. Risk mitigation (such as information that may reduce the risk of fraud).
C. Location of individuals (such as identifying an individual from partial information).
D. Marketing (such as appending data to customer information that a marketing company already has).

Answer: C

Explanation:
Data brokers are companies that collect, analyze, and share personal information about consumers for various purposes, such as marketing, risk mitigation, and research. The U.S. Federal Trade Commission (FTC) conducted a study of nine data brokers in 2012 and published a report in 2014, titled “Data Brokers: A Call for Transparency and Accountability”. In the report, the FTC identified three broad categories of products offered by data brokers, based on the primary purposes for which the products are used by their customers. The three categories are: 12
Marketing products: These products help customers target potential customers, tailor marketing offers, measure the effectiveness of marketing campaigns, and improve customer relationships. Marketing products include data elements, segments, scores, lists, and analytics that are derived from consumer data. Data brokers may provide marketing products through direct marketing (such as postal mail, e-mail, or phone), online marketing (such as online display ads, social media, or mobile apps), or marketing analytics (such as measuring consumer behavior, preferences, and trends)12
Risk mitigation products: These products help customers verify and authenticate consumers’ identities, prevent fraud, and comply with legal obligations. Risk mitigation products include identity verification, identity authentication, fraud prevention, and compliance products that are based on consumer data. Data brokers may provide risk mitigation products through various methods, such as matching consumer-provided information with data broker records, generating questions or challenges based on consumer data, or providing scores or indicators of fraud risk or compliance status12
Research products: These products help customers understand consumer behavior, preferences, and trends, as well as market conditions, industry developments, and economic factors. Research products include reports, studies, statistics, and insights that are derived from consumer data. Data brokers may provide research

products through various formats, such as online portals, dashboards, newsletters, or custom reports12

The FTC report did not include location of individuals as one of the three broad categories of products offered by data brokers. Location of individuals may be a specific type of product or service that some data brokers provide, but it is not a primary purpose for which data brokers use consumer data. Therefore, the correct answer is C. Location of individuals (such as identifying an individual from partial information).

Reference:

Data Brokers: A Call For Transparency and Accountability: A Report of the Federal Trade Commission (May 2014)

IAPP CIPP/US Certified Information Privacy Professional Study Guide, Chapter 5: State Privacy Laws, Section 5.3: Data Broker Laws

Question: 136

What information did the Red Flag Program Clarification Act of 2010 add to the original Red Flags rule?

A. The most common methods of identity theft.
B. The definition of what constitutes a creditor.
C. The process for proper disposal of sensitive data.
D. The components of an identity theft detection program.

Answer: B

Explanation:

The Red Flag Program Clarification Act of 2010 amended the original Red Flags rule, which required certain financial institutions and creditors to develop and implement a written identity theft prevention program. The Clarification Act narrowed the definition of creditor to include only those who regularly and in the ordinary course of business advance funds to or on behalf of a person, based on an obligation of the person to repay the funds or repayable from specific property pledged by or on behalf of the person12. This excludes creditors who advance funds for expenses incidental to a service provided by the creditor to that person3.

Reference:

CIPP/US Practice Questions (Sample Questions), Question 133, Answer B, Explanation B.

IAPP CIPP/US Certified Information Privacy Professional Study Guide, Chapter 4, Section 4.3, p. 108109.

Red Flag Program Clarification Act of 2010, Section 2, Subsection (b).

Question: 137

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 risk of sexual harassment.

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

Answer: C

Explanation:

The strongest example of excessive monitoring by the employer is C. An employer who installs video monitors in physical locations, such as a changing room, to reduce the risk of sexual harassment. This would be considered an unreasonable invasion of employees' privacy, as it would violate their legitimate expectation of privacy in a place where they change their clothes. Such monitoring would also likely violate the Electronic Communications Privacy Act (ECPA), which prohibits the interception of oral communications without consent or authorization. Moreover, such monitoring would not be justified by a legitimate business interest, as there are less intrusive ways to prevent or address sexual harassment, such as policies, training, and reporting mechanisms. Reference: [IAPP CIPP/US Study Guide], Chapter 4: Workplace Privacy, pp. 109-110.
IAPP CIPP/US Body of Knowledge, Section IV: Workplace Privacy, Subsection A: Employee Privacy Expectations, Topic 1: Employee Monitoring.
IAPP CIPP/US Practice Questions, Question 134.

Question: 138

Which of the following became the first state to pass a law specifically regulating the collection of biometric data?

A. California.
B. Texas.
C. Illinois.
D. Washington.

Answer: C

Explanation:
Illinois became the first state to pass a law specifically regulating the collection of biometric data in 2008, when it enacted the Biometric Information Privacy Act (BIPA). BIPA defines biometric identifiers as retina or iris scans, fingerprints, voiceprints, or scans of hand or face geometry, and biometric information as any information based on biometric identifiers used to identify an individual. BIPA requires entities that collect, store, or use biometric identifiers or information to obtain informed consent from individuals, provide written policies on data retention and destruction, limit disclosure and sale of biometric data, and protect biometric data using reasonable security measures. BIPA also provides a private right of action for individuals whose biometric data is collected, stored, or used in violation of the law, and allows them to recover statutory damages of $1,000 or actual damages, whichever is greater, for each negligent violation, and $5,000 or actual damages, whichever is greater, for each intentional or reckless violation, as well as attorneys' fees and costs, and injunctive relief. Reference: U.S. Biometrics Laws Part I: An Overview of 2020, Is Biometric Information Protected by Privacy Laws?, Biometric Data Privacy Laws

Question: 139

SCENARIO
Please use the following to answer the next QUESTION

Felicia has spent much of her adult life overseas, and has just recently returned to the U.S. to help her friend Celeste open a jewelry store in Californi
E. Felicia, despite being excited at the prospect, has a number of security concerns, and has only grudgingly accepted the need to hire other employees. In order to guard against the loss of valuable merchandise, Felicia wants to carefully screen applicants. With their permission, Felicia would like to run credit checks, administer polygraph tests, and scrutinize videos of interviews. She intends to read applicants' postings on social media, ask QUESTION NO:s about drug addiction, and solicit character references. Felicia believes that if potential employees are serious about becoming part of a dynamic new business, they will readily agree to these requirements.

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.

Regarding credit checks of potential employees, Celeste has a misconception regarding what?

A. Consent requirements.
B. Disclosure requirements.
C. Employment-at-will rules.
D. Records retention policies

Answer: A

Celeste has a misconception regarding the consent requirements for conducting credit checks of potential employees in California. She thinks that verbal consent from the applicants is sufficient, and that they only need to be offered access to the results. However, under the California Consumer Credit Reporting Agencies Act (CCRAA), employers who want to obtain a consumer credit report for employment purposes must comply with the following consent and disclosure requirements12:

Before requesting a consumer credit report, the employer must provide the applicant with a clear and conspicuous written disclosure that informs them of the following:

The specific purpose for obtaining the report.

The source of the report.

The applicant's right to obtain a free copy of the report from the source within 60 days.

The applicant's right to dispute the accuracy or completeness of any information in the report.

The employer must also obtain the applicant's written authorization to obtain the report.

If the employer intends to take an adverse action based on the report, such as denying employment, the employer must provide the applicant with a copy of the report and a summary of their rights under the CCRAA before taking the action.

After taking the adverse action, the employer must provide the applicant with a notice that includes the following:

The name, address, and telephone number of the source of the report.

A statement that the source of the report did not make the decision and cannot explain why the decision was made.

A statement that the applicant has the right to obtain another free copy of the report from the source within 60 days.

A statement that the applicant has the right to dispute the accuracy or completeness of any information in the report.

Therefore, Celeste is wrong to assume that verbal consent and optional access to the results are enough to comply with the CCRAA. She should follow the written consent and disclosure requirements to avoid violating the law and potentially facing civil penalties or lawsuits. References: California Consumer Credit Reporting Agencies Act

Employment Credit Checks: What You Need to Know | Nolo

Question: 140

One of the most significant elements of Senate Bill No. 260 relating to Internet privacy is the introduction of what term into Nevada law?

A. Data Ethics
B. Data Brokers
C. Artificial Intelligence.
D. Transfer Mechanism

Answer: B

Explanation:

One of the most significant changes introduced by Nevada Senate Bill 260 (SB 260) is the inclusion of the term "Data Brokers" into Nevada privacy law. The bill requires data brokers to register with the Nevada Secretary of State and comply with new privacy requirements, such as responding to consumer opt-out requests. This addition aligns Nevada's privacy framework more closely with laws like Vermont's data broker law.

Key Provisions of SB 260:

Definition of Data Brokers:

A data broker is defined as a company that collects, sells, or licenses consumer data and does not have a direct relationship with the consumer.

Registration Requirements:

Data brokers must register annually with the Nevada Secretary of State.

Consumer Rights:

Consumers are granted the right to opt out of the sale of their personal information, extending the scope of Nevada's existing privacy law.

Explanation of Options:

A . Data Ethics:

While data ethics is an important concept, it is not introduced as a specific term under SB 260.

B . Data Brokers:

This is correct. The inclusion of data brokers as a regulated entity is the primary addition introduced by SB 260.

C . Artificial Intelligence:

SB 260 does not address artificial intelligence directly.

D . Transfer Mechanism:

SB 260 focuses on regulating data brokers, not cross-border data transfer mechanisms.

Reference from CIPP/US Materials:

Nevada Senate Bill 260 (SB 260): Introduces data broker registration and opt-out rights.

IAPP CIPP/US Certification Textbook: Discusses state-specific privacy laws, including Nevada's privacy framework.

Question: 141

SCENARIO

Please use the following to answer the next QUESTION

Felicia has spent much of her adult life overseas, and has just recently returned to the U.S. to help her friend Celeste open a jewelry store in Californi

a. Felicia, despite being excited at the prospect, has a number of security concerns, and has only grudgingly accepted the need to hire other employees. In order to guard against the loss of valuable merchandise, Felicia wants to carefully screen applicants. With their permission, Felicia would like to run credit checks, administer polygraph tests, and scrutinize videos of interviews. She intends to read applicants' postings on social media, ask QUESTION NO:s about drug addiction, and solicit character references. Felicia believes that if potential employees are serious about becoming part of a dynamic new business, they will readily agree to these requirements.

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. The Americans with Disabilities Act (ADA).
B. The Occupational Safety and Health Act (OSHA).
C. The Genetic Information Nondiscrimination Act of 2008.
D. The Health Insurance Portability and Accountability Act (HIPAA).

Answer: A

The ADA prohibits employers from discriminating against qualified individuals with disabilities in all aspects of employment, including hiring, firing, promotion, compensation, and training. The ADA also limits the types of medical inquiries and examinations that employers can make of applicants and employees. Under the ADA, a disability is defined as a physical or mental impairment that substantially limits one or more major life activities, a record of such an impairment, or being regarded as having such an impairment. The ADA covers current, past, and perceived drug addiction as a disability, unless the individual is currently engaging in the illegal use of drugs. Therefore, Felicia's plan to ask applicants about drug addiction may violate the ADA, unless she can show that the inquiry is job-related and consistent with business necessity. The other laws are not directly relevant to Felicia's plan, although they may have other implications for her business.
References: ADA, IAPP CIPP/US Study Guide (p. 95-96)

Question: 142

Your company, an online store selling digital keys to video games, has received a data access request from an individual. Specifically, the individual wants access to her recent purchase history, as she has misplaced the emails containing the digital keys to multiple game purchases she made last month. From a security standpoint, what would the user have to do under CCPA in order to acceptably verify her identity?

A. Take a photo of herself with her driver license
B. Provide a notarized affidavit signed by two witnesses.
C. Log in to her password-protected account with the company
D. Phone the company and provide her contact details and credit card number

Answer: C

Explanation:

Under the California Consumer Privacy Act (CCPA), businesses must verify the identity of individuals making data access requests to ensure the security of personal information. The most secure and straightforward way to verify a consumer's identity is by requiring the individual to log in to their password-protected account, as this demonstrates that the requester is the account owner.

Why Password-Protected Accounts Are Best for Verification:

Account-Based Relationship:

If the consumer has a password-protected account with the business, verification can typically be achieved by having the consumer log in to the account. This is considered a sufficient method of verifying identity under CCPA guidelines.

Minimizing Risk:

Verifying identity through account login reduces the risk of fraudulent access to personal information, as only the account owner has access to the login credentials.

Explanation of Options:

A. Take a photo of herself with her driver license:

While this might verify identity, it is more intrusive and poses unnecessary risks of identity theft. This is not a preferred or common method under the CCPA.

B. Provide a notarized affidavit signed by two witnesses:

This is excessive and impractical for verifying identity in most cases, particularly for an online store.

C. Log in to her password-protected account with the company:

This is correct. Logging into a password-protected account is a straightforward and secure way to verify the identity of a requester under the CCPA.

D. Phone the company and provide her contact details and credit card number:

This method is insecure, as it could lead to identity theft or fraudulent access if someone else provides this information.

Reference from CIPP/US Materials:

CCPA Regulations (11 CCR § 999.323): Specifies identity verification requirements, including the use of password-protected accounts.

IAPP CIPP/US Certification Textbook: Covers secure methods for verifying consumer identity under the CCPA.

Question: 143

Which of the following would NOT be regulated by the Illinois Biometnc Information Pnvacy Act (BIPA)?

A. Photographs of local convicted felons uploaded lo a news website.

B. Fingerprint scans of elementary school students used to open their lockers

C. Security software designed to identify local convicted felons in retail stores via facial recognition.

D. Retina scans of elementary school students used to verify their identities for attendance purposes

Answer: A

Explanation:

The Illinois Biometric Information Privacy Act (BIPA) regulates the collection, storage, and use of biometric identifiers and biometric information, such as fingerprints, retina scans, and facial recognition data. However,

BIPA does not regulate photographs, as they are explicitly excluded from the definition of "biometric identifiers" under the law.

Key Definitions Under BIPA:

Biometric Identifier:

Includes fingerprints, retina or iris scans, voiceprints, and scans of hand or face geometry.

Biometric Information:

Refers to any information derived from biometric identifiers.

Exclusions:

BIPA explicitly excludes certain types of data from regulation, such as photographs, writing samples, and physical descriptions.

Explanation of Options:

A. Photographs of local convicted felons uploaded to a news website:

This is correct because photographs are explicitly excluded from BIPA's definition of biometric identifiers.

B. Fingerprint scans of elementary school students used to open their lockers:

This would be regulated under BIPA, as fingerprints are considered biometric identifiers.

C. Security software designed to identify local convicted felons in retail stores via facial recognition: This would also be regulated under BIPA, as facial recognition involves scans of face geometry, which qualify as biometric identifiers.

D. Retina scans of elementary school students used to verify their identities for attendance purposes: Retina scans are biometric identifiers under BIPA and would therefore be regulated.

Reference from CIPP/US Materials:

Illinois BIPA (740 ILCS 14/10): Defines biometric identifiers and excludes photographs from regulation.

IAPP CIPP/US Certification Textbook: Discusses the scope and application of BIPA.

Question: 144

SCENARIO

Please use the following to answer the next QUESTION

Felicia has spent much of her adult life overseas, and has just recently returned to the U.S. to help her friend Celeste open a jewelry store in Californi

a. Felicia, despite being excited at the prospect, has a number of security concerns, and has only grudgingly accepted the need to hire other employees. In order to guard against the loss of valuable merchandise, Felicia wants to carefully screen applicants. With their permission, Felicia would like to run credit checks, administer polygraph tests, and scrutinize videos of interviews. She intends to read applicants' postings on social media, ask QUESTION NO:s about drug addiction, and solicit character references. Felicia believes that if potential employees are serious about becoming part of a dynamic new business, they will readily agree to these requirements.

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.

Based on Felicia's Bring Your Own Device (BYOD) plan, the business consultant will most likely advise Felicia and Celeste to do what?

A. Reconsider the plan in favor of a policy of dedicated work devices.
B. Adopt the same kind of monitoring policies used for work-issued devices.
C. Weigh any productivity benefits of the plan against the risk of privacy issues.
D. Make employment decisions based on those willing to consent to the plan in writing.

Answer: C

BYOD is a practice that allows employees to use their own personal devices, such as smartphones, tablets, or laptops, for work-related purposes. BYOD can offer some benefits for both employers and employees, such as increased flexibility, convenience, and productivity. However, BYOD also poses significant privacy and security risks, such as data breaches, unauthorized access, loss or theft of devices, malware infections, and compliance challenges. Therefore, the business consultant will most likely advise Felicia and Celeste to weigh any productivity benefits of the plan against the risk of privacy issues, and to implement a comprehensive BYOD policy that addresses the following aspects: The scope and purpose of the BYOD program, including the types of devices, data, and applications that are allowed or prohibited.

The roles and responsibilities of the employer and the employees, including the ownership, control, and access rights of the devices and the data.

The security measures and controls that are required to protect the devices and the data, such as encryption, passwords, remote wipe, antivirus software, firewalls, and VPNs.

The privacy expectations and obligations of the employer and the employees, such as the notice, consent, and disclosure requirements, the limits on data collection and monitoring, the retention and deletion policies, and the rights of access and correction.

The legal and regulatory compliance requirements that apply to the BYOD program, such as the FTC Act, the GLBA, the HIPAA, the COPPA, the CCPA, and the GDPR.

The incident response and reporting procedures that are followed in the event of a data breach, loss, or theft of a device, or any other privacy or security issue.

The training and education programs that are provided to the employees to raise awareness and understanding of the BYOD policy and the best practices.

The enforcement and audit mechanisms that are used to ensure compliance and accountability of the BYOD policy, such as sanctions, penalties, reviews, and audits. References: IAPP CIPP/US Body of Knowledge, Section III.C.2

IAPP CIPP/US Textbook, Chapter 3, pp. 113-115

FTC Mobile Device Security

Question: 145

What privacy concept grants a consumer the right to view and correct errors on his or her credit report?

A. Access.
B. Notice.
C. Action.
D. Choice.

Answer: A

Explanation:
Access is the privacy concept that grants a consumer the right to view and correct errors on his or her credit report. The Fair Credit Reporting Act (FCRA) gives consumers the right to access their credit reports from the three nationwide credit reporting agencies (Equifax, Experian, and TransUnion) once every 12 months for free. Consumers also have the right to dispute any inaccurate or incomplete information in their credit reports and request that the credit reporting agencies investigate and correct the errors. The FCRA also requires the credit reporting agencies to provide consumers with a notice of their rights and a summary of the dispute process.
Reference: IAPP CIPP/US Certified Information Privacy Professional Study Guide, Chapter 2: Limits on Private-sector Collection and Use of Data, Section 2.2: Consumer Privacy, p. 38-39
IAPP CIPP/US Body of Knowledge, Domain II: Limits on Private-sector Collection and Use of Data, Objective II.B: Identify the privacy requirements for consumer data, Subobjective II.B.1: Identify the consumer rights under the Fair Credit Reporting Act, p. 13
IAPP CIPP/US Exam Blueprint, Domain II: Limits on Private-sector Collection and Use of Data, Objective II.B: Identify the privacy requirements for consumer data, Subobjective II.B.1: Identify the consumer rights under the Fair Credit Reporting Act, p. 4

Question: 146

A company's employee wellness portal offers an app to track exercise activity via users' mobile devices. Which of the following design techniques would most effectively inform users of their data privacy rights and privileges when using the app?

A. Offer information about data collection and uses at key data entry points.
B. Publish a privacy policy written in clear, concise, and understandable language.
C. Present a privacy policy to users during the wellness program registration process.
D. Provide a link to the wellness program privacy policy at the bottom of each screen.

Answer: A

Explanation:
The design technique that would most effectively inform users of their data privacy rights and privileges when

using the app is to offer information about data collection and uses at key data entry points. This technique is also known as "just-in-time" or "layered" notice, and it is recommended by the U.S. Federal Trade Commission (FTC) as a best practice for mobile app developers12 The idea behind this technique is to provide users with relevant and timely information about how their data is collected and used by the app, and what choices they have to control their data, at the moment when they are asked to provide or access their data. For example, if the app collects location data from the user's device, it should display a pop-up notice explaining why it needs the location data, how it will use it, and how the user can opt-out or change the settings. This way, the user can make an informed decision about whether to allow or deny the app's access to their data, and understand the consequences of their choice12

The advantage of this technique is that it avoids overwhelming the user with too much information at once, and instead provides concise and contextual information that is easy to understand and act upon. It also increases the user's trust and confidence in the app, as they feel more in control of their data and privacy12

The other design techniques are less effective because they do not provide the user with sufficient or timely information about their data privacy rights and privileges when using the app. Publishing a privacy policy written in clear, concise, and understandable language is a good practice, but it is not enough to inform the user of their data privacy rights and privileges, as many users may not read or understand the policy, or may not be aware of where to find it. Presenting a privacy policy to users during the wellness program registration process is also a good practice, but it may not capture all the data collection and uses that the app may perform, and it may not give the user enough opportunity to review and consent to the policy. Providing a link to the wellness program privacy policy at the bottom of each screen is also a good practice, but it may not be noticeable or accessible to the user, and it may not provide the user with the specific information they need at the point of data entry or access12 Reference:

Mobile Privacy Disclosures: Building Trust Through Transparency: A Federal Trade Commission Staff Report (February 2013)

IAPP CIPP/US Certified Information Privacy Professional Study Guide, Chapter 6: Privacy Program Management, Section 6.4: Privacy by Design

Question: 147

Under the Fair Credit Reporting Act (FCRA), what must a person who is denied employment based upon his credit history receive?

A. A prompt notification from the employer.
B. An opportunity to reapply with the employer.
C. Information from several consumer reporting agencies (CRAs).
D. A list of rights from the Consumer Financial Protection Bureau (CFPB).

Answer: A

Explanation:

The FCRA requires that an employer who takes an adverse action against an applicant or employee based on information in a consumer report must provide a notice of the adverse action to the individual. The notice must include the name, address, and phone number of the CRA that supplied the report; a statement that the CRA did not make the decision and cannot explain why the adverse action was taken; a notice of the individual's right to dispute the accuracy or completeness of the information in the report; and a notice of the individual's right to obtain a free copy of the report from the CRA within 60 days12. Reference:

CIPP/US Practice Questions (Sample Questions), Question 141, Answer A, Explanation A.

IAPP CIPP/US Certified Information Privacy Professional Study Guide, Chapter 4, Section 4.2, p. 101102.
Fair Credit Reporting Act (FCRA), Section 615, Subsection (a).

Question: 148

Which statement is FALSE regarding the provisions of the Employee Polygraph Protection Act of 1988 (EPPA)?

A. The EPPA requires that employers post essential information about the Act in a conspicuous location.
B. The EPPA includes an exception that allows polygraph tests in professions in which employee honesty is necessary for public safety.
C. Employers are prohibited from administering psychological testing based on personality traits such as honesty, preferences or habits.
D. Employers involved in the manufacture of controlled substances may terminate employees based on polygraph results if other evidence exists.

Answer: C

Explanation:
The false statement regarding the provisions of the EPPA is C. Employers are prohibited from administering psychological testing based on personality traits such as honesty, preferences or habits. The EPPA does not regulate psychological testing, only polygraph testing. Psychological testing is a broad term that covers various types of assessments that measure cognitive abilities, personality traits, interests, values, and skills. Employers may use psychological testing for various purposes, such as hiring, promotion, training, or development, as long as they comply with other laws and regulations, such as the Americans with Disabilities Act (ADA), the Equal Employment
Opportunity Commission (EEOC) guidelines, and the Uniform Guidelines on Employee Selection Procedures. However, employers should be careful to ensure that the psychological tests they use are valid, reliable, job-related, and nondiscriminatory, and that they respect the privacy and dignity of the test takers.
Reference:
[IAPP CIPP/US Study Guide], Chapter 4: Workplace Privacy, pp. 115-116.
IAPP CIPP/US Body of Knowledge, Section IV: Workplace Privacy, Subsection A: Employee Privacy Expectations, Topic 2: Employee Polygraph Protection Act.
IAPP CIPP/US Practice Questions, Question 142.

Question: 149

U.S. federal laws protect individuals from employment discrimination based on all of the following EXCEPT?

A. Age.
B. Pregnancy.
C. Marital status.
D. Genetic information.

Answer: C

Explanation:

U.S. federal laws protect individuals from employment discrimination based on a number of protected characteristics, such as age, pregnancy, and genetic information. However, marital status is not one of them. There is no federal law that prohibits employment discrimination based on marital status, although some states and localities have enacted such laws. The other statements are incorrect because:

A . Age is a protected characteristic under the Age Discrimination in Employment Act of 1967 (ADEA), which protects people who are 40 or older from discrimination because of age1.

B . Pregnancy is a protected characteristic under the Pregnancy Discrimination Act, which amended Title VII of the Civil Rights Act of 1964 to make it illegal to discriminate against a woman because of pregnancy, childbirth, or a medical condition related to pregnancy or childbirth2.

D . Genetic information is a protected characteristic under the Genetic Information Nondiscrimination Act of 2008 (GINA), which makes it illegal to discriminate against employees or applicants because of genetic information, such as family medical history, genetic tests, or participation in genetic research2. Reference: Prohibited Employment Policies/Practices, Employment discrimination law in the United States, Civil Rights Requirements- Federal Employment Discrimination Laws

Question: 150

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.

Answer: A

Explanation:

The Fair Credit Reporting Act (FCRA) is considered part of U.S. federal privacy law because it regulates the collection, use, and disclosure of personal information by consumer reporting agencies, such as credit bureaus, background check companies, and tenant screening services. The FCRA aims to protect the privacy, accuracy, and fairness of consumer credit information, and to ensure that consumers have access to and control over their own credit reports. The FCRA also imposes obligations on users and furnishers of consumer reports, such as creditors, employers, insurers, and landlords, to obtain consent, provide notice, and correct errors when using consumer reports for various purposes. The FCRA is enforced by the Federal Trade Commission (FTC) and other federal agencies, as well as by private lawsuits and state attorneys general. The FCRA was enacted in 1970 and has been amended several times, most notably by the Fair and Accurate Credit Transactions Act of 2003 (FACTA), which added provisions on identity theft prevention, fraud alerts, free credit reports, and disposal of consumer information. Reference:

Fair Credit Reporting Act - Wikipedia

Fair Credit Reporting Act | Federal Trade Commission Fair Credit Reporting Act (FCRA) - Consumer

Information Fair Credit Reporting Act (FCRA) | Privacy Rights Clearinghouse

Question: 151

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.

Answer: C

Explanation:

In 2012, the White House released a report titled "Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy", which proposed a Consumer Privacy Bill of Rights based on the Fair Information Practice Principles (FIPPs). The report called for a comprehensive privacy framework that would apply to all commercial sectors and all personal data, regardless of the technology or business model involved. The report also urged

Congress to enact legislation to implement the framework and empower the FTC to enforce it. Similarly, the FTC released a report titled "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers", which outlined a set of best practices for businesses to protect consumer privacy and foster innovation. The report also advocated for a comprehensive privacy framework that would cover both online and ofline data, and apply to all entities that collect or use consumer data that can be reasonably linked to a specific consumer, computer, or device. The report also recommended that Congress consider enacting baseline privacy legislation and giving the FTC rulemaking authority to implement it. Therefore, both reports can be described as advocating a comprehensive approach to privacy enforcement, rather than a harmbased, self-regulatory, or notice and choice approach. Reference: White House Report, FTC Report, IAPP CIPP/US Study Guide (p. 31-32)

Question: 152

The FTC often negotiates consent decrees with companies found to be in violation of privacy principles. How does this benefit both parties involved?

A. It standardizes the amount of fines.
B. It simplifies the audit requirements.
C. It avoids potentially harmful publicity.
D. It spares the expense of going to trial.

Answer: D

Explanation:

A consent decree is a settlement agreement between the FTC and a company that has engaged in unfair or deceptive privacy practices. A consent decree typically requires the company to stop the unlawful conduct, implement remedial measures, pay a civil penalty, and submit to ongoing monitoring and reporting. A consent decree benefits both parties involved because it spares the expense of going to trial, which can be costly, time-consuming, and uncertain. A consent decree also allows the parties to negotiate the terms of the settlement, rather than having a court impose a judgment. A consent decree does not admit liability or wrongdoing by the company, but it has the force of law and can be enforced by the FTC or the courts if the company violates its terms. Reference:
IAPP CIPP/US Body of Knowledge, Section I.A.1.a
IAPP CIPP/US Textbook, Chapter 1, pp. 10-11 FTC Consent Decrees

Question: 153

When developing a company privacy program, which of the following relationships will most help a privacy professional develop useful guidance for the organization?

A. Relationships with individuals within the privacy professional community who are able to share expertise and leading practices for different industries.
B. Relationships with clients, vendors, and customers whose data will be primarily collected and used throughout the organizational program.
C. Relationships with company leaders responsible for approving, implementing, and periodically reviewing the corporate privacy program.
D. Relationships with individuals across company departments and at different levels in the organization's hierarchy.

Answer: D

Explanation:

When developing a company privacy program, a privacy professional needs to understand the business objectives, processes, and risks of the organization, as well as the legal and regulatory requirements and best practices for privacy. To achieve this, a privacy professional should establish and maintain relationships with individuals across company departments and at different levels in the organization's hierarchy, such as IT, marketing, human resources, legal, compliance, security, and senior management. These relationships will help the privacy professional to gather relevant information, identify privacy issues and gaps, communicate privacy policies and procedures, provide training and awareness, monitor compliance, and resolve conflicts. The other relationships listed are also important, but not as essential as the internal relationships for developing a company privacy program. Reference:
IAPP CIPP/US Certified Information Privacy Professional Study Guide, Chapter 5: Developing a Privacy Program, Section 5.1: Privacy Program Framework, p. 145-146
IAPP CIPP/US Body of Knowledge, Domain V: Developing a Privacy Program, Objective V.A: Identify the components of a privacy program framework, Subobjective V.A.1: Identify the roles and responsibilities of

individuals within the organization, p. 23
IAPP CIPP/US Exam Blueprint, Domain V: Developing a Privacy Program, Objective V.A: Identify the components of a privacy program framework, Subobjective V.A.1: Identify the roles and responsibilities of individuals within the organization, p. 7

Question: 154

The Family Educational Rights and Privacy Act (FERPA) requires schools to do all of the following EXCEPT?

A. Verify the identity of students who make requests for access to their records.
B. Provide students with access to their records within a specified amount of time.
C. Respond to all reasonable student requests regarding explanation of their records.
D. Obtain student authorization before releasing directory information in their records.

Answer: D

Explanation:
The Family Educational Rights and Privacy Act (FERPA) is a federal law that protects the privacy of student education records and gives parents or eligible students the right to access, amend, and control the disclosure of their records. FERPA applies to all educational agencies and institutions that receive funds under any program administered by the U.S. Department of Education12 FERPA requires schools to do all of the following:
Verify the identity of students who make requests for access to their records. Schools must use reasonable methods to identify and authenticate the identity of parents, students, school officials, and any other parties to whom they disclose education records12
Provide students with access to their records within a specified amount of time. Schools must provide parents or eligible students with an opportunity to inspect and review the student's education records within 45 days of receiving a request. Schools are not required to provide copies of records unless it is impossible for parents or eligible students to review the records at the school12 Respond to all reasonable student requests regarding explanation of their records. Schools must provide parents or eligible students with an opportunity to request the amendment of the student's education records that they believe are inaccurate, misleading, or otherwise in violation of the student's privacy rights. Schools must consider the request and decide whether to amend the records within a reasonable time. If the school decides not to amend the records, it must inform the parent or eligible student of their right to a hearing on the matter12
FERPA does not require schools to do the following:
Obtain student authorization before releasing directory information in their records. Directory information is information contained in a student's education record that would not generally be considered harmful or an invasion of privacy if disclosed. Examples of directory information include the student's name, address, phone number, e-mail address, date and place of birth, major field of study, participation in sports and activities, dates of attendance, degrees and awards received, and most recent school attended. Schools may disclose directory information without consent unless the parent or eligible student has opted out of such disclosure. Schools must notify parents and eligible students of the types of information they designate as directory information and of their right to opt out of directory information disclosure12
Therefore, the correct answer is D. Obtain student authorization before releasing directory information in their records.
Reference:
Family Educational Rights and Privacy Act (FERPA)

IAPP CIPP/US Certified Information Privacy Professional Study Guide, Chapter 4: Federal Privacy Laws, Section 4.3: The Family Educational Rights and Privacy Act (FERPA)

Question: 155

Chanel Hair Studio is a busy high-end hair salon. In an effort to maximize efficiency of its operations and reduce wait times for appointments, Chanel decides to implement artificial intelligence software that will use client profiles and history to predict which clients will likely be late for their appointments. Information used to create the client profile included appointment history, distance from the salon, and any references to being tardy pulled from the client's social media accounts. If a client is predicted to be late, their appointment will be cancelled within 5 minutes.

Based on the details, what is the biggest potential privacy concern related to Chanel's use of this new software?

A. Scanning a client's social media accounts to use in a client profile without notice to the client.

B. Calculating client profile address distance from the salon to determine location from salon to help predict if the client will be late.

C. Using client profile information for any purpose other than setting up an appointment.

D. Assessing client tardiness history with the salon for predictive purposes.

Answer: A

Explanation:

The biggest potential privacy concern related to Chanel's use of this new software is scanning a client's social media accounts to use in a client profile without notice to the client. This could violate the client's reasonable expectation of privacy and consent, as well as the privacy policies of the social media platforms. The client may not be aware that their social media posts are being used for this purpose, and may not have given their permission or opt-in consent for such data collection and processing. This could also expose the client to potential discrimination or harm based on their social media activity, such as losing their appointment or being charged a cancellation fee. Furthermore, this practice could conflict with the Fair Information Practice Principles (FIPPs), such as transparency, purpose specification, and data minimization12.

Reference:

CIPP/US Practice Questions (Sample Questions), Question 149, Answer A, Explanation A.

IAPP CIPP/US Certified Information Privacy Professional Study Guide, Chapter 1, Section 1.1, p. 9-10.

Question: 156

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

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: 157

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

Answer: D

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 Reference: 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

Question: 158

A financial services company install "bossware" software on its employees' remote computers to monitor performance. The software logs screenshots, mouse movements, and keystrokes to determine whether an employee is being productive. The software can also enable the computer webcams to record video footage.

Which of the following would best support an employee claim for an intrusion upon seclusion tort?

A. The webcam is enabled to record video any time the computer is turned on.
B. The company creates and saves a biometric template for each employee based upon keystroke dynamics.
C. The software automatically sends a notification to a supervisor any time the employee's mouse is dormant for more than five minutes.
D. The webcam records video of an employee using a company laptop to perform personal business while at a coffee shop during work hours.

Answer: A

Explanation:
An intrusion upon seclusion tort occurs when someone intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, if the intrusion would be highly offensive to a reasonable person12. The intrusion does not need to involve a physical trespass, but can also be an electronic or optical intrusion, such as using a webcam to record a person who has a reasonable expectation of privacy2. The intrusion must also cause mental anguish or suffering to the plaintiff2.
In this case, option A would best support an employee claim for an intrusion upon seclusion tort, because the webcam is enabled to record video any time the computer is turned on, regardless of whether the employee is working or not, or whether the employee is in a private or public place. This would be an intentional and highly offensive intrusion into the employee's seclusion or private affairs, and would likely cause the employee distress or anxiety.
Option B would not support an intrusion upon seclusion tort, because the creation and saving of a biometric template based on keystroke dynamics is not an intrusion into the employee's seclusion or private affairs, but rather a data collection and processing activity that may implicate other privacy laws or principles, such as notice, consent, and security3.
Option C would not support an intrusion upon seclusion tort, because the software sending a notification to a supervisor when the employee's mouse is dormant for more than five minutes is not an intrusion into the employee's seclusion or private affairs, but rather a performance monitoring activity that may be justified by the employer's legitimate business interests4.

Option D would not support an intrusion upon seclusion tort, because the webcam recording video of an employee using a company laptop to perform personal business while at a coffee shop during work hours is not an intrusion into the employee's seclusion or private affairs, but rather a misuse of company property and time that may be subject to the employer's policies and disciplinary actions5. Moreover, the employee may not have a reasonable expectation of privacy in a public place like a coffee shop. Reference: 1: Intrusion on seclusion - Wikipedia 2: Elements of an Intrusion Claim | Digital Media Law Project 3: Biometrics - IAPP 4: Employee Monitoring - IAPP 5: Employee Privacy - IAPP : Privacy in Public Places - IAPP

Question: 159

The CFO of a pharmaceutical company is duped by a phishing email and discloses many of the company's employee personnel files to an online predator. The files include employee contact information, job applications, performance reviews, discipline records, and job descriptions.

Which of the following state laws would be an affected employee's best recourse against the employer?

A. The state social security number confidentiality statute.
B. The state personnel record review statute.
C. The state data destruction statute.
D. The state UDAP statute.

Answer: D

Explanation:
The state UDAP statute, which stands for Unfair and Deceptive Acts and Practices, is a law that protects consumers from unfair or deceptive business practices. In this case, the employer's failure to protect the employee's personal information from a phishing attack could be considered an unfair or deceptive act or practice that harmed the employee. The employee could sue the employer under the state UDAP statute for damages, injunctive relief, or other remedies. The other options are not relevant to this scenario, as they deal with different aspects of data protection, such as confidentiality, access, or destruction of personal information. Reference: [IAPP CIPP/US Study Guide], Chapter 8, Section 8.3.1, page 227 IAPP CIPP/US Practice Questions, Question 153, page 13

Question: 160

A company based in United States receives information about its UK subsidiary's employees in connection with the centralized HR service it provides.
How can the UK company ensure an adequate level of data protection that would allow the restricted data transfer to continue?

A. By signing up to an approved code of conduct under UK GDPR to demonstrate compliance with its requirements, both for the parent and the subsidiary companies.
B. By revising the contract with the United States parent company incorporating EU SCCs, as it continues to be valid for restricted transfers under the UK regime.
C. By submitting to the ICO a new application for the UK BCRs using the UK BCR application forms, as their existing authorized EU BCRs are not recognized.

D. By allowing each employee the option to opt-out to the restricted transfer, as it is necessary to send their names in order to book the sales bonuses.

Answer: B

Explanation:

The UK company can ensure an adequate level of data protection for the restricted data transfer to the US parent company by using the EU Standard Contractual Clauses (SCCs), which are contractual terms that provide safeguards for personal data transferred from the UK to third countries. The UK GDPR recognizes the validity of the EU SCCs adopted before the end of the Brexit transition period, and allows the UK Information Commissioner's Office (ICO) to issue new SCCs in the future. The other options are not correct because:

A . Signing up to an approved code of conduct under the UK GDPR is not sufficient to ensure an adequate level of data protection for restricted transfers, as it is not a transfer mechanism on its own. The UK company would still need to use another appropriate safeguard, such as SCCs or Binding Corporate Rules (BCRs), to transfer personal data to the US parent company.

C . Submitting a new application for the UK BCRs is not necessary, as the UK GDPR recognizes the existing authorized EU BCRs as valid for restricted transfers from the UK. The UK company can continue to rely on its EU BCRs, as long as they are updated to reflect the UK GDPR requirements and the role of the ICO as the competent supervisory authority.

D . Allowing each employee the option to opt-out to the restricted transfer is not a valid transfer mechanism under the UK GDPR, as it does not provide adequate safeguards for the personal data of the employees. The UK company would need to obtain the explicit consent of each employee for the restricted transfer, which must be freely given, specific, informed, and unambiguous. Reference: UK GDPR, Chapter V, Article 46
UK GDPR, Chapter V, Article 47
UK GDPR, Chapter V, Article 49
ICO guidance on international transfers
IAPP CIPP/US Study Guide, Chapter 10, Section 10.3.2

Question: 161

Which of the following state laws has an entity exemption for organizations subject to the Gramm- Leach-Bliley Act (GLBA)?

A. Nevada Privacy Law.
B. California Privacy Rights Act.
C. California Consumer Privacy Act.
D. Virginia Consumer Data Protection Act

Answer: B

Explanation:

The Virginia Consumer Data Protection Act (VCDPA) is a state law that provides comprehensive privacy rights and obligations for consumers and businesses in Virginia. The VCDPA applies to any entity that conducts business in Virginia or produces products or services that are targeted to residents of Virginia and that either: (a) controls or processes personal data of at least 100,000 consumers; or (b) controls or processes personal data of at least 25,000 consumers and derives over 50% of gross revenue from the sale of personal data.

However, the VCDPA also provides several exemptions for certain types of entities and data, including an entity exemption for financial

institutions or data subject to the Gramm-Leach-Bliley Act (GLBA). This means that organizations that are regulated by the GLBA are not subject to the VCDPA, regardless of the type or source of data they collect or process. The GLBA is a federal law that regulates the collection, use, and disclosure of personal financial information by financial institutions and their affiliates. The GLBA applies to any business that is significantly engaged in financial activities, such as banks, credit unions, securities firms, insurance companies, and certain fintech companies. The GLBA requires financial institutions to provide notice and choice to consumers about their privacy practices, to safeguard the security and confidentiality of consumer information, and to limit the sharing of consumer information with third parties. The GLBA also preempts state laws only to the extent that they are inconsistent with the GLBA, unless the state law provides greater protection to consumers.

The other state laws listed in the question do not have an entity exemption for organizations subject to the GLBA, but they may have partial or data exemptions for certain types of information that are regulated by the GLBA. For example, the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA) are state laws that provide comprehensive privacy rights and obligations for consumers and businesses in California. The CCPA and the CPRA apply to any business that collects or sells the personal information of California residents and that meets one or more of the following thresholds: (a) has annual gross revenues in excess of $25 million; (b) alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, the personal information of 50,000 or more consumers, households, or devices; or © derives 50% or more of its annual revenues from selling consumers' personal information. However, the CCPA and the CPRA also provide several exemptions for certain types of entities and data, including a data exemption for personal information collected, processed, sold, or disclosed pursuant to the GLBA, if it is in conflict with the GLBA. This means that information that is subject to the GLBA is exempt from the privacy requirements of the CCPA and the CPRA, but not from the data breach liability provisions. The CCPA and the CPRA do not exempt financial institutions or other entities that are regulated by the GLBA from their scope, unless they only collect or process information that is subject to the GLBA.

The Nevada Privacy Law is a state law that provides privacy rights and obligations for consumers and operators of websites or online services in Nevada. The Nevada Privacy Law applies to any person who owns or operates an Internet website or online service for commercial purposes that collects and maintains covered information from consumers who reside in Nevada and use or visit the Internet website or online service. Covered information includes any one or more of the following items of personally identifiable information about a consumer collected by an operator through an Internet website or online service and maintained by the operator in an accessible form: (a) a first and last name; (b) a home or other physical address which includes the name of a street and the name of a city or town; © an electronic mail address; (d) a telephone number; (e) a social security number; (f) an identifier that allows a specific person to be contacted either physically or online; or (g) any other information concerning a person collected from the person through the Internet website or online service of the operator and maintained by the operator in combination with an identifier in a form that makes the information personally identifiable. However, the Nevada Privacy Law also provides several exemptions for certain types of entities and data, including a data exemption for any data that is subject to the GLBA. This means that information that is regulated by the GLBA is exempt from the Nevada Privacy Law, regardless of the type or source of data. The Nevada Privacy Law does not exempt financial institutions or other entities that are subject to the GLBA from its scope, unless they only collect or process information that is subject to the GLBA.

Reference:

VCDPA, Section 59.1-572 (A) (1)

GLBA, 15 U.S.C. § 6801 et seq.

CCPA, Section 1798.145 (e)

CPRA, Section 1798.121 ©

Nevada Privacy Law, Section 603A.340 (1) (a)

Question: 162

When designing contact tracing apps in relation to COVID-19 or any other diagnosed virus, all of the following privacy measures should be considered EXCEPT?

A. Data retention.
B. Use limitations.
C. Opt-out choice.
D. User confidentiality.

Answer: C

Explanation:

Contact tracing apps are designed to help public health authorities track and contain the spread of COVID-19 or any other diagnosed virus by notifying users who have been in close contact with an infected person. However, these apps also raise privacy concerns, as they collect and process sensitive personal data, such as health status and location information. Therefore, contact tracing apps should follow the principles of privacy by design and default, which means that they should incorporate privacy measures into their development and operation, and offer the highest level of privacy protection to users.

Some of the privacy measures that should be considered when designing contact tracing apps are: Data retention: Contact tracing apps should only retain the personal data they collect for as long as necessary to achieve their public health purpose, and delete or anonymize the data afterwards. Data retention periods should be clearly communicated to users and based on scientific evidence and legal requirements.

Use limitations: Contact tracing apps should only use the personal data they collect for the specific and legitimate purpose of contact tracing, and not for any other purposes, such as commercial, law enforcement, or surveillance. Use limitations should be enforced by technical and organizational measures, such as encryption, access controls, and audits.

User confidentiality: Contact tracing apps should protect the confidentiality of users' personal data and identity, and not disclose them to third parties without their consent or legal authorization. User confidentiality should be ensured by technical and organizational measures, such as pseudonymization, aggregation, and data minimization.

Opt-out choice, on the other hand, is not a privacy measure that should be considered when designing contact tracing apps, as it would undermine their effectiveness and public health objective. Contact tracing apps rely on voluntary participation and widespread adoption by users to function properly and achieve their purpose. Therefore, offering users the option to opt out of the app or certain features, such as data sharing or notifications, would reduce the app's coverage and accuracy, and potentially expose users and others to greater health risks. Instead of opt-out choice, contact tracing apps should provide users with clear and transparent information about how the app works, what data it collects and how it uses it, what benefits and risks it entails, and what rights and controls users have over their data. This way, users can make an informed and voluntary decision to use the app or not, based on their own preferences and values.

Reference:

[IAPP CIPP/US Study Guide], Chapter 2: Privacy by Design and Default, pp. 35-36.

[IAPP CIPP/US Body of Knowledge], Section II: Limits on Private-sector Collection and Use of Data, Subsection B: Privacy by Design, pp. 9-10.

[IAPP Glossary], Terms: Contact Tracing, Privacy by Design, Privacy by Default.

Question: 163

SCENARIO -

Please use the following to answer the next question:

Jane is a U.S. citizen and a senior software engineer at California-based Jones Labs, a major software supplier to the U.S. Department of Defense and other U.S. federal agencies. Jane's manager, Patrick, is a French citizen who has been living in California for over a decade. Patrick has recently begun to suspect that Jane is an insider secretly transmitting trade secrets to foreign intelligence. Unbeknownst to Patrick, the FBI has already received a hint from anonymous whistleblower, and jointly with the National Security Agency is investigating Jane's possible implication in a sophisticated foreign espionage campaign.

Ever since the pandemic, Jane has been working from home. To complete her daily tasks she uses her corporate laptop, which after each login conspicuously provides notice that the equipment belongs to Jones Labs and may be monitored according to the enacted privacy policy and employment handbook. Jane also has a corporate mobile phone that she uses strictly for business, the terms of which are defined in her employment contract and elaborated upon in her employee handbook. Both the privacy policy and the employee handbook are revised annually by a reputable California law firm specializing in privacy law. Jane also has a personal iPhone that she uses for private purposes only.

Jones Labs has its primary data center in San Francisco, which is managed internally by Jones Labs engineers. The secondary data center, managed by Amazon AWS, is physically located in the UK for disaster recovery purposes. Jones Labs' mobile devices backup is managed by a mid-sized mobile defense company located in Denver, which physically stores the data in Canada to reduce costs. Jones Labs MS Office documents are securely stored in a Microsoft Office 365 data center based in Ireland. Manufacturing data of Jones Labs is stored in Taiwan and managed by a local supplier that has no presence in the U.S.

Before inspecting any GPS geolocation data from Jane's corporate mobile phone, Patrick should first do what?

A. Obtain prior consent from Jane pursuant to the Telephone Consumer Protection Act
B. Revise emerging workplace privacy best practices with a reputable advocacy organization.
C. Obtain a subpoena from law enforcement, or a court order, directing Jones Labs to collect the GPS geolocation data.
D. Ensure that such activity is permitted under Jane's employment contract or the company's employee privacy policy.

Answer: D

Explanation:

Patrick should first ensure that inspecting GPS geolocation data from Jane’s corporate mobile phone is permitted under Jane’s employment contract or the company’s employee privacy policy. This is because Jane has a reasonable expectation of privacy in her location information, even if she uses a corporate-owned device for business purposes. The Fourth Amendment protects individuals from unreasonable searches and seizures by the government, and the Electronic Communications Privacy Act (ECPA) prohibits unauthorized interception or access to electronic communications by private parties. Therefore, Patrick cannot inspect Jane’s GPS data without a valid legal basis, such as consent, contract, or court order. Obtaining prior consent from Jane

pursuant to the Telephone Consumer Protection Act (A) is not relevant, as this law regulates unsolicited calls and text messages, not location tracking. Revising emerging workplace privacy best practices with a reputable advocacy organization (B) is not sufficient, as Patrick still needs to comply with the existing legal obligations and contractual terms. Obtaining a subpoena from law enforcement, or a court order, directing Jones Labs to collect the GPS geolocation data © is not necessary, as Patrick is not acting on behalf of the government or in response to a legal request. However, if Patrick does obtain such a legal order, he should also comply with it and notify Jane of the disclosure, unless prohibited by law. Reference: IAPP CIPP/US Study Guide, Chapter 4, Section 4.1.2, p. 115-116

IAPP CIPP/US Study Guide, Chapter4, Section 4.2.1,p. 118-119
IAPP CIPP/US Study Guide, Chapter4, Section 4.2.2,p. 120-121
IAPP CIPP/US Study Guide, Chapter4, Section 4.2.3,p. 122-123
IAPP CIPP/US Study Guide, Chapter4, Section 4.3.1,p. 124-125
IAPP CIPP/US Study Guide, Chapter4, Section 4.3.2,p. 126-127
IAPP CIPP/US Study Guide, Chapter4, Section 4.3.3,p. 128-129
IAPP CIPP/US Study Guide, Chapter4, Section 4.3.4,p. 130-131
IAPP CIPP/US Study Guide, Chapter4, Section 4.3.5,p. 132-133
IAPP CIPP/US Study Guide, Chapter4, Section 4.3.6,p. 134-135
IAPP CIPP/US Study Guide, Chapter4, Section 4.3.7,p. 136-137
IAPP CIPP/US Study Guide, Chapter4, Section 4.3.8,p. 138-139
IAPP CIPP/US Study Guide, Chapter4, Section 4.3.9,p. 140-141
IAPP CIPP/US Study Guide, Chapter4, Section 4.3.10, p.142-143
IAPP CIPP/US Study Guide, Chapter4, Section 4.3.11, p.144-145
IAPP CIPP/US Study Guide, Chapter4, Section 4.3.12, p.146-147
IAPP CIPP/US Study Guide, Chapter4, Section 4.3.13, p.148-149
IAPP CIPP/US Study Guide, Chapter4, Section 4.3.14, p.150-151
IAPP CIPP/US Study Guide, Chapter4, Section 4.3.15, p.152-153
IAPP CIPP/US Study Guide, Chapter4, Section 4.3.16, p.154-155
IAPP CIPP/US Study Guide, Chapter 4, Section 4.3.17, p. 156-157

Question: 164

Once a breach has been definitively established, which task should be prioritized next?

A. Involving law enforcement and state Attorneys General.
B. Determining what was responsible for the breach and neutralizing the threat.
C. Providing notice to the affected parties so they can take precautionary measures.
D. Implementing remedial measures and evaluating how to prevent future breaches.

Answer: C

Explanation:

According to the IAPP CIPP/US study guide, the first priority after a breach has been confirmed is to notify the affected individuals, regulators, and other stakeholders as required by law or contract. This is to allow them to take steps to protect themselves from potential harm, such as identity theft, fraud, or reputational damage. Providing timely and accurate notice also helps to mitigate legal liability, preserve customer trust, and comply with applicable laws and regulations. The other tasks are also important, but they are not the immediate priority after a breach has been established. Reference: IAPP CIPP/US study guide, Chapter

6, Section 6.4.2, page 211.

Question: 165

SCENARIO -

Please use the following to answer the next question:

Miraculous Healthcare is a large medical practice with multiple locations in California and Nevad a. Miraculous normally treats patients in person, but has recently decided to start offering telehealth appointments, where patients can have virtual appointments with on-site doctors via a phone app. For this new initiative, Miraculous is considering a product built by MedApps, a company that makes quality telehealth apps for healthcare practices and licenses them to be used with the practices' branding. MedApps provides technical support for the app, which it hosts in the cloud. MedApps also offers an optional benchmarking service for providers who wish to compare their practice to others using the service.

Riya is the Privacy Officer at Miraculous, responsible for the practice's compliance with HIPAA and other applicable laws, and she works with the Miraculous procurement team to get vendor agreements in place. She occasionally assists procurement in vetting vendors and inquiring about their own compliance practices, as well as negotiating the terms of vendor agreements. Riya is currently reviewing the suitability of the MedApps app from a privacy perspective.

Riya has also been asked by the Miraculous Healthcare business operations team to review the MedApps' optional benchmarking service. Of particular concern is the requirement that Miraculous Healthcare upload information about the appointments to a portal hosted by MedApps.

What HIPAA compliance issue would Miraculous have to consider before using the telehealth app?

A. HIPAA does not permit healthcare providers to use cloud hosting services.
B. HIPAA does not permit in-person appointment data to be hosted in the cloud.
C. HIPAA would require Miraculous and MedApps to enter into a Business Associate Agreement.
D. HIPAA would require Miraculous to obtain patient consent before in-person appointment data can be shared with third parties.

Answer: C

Explanation:

According to HIPAA, a business associate is a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information (PHI) on behalf of, or provides services to, a covered entity. A business associate agreement (BAA) is a written contract

between a covered entity and a business associate that establishes the permitted and required uses and disclosures of PHI by the business associate, as well as the safeguards that the business associate must implement to protect the PHI. In this scenario, MedApps is a business associate of Miraculous, since it provides a telehealth app that involves the use or disclosure of PHI on behalf of Miraculous. Therefore, HIPAA would require Miraculous and MedApps to enter into a BAA before using the telehealth app. The other options are incorrect because HIPAA does not prohibit the use of cloud hosting services or the hosting of in-person appointment data in the cloud, as long as the appropriate safeguards and agreements are in place. HIPAA also does not require patient consent for the sharing of PHI with third parties for treatment, payment, or health care operations purposes, which would include the use of the telehealth app. Reference:

HIPAA and Telehealth - Office for Civil Rights

HIPAA Rules for telehealth technology - Telehealth.HHS.gov

Notification of Enforcement Discretion for Telehealth - Office for Civil Rights

Guidance: How the HIPAA Rules Permit Covered Health Care Providers and Health Plans to Provide Audio-

Only Telehealth - Office for Civil Rights

HIPAA Compliant App - Telehealth.org

IAPP CIPP/US Certified Information Privacy Professional Study Guide - Chapter 3: HIPAA and HITECH, pages 75-76, 81-82, 86-87.

Question: 166

Which of the following conditions would NOT be sufficient to excuse an entity from providing breach notification under state law?

A. If the data involved was encrypted.
B. If the data involved was accessed but not exported.
C. If the entity was subject to the GLBA Safeguards Rule.
D. If the entity followed internal notification procedures compatible with state law.

Answer: B

Explanation:

Most state breach notification laws require entities to notify affected individuals and/or regulators when there is unauthorized access to or acquisition of personal information that compromises its security, confidentiality, or integrity. However, some states provide exceptions to this requirement under certain conditions, such as:

If the data involved was encrypted or otherwise rendered unreadable or unusable, and the encryption key or other means of access was not compromised. This is based on the assumption that encrypted data is not accessible to unauthorized parties, even if they obtain the data.

If the entity was subject to and complied with another federal or state law that provides similar or greater protection and notification requirements, such as the GLBA Safeguards Rule or the HIPAA Breach Notification Rule. This is to avoid duplication or inconsistency of obligations for entities that are already regulated by other laws.

If the entity conducted a risk assessment and determined that there is no reasonable likelihood of harm to the affected individuals, based on factors such as the nature and extent of the data, the circumstances of the breach, the evidence of misuse, and the ability to mitigate the risk. This is to allow entities to exercise some discretion and judgment in evaluating the potential impact of the breach.

However, none of the state laws provide an exception for the mere access of data without exportation. Access alone is considered a breach that triggers the notification requirement, unless one of the other conditions applies. Therefore, option B is not a sufficient excuse for not providing breach notification under state law.

Reference:

[IAPP CIPP/US Study Guide], Chapter 9: State Data Security Laws, pp. 209-211.

CIPP/US Practice Questions (Sample Questions), Question 29.

Question: 167

The use of cookies on a website by a service provider is generally not deemed a 'sale' of personal information by CCPA, as long as which of the following conditions is met?

A. The third party stores personal information to trigger a response to a consumer's request to exercise their right to opt in.

B. The analytics cookies placed by the service provider are capable of being tracked but cannot be linked to a particular consumer of that business.

C. The service provider retains personal information obtained in the course of providing the services specified in the agreement with the subcontractors.

D. The information collected by the service provider is necessary to perform debugging and the business and service provider have entered into an appropriate agreement.

Answer: D

Explanation:

The California Consumer Privacy Act (CCPA) defines a 'sale' of personal information as any transfer or disclosure of personal information to another business or third party for monetary or other valuable consideration. However, the CCPA also provides some exceptions to this definition, such as: If the consumer has directed the business to intentionally disclose the personal information or use the personal information to interact with a third party, provided the third party does not also sell the personal information.

If the business transfers the personal information to a service provider that is contractually prohibited from retaining, using, or disclosing the personal information for any purpose other than performing the services specified in the contract with the business.

If the business transfers the personal information to a third party as part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the business, provided the information is used or shared consistently with the CCPA.

The use of cookies on a website by a service provider is generally not deemed a sale of personal information by the CCPA, as long as the information collected by the service provider is necessary to perform the services specified in the contract with the business, and the service provider does not further collect, sell, or use the personal information of the consumer except as necessary to perform the business purpose. One of the examples of a valid business purpose is to perform debugging to identify and repair errors that impair existing intended functionality.

Therefore, option D is the correct answer, as it describes a scenario where the use of cookies by a service provider is not a sale of personal information under the CCPA, assuming the service provider complies with the contractual obligations and does not further use or disclose the information.

Option A is incorrect, as it does not describe a valid exception to the definition of a sale. The third party that stores personal information to trigger a response to a consumer's request to opt in is not acting as a service provider, but as a separate entity that may have its own interest in the personal information. The consumer's request to opt in does not necessarily imply that the consumer has directed the business to disclose the personal information to the third party.

Option B is incorrect, as it does not describe a valid exception to the definition of a sale. The analytics cookies placed by the service provider may still constitute a sale of personal information, even if they cannot be linked to a particular consumer of that business. The CCPA defines personal information broadly to include any information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Therefore, the analytics cookies may still fall within the scope of personal information, and their use by the service provider may still be a sale, unless one of the exceptions applies.

Option C is incorrect, as it does not describe a valid exception to the definition of a sale. The service provider that retains personal information obtained in the course of providing the services specified in the agreement with the subcontractors is not acting as a service provider to the business, but as a separate entity that may have its own interest in the personal information. The agreement with the subcontractors does not necessarily

imply that the business has authorized the service provider to retain, use, or disclose the personal information for any purpose other than performing the services specified in the contract with the business.

Reference:

[IAPP CIPP/US Study Guide], Chapter 10: California Consumer Privacy Act, pp. 223-226.

CIPP/US Practice Questions (Sample Questions), Question 30.

Question: 168

Under the Driver's Privacy Protection Act (DPPA), which of the following parties would require consent of an individual in order to obtain his or her Department of Motor Vehicle information?

A. Law enforcement agencies performing investigations.
B. Insurance companies needing to investigate claims.
C. Attorneys gathering information related to lawsuits.
D. Marketers wishing to distribute bulk materials.

Answer: D

Explanation:

The Driver's Privacy Protection Act (DPPA) is a federal law that regulates the disclosure of personal information obtained by state departments of motor vehicles (DMVs). The DPPA prohibits DMVs and other entities that receive such information from DMVs from disclosing it to anyone without the express consent of the individual to whom the information pertains, unless the disclosure falls under one of the 14 exceptions listed in the statute.

Some of the exceptions that allow disclosure of personal information from DMV records without consent are:

For use by any government agency, including any court or law enforcement agency, in carrying out its functions, or any private person or entity acting on behalf of a government agency in carrying out its functions.

For use in connection with matters of motor vehicle or driver safety and theft; motor vehicle emissions; motor vehicle product alterations, recalls, or advisories; performance monitoring of motor vehicles, motor vehicle parts and dealers; motor vehicle market research activities, including survey research; and removal of non-owner records from the original owner records of motor vehicle manufacturers.

For use in the normal course of business by a legitimate business or its agents, employees, or contractors, but only to verify the accuracy of personal information submitted by the individual to the business or its agents, employees, or contractors; and if such information as so submitted is not correct or is no longer correct, to obtain the correct information, but only for the purposes of preventing fraud by, pursuing legal remedies against, or recovering on a debt or security interest against, the individual.

For use in connection with any civil, criminal, administrative, or arbitral proceeding in any federal, state, or local court or agency or before any self-regulatory body, including the service of process, investigation in anticipation of litigation, and the execution or enforcement ofjudgments and orders, or pursuant to an order of a federal, state, or local court.

For use in research activities, and for use in producing statistical reports, so long as the personal information is not published, redisclosed, or used to contact individuals.

For use by any insurer or insurance support organization, or by a self-insured entity, or its agents, employees,

or contractors, in connection with claims investigation activities, antifraud activities, rating or underwriting.

For use in providing notice to the owners of towed or impounded vehicles.

For use by any licensed private investigative agency or licensed security service for any purpose permitted under this subsection.

For use by an employer or its agent or insurer to obtain or verify information relating to a holder of a commercial driver's license that is required under chapter 313 of title 49.

For use in connection with the operation of private toll transportation facilities.

For any other use specifically authorized under the law of the state that holds the record, if such use is related to the operation of a motor vehicle or public safety.

None of the exceptions above apply to the use of personal information from DMV records by marketers wishing to distribute bulk materials. Therefore, such use would require the consent of the individual to whom the information pertains, according to the DPPA. Hence, option D is the correct answer.

Option A is incorrect, as law enforcement agencies performing investigations are exempt from the consent requirement under the first exception.

Option B is incorrect, as insurance companies needing to investigate claims are exempt from the consent requirement under the sixth exception.

Option C is incorrect, as attorneys gathering information related to lawsuits are exempt from the consent requirement under the fourth exception.

Reference:

[IAPP CIPP/US Study Guide], Chapter 8: Federal Privacy Laws, pp. 181-182.

CIPP/US Practice Questions (Sample Questions), Question 31.

Question: 169

Which of the following federal agencies does NOT have regulatory authority related to privacy?

A. Consumer Financial Protection Bureau.
B. U.S. Department of Transportation.
C. U.S. Department of Commerce.
D. Federal Reserve

Answer: C

Explanation:

The U.S. Department of Commerce (DOC) is a federal agency that promotes economic growth, trade, and innovation, but does not have regulatory authority related to privacy. The DOC administers several voluntary privacy frameworks, such as the Privacy Shield, the APEC Cross-Border Privacy Rules, and the NIST Privacy Framework, but these are not legally binding or enforceable by the DOC12. The DOC also participates in international privacy negotiations and dialogues, but does not have the power to issue rules or regulations on privacy matters3.

The other three options are examples of federal agencies that do have regulatory authority related to privacy. The Consumer Financial Protection Bureau (CFPB) is an independent agency that enforces consumer protection laws, such as the Fair Credit Reporting Act, the Gramm-Leach-Bliley Act, and the Dodd-Frank Act, which contain privacy and data security provisions4. The U.S. Department of Transportation (DOT) is a federal agency that regulates transportation safety, security, and infrastructure, and has issued privacy rules for airlines, motor carriers, and railroads. The Federal Reserve (FRB) is an independent agency that oversees the nation's monetary policy, banking system, and financial stability, and has issued privacy rules for financial institutions under its jurisdiction. Reference: 1: Privacy Shield Program Overview | International Trade

Administration 2: NIST Privacy Framework | NIST 3: Privacy and Data Security | U.S. Department of Commerce 4: Consumer Financial Protection Bureau - Wikipedia : [Privacy | US Department of Transportation] : [Privacy - Federal Reserve Board]

Question: 170

Which of the following practices is NOT a key component of a data ethics framework?

A. Automated decision-making.
B. Preferability testing.
C. Data governance.
D. Auditing.

Answer: A

Explanation:
A data ethics framework is a set of principles and guidelines that help organizations ensure that their data practices are ethical, responsible, and trustworthy. According to the IAPP CIPP/US Study Guide, some of the key components of a data ethics framework are1:

Data governance: the policies, processes, and standards that govern how data is collected, used, stored, and shared within an organization.

Preferability testing: the process of assessing the potential impacts and risks of data-driven solutions on stakeholders, such as customers, employees, and society.

Auditing: the process of monitoring, reviewing, and verifying the compliance and performance of data practices against the established ethical standards and legal requirements. Automated decisionmaking, on the other hand, is not a key component of a data ethics framework, but rather a data practice that may raise ethical issues and challenges. Automated decision-making refers to the use of algorithms, artificial intelligence, or machine learning to make decisions or recommendations without human intervention2. While automated decision-making can offer benefits such as efficiency, accuracy, and consistency, it can also pose risks such as bias, discrimination, lack of transparency, and accountability3. Therefore, automated decision-making should be subject to ethical evaluation and oversight, but it is not itself a part of a data ethics framework. Reference: [IAPP CIPP/US Study Guide], Chapter 10, Section 10.4, page 287 [IAPP Glossary], Automated Decision-Making
IAPP Resources, Ethical Data Use and Automated Decision-Making: A Practical Guide

Question: 171

What was unique about the action that the Federal Trade Commission took against B.J.'s Wholesale Club in 2005?

A. It made third-party audits a penalty for policy violations.
B. It was based on matters of fairness rather than deception.
C. It was the first substantial U.S.-EU Safe Harbor enforcement.
D. It made user consent mandatory after any revisions of policy.

Answer: B

Explanation:

The Federal Trade Commission (FTC) is the primary federal agency that enforces consumer privacy and data security laws in the United States. The FTC has the authority to bring enforcement actions against businesses that engage in unfair or deceptive acts or practices that affect commerce, under Section 5 of the FTC Act. Unfair acts or practices are those that cause or are likely to cause substantial injury to consumers that is not reasonably avoidable by consumers and is not outweighed by countervailing benefits to consumers or competition. Deceptive acts or practices are those that involve a material representation, omission, or practice that is likely to mislead consumers acting reasonably under the circumstances.

The FTC's action against B.J.'s Wholesale Club in 2005 was unique because it was based on matters of fairness rather than deception. The FTC alleged that B.J.'s Wholesale Club, a retailer that operates warehouse stores and gas stations, failed to provide reasonable security for the sensitive information of its customers, such as name, card number, and expiration date, that it collected from the magnetic stripes of credit and debit cards. The FTC claimed that this information was used by unauthorized persons to make millions of dollars of fraudulent purchases. The FTC did not allege that B.J.'s Wholesale Club made any false or misleading statements or omissions about its data security practices, but rather that its failure to take appropriate security measures was an unfair practice that violated Section 5 of the FTC Act. The FTC argued that B.J.'s Wholesale Club's lax security caused or was likely to cause substantial injury to consumers that was not reasonably avoidable by consumers and was not outweighed by any benefits to consumers or competition.

The FTC's action against B.J.'s Wholesale Club was one of the first cases in which the FTC used its unfairness authority to address data security issues, and it set a precedent for future enforcement actions against businesses that fail to protect consumer data. The settlement required B.J.'s Wholesale Club to implement a comprehensive information security program and obtain audits by an independent third-party security professional every other year for 20 years. Reference: FTC Complaint, Paragraphs 1-23

FTC Agreement Containing Consent Order, Paragraphs 1-9

FTC Analysis of Proposed Consent Order to Aid Public Comment, Pages 1-3

[IAPP CIPP/US Study Guide], Pages 69-70

Question: 172

Mega Corp. is a U.S.-based business with employees in California, Virginia, and Colorado. Which of the following must Mega Corp. comply with in regard to its human resources data?

A. California Privacy Rights Act.
B. California Privacy Rights Act and Virginia Consumer Data Protection Act.
C. California Privacy Rights Act and Colorado Privacy Act.
D. California Privacy Rights Act, Virginia Consumer Data Protection Act, and Colorado Privacy Act.

Answer: D

Explanation:

Mega Corp. is a U.S.-based business with employees in California, Virginia, and Colorado. Therefore, it must comply with the privacy laws of these three states in regard to its human resources data, unless it qualifies for an exemption under each law.

The California Privacy Rights Act (CPRA) is an amendment to the California Consumer Privacy Act (CCPA) that

was approved by voters in November 2020 and will take effect on January 1, 2023. The CPRA expands the rights and protections of California residents with respect to their personal information and creates a new category of sensitive personal information that includes certain employment-related data, such as Social Security numbers, driver's license numbers, passport numbers, financial account information, biometric information, and geolocation data. The CPRA also establishes a new enforcement agency, the California Privacy Protection Agency, to oversee and enforce the law.

The Virginia Consumer Data Protection Act (VCDPA) is a comprehensive privacy law that was enacted in March 2021 and will take effect on January 1, 2023. The VCDPA grants Virginia residents several rights with respect to their personal data, such as the right to access, correct, delete, port, and opt out of certain processing activities. The VCDPA also imposes various obligations on businesses that control or process personal data of Virginia residents, such as conducting data protection assessments, entering into contracts with processors, and providing privacy notices.

The Colorado Privacy Act (CPA) is another comprehensive privacy law that was enacted in July 2021 and will take effect on July 1, 2023. The CPA grants Colorado residents similar rights as the VCDPA, with some variations, such as the right to appeal a business's response to a request and the right to opt out of targeted advertising, the sale of personal data, and certain profiling activities. The CPA also imposes similar obligations as the VCDPA, with some differences, such as requiring opt-in consent for the processing of sensitive data and allowing businesses to join a universal opt-out mechanism.

All three laws apply to businesses that conduct business in or target consumers in the respective states and meet certain thresholds of revenue or data processing volume. However, all three laws also provide exemptions for certain types of data or entities that are subject to other federal or state laws, such as the Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA), the Fair Credit Reporting Act (FCRA), and the Family Educational Rights and Privacy Act (FERPA).

One of the exemptions that may be relevant for Mega Corp. is the employee data exemption, which excludes personal data that is collected and used by an employer within the context of an employment relationship or for emergency contact or benefits administration purposes. However, this exemption is not permanent or uniform across the three laws. The CPRA's employee data exemption is set to expire on January 1, 2023, unless extended by the legislature. The VCDPA's employee data exemption is set to expire on January 1, 2023, unless repealed by the legislature. The CPA's employee data exemption does not have an expiration date, but it does not apply to the right to opt out of the sale of personal data or the right to appeal a business's response to a request. Therefore, depending on the type and scope of the human resources data that Mega Corp. collects and processes, it may have to comply with the California Privacy Rights Act, the Virginia Consumer Data Protection Act, and the Colorado Privacy Act, unless it qualifies for another exemption under each law.

Reference:

[IAPP CIPP/US Study Guide], Chapter 10: State Data Security Laws, pp. 227-229.

CIPP/US Practice Questions (Sample Questions), Question 32.

Question: 173

Which of the following privacy rights is NOT available under the Colorado Privacy Act?

A. The right to access sensitive data.
B. The right to correct sensitive data.
C. The right to delete sensitive data.
D. The right to limit the use of sensitive data.

Answer: D

Explanation:

The Colorado Privacy Act (CPA) grants consumers the right to access, correct, or delete their personal data, including sensitive data, that is processed by a controller1. Sensitive data is defined as personal data that reveals racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, sex life or sexual orientation, citizenship or citizenship status, genetic or biometric data, or personal data from a known child2. The CPA also grants consumers the right to opt out of the processing of their personal data for purposes of targeted advertising, the sale of personal data, or certain kinds of profiling3. However, the CPA does not grant consumers the right to limit the use of sensitive data for other purposes, such as providing a product or service requested by the consumer, complying with legal obligations, or protecting the vital interests of the consumer or another person. Therefore, option D is the correct answer, as it is not a privacy right available under the CPA. Reference: 1: Colorado Privacy Act (CPA) - Colorado Attorney General 2: Protect Personal Data Privacy | Colorado General Assembly 3: SENATE BILL 21-190 Woodward, Garcia; PRIVACY. COLORADO PRIVACY ACT ... : Colorado Privacy Act: What You Need to Know | OneTrust DataGuidance

Question: 174

SuperMart is a large Nevada-based business that has recently determined it sells what constitutes "covered information" under Nevada's privacy law, Senate Bill 260. Which of the following privacy compliance steps would best help SuperMart comply with the law?

A. Providing a mechanism for consumers to opt out of sales.
B. Implementing internal protocols for handling access and deletion requests.
C. Preparing a notice of financial incentive for any loyalty programs offered to its customers.
D. Reviewing its vendor contracts to ensure that the vendors are subject to service provider restrictions.

Answer: A

Explanation:

Nevada's privacy law, Senate Bill 260 (SB 260), is an amendment to the existing Nevada Revised Statutes (NRS) Chapter 603A that was enacted in June 2021 and will take effect on October 1, 2021. SB 260 expands the scope and definition of "covered information" under NRS 603A to include any information that identifies, relates to, describes, or is capable of being associated with a consumer, such as name, address, email, phone number, social security number, biometric data, geolocation data, and online identifiers. SB 260 also grants Nevada consumers the right to opt out of the sale of their covered information by an operator of a website or online service that collects and maintains such information.

Under SB 260, an operator is defined as a person who owns or operates a website or online service for commercial purposes, collects and maintains covered information from consumers who reside in Nevada and use or visit the website or online service, and purposefully directs its activities toward Nevada. A sale is defined as the exchange of covered information for monetary consideration by the operator to a person for the person to license or sell the covered information to additional persons. However, there are some exceptions to the definition of a sale, such as:

If the consumer has consented to the sale after being provided with clear and conspicuous notice of the sale and the opportunity to opt out.

If the sale is to a person who processes the covered information on behalf of the operator.

If the sale is to a person with whom the consumer has a direct relationship for the purposes of providing a product or service requested by the consumer.
If the sale is to a person for purposes that are consistent with the reasonable expectations of the consumer considering the context in which the consumer provided the covered information to the operator.
If the sale is to a person who is an affiliate of the operator.
If the sale is to a person as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the person assumes control of all or part of the operator's assets.
To comply with SB 260, an operator that sells covered information must provide a designated request address through which a consumer may submit a verified request to opt out of the sale. The designated request address may be an email address, a toll-free telephone number, or an Internet website. The operator must respond to the verified request within 60 days, and may extend the response period for an additional 30 days if reasonably necessary. The operator must also provide a
notice to the consumer that identifies the categories of covered information that the operator collects and the categories of third parties to whom the operator may disclose the covered information.
Therefore, the best privacy compliance step for SuperMart to comply with SB 260 is to provide a mechanism for consumers to opt out of sales, as this is the core requirement of the law. Option A is the correct answer.
Option B is incorrect, as SB 260 does not grant consumers the right to access or delete their covered information, unlike other state privacy laws such as the California Consumer Privacy Act (CCPA) or the Virginia Consumer Data Protection Act (VCDPA).
Option C is incorrect, as SB 260 does not require operators to provide a notice of financial incentive for any loyalty programs offered to their customers, unlike the CCPA.
Option D is incorrect, as SB 260 does not impose service provider restrictions on the vendors of the operators, unlike the CCPA or the VCDPA.
Reference:
[IAPP CIPP/US Study Guide], Chapter 10: State Data Security Laws, pp. 229-230.
CIPP/US Practice Questions (Sample Questions), Question 33.

Question: 175

Under GLB
A. which of these organizations would not be required to provide its customers with an annual privacy notice?

A. An insurance company that has no privacy department
B. An auction house that also acts as a financial institution
C. A credit union that has made changes to its privacy notice from last year.
D. A credit union that has not made changes to its privacy notice from last year

Answer: D

Explanation:
Under the Gramm-Leach-Bliley Act (GLBA), financial institutions are required to provide their customers with an annual privacy notice that explains how they collect, share, and protect customers' personal information. However, the GLBA Privacy Rule (16 CFR Part 313) was amended by the Fixing America's Surface Transportation Act (FAST Act) in 2015, which introduced an exception to this requirement.
According to the FAST Act, financial institutions are not required to provide annual privacy notices if they meet two conditions:

No changes have been made to their privacy policy or practices since the last notice was sent to customers.
The financial institution does not share customers' nonpublic personal information with nonaffiliated third parties in a way that triggers an opt-out requirement under GLBA.
Explanation of Options:
A . An insurance company that has no privacy department: This is irrelevant. The requirement to provide privacy notices depends on whether the organization falls under GLBA's definition of a "financial institution" and their compliance with privacy practices, not on the presence of a privacy department.
B . An auction house that also acts as a financial institution: If the auction house qualifies as a financial institution under GLBA (e.g., if it arranges financing), it would still need to comply with GLBA privacy requirements, including issuing annual privacy notices unless it qualifies for the exception.
C . A credit union that has made changes to its privacy notice from last year: If any changes are made to the privacy policy, the credit union must issue an updated privacy notice to its customers.
D . A credit union that has not made changes to its privacy notice from last year: This is the correct answer. If the credit union has not made any changes to its privacy notice and meets the FAST Act exception criteria (outlined above), it is not required to issue an annual privacy notice.
Reference from CIPP/US Materials:
GLBA Privacy Rule (16 CFR Part 313): This rule outlines the requirements for financial institutions to provide privacy notices.
FAST Act (2015) Amendment to GLBA Privacy Rule: This amendment introduced exceptions to the annual notice requirement for institutions that meet specific criteria.
IAPP CIPP/US Certification Textbook: Details the conditions under which GLBA exceptions apply and describes how the FAST Act impacted annual privacy notice requirements.

Question: 176

The concept of data portability refers to what?

A. The practice of disclosing all the data sources one organization uses to enhance data collection from different social media platforms
B. The technical measures organizations use to empower consumers' control in case data is being transferred to service providers
C. The ability of individuals to obtain and reuse their personal data for their own purposes across different services.
D. The ability of individuals to easily change to another similar service provider if fees are unlawfully being raised

Answer: C

Explanation:
The concept of data portability refers to an individual's right to access and transfer their personal data from one organization to another. It enables individuals to obtain and reuse their personal data for their own purposes across different services. For example, an individual can request their data from one service provider and transfer it to another provider, facilitating competition and giving consumers more control over their data.
This right is commonly associated with General Data Protection Regulation (GDPR) but is becoming more widely discussed in U.S. privacy contexts, such as under the California Consumer Privacy Act (CCPA) and similar state laws. Although the CCPA does not explicitly mention "data portability," the concept aligns with its

provision that grants individuals the right to access their data in a portable and usable format.

Explanation of Options:

A . The practice of disclosing all the data sources one organization uses to enhance data collection from different social media platforms: This describes a data disclosure practice, not data portability. B . The technical measures organizations use to empower consumers' control in case data is being transferred to service providers: This refers to technical controls but does not fully capture the essence of data portability.

C . The ability of individuals to obtain and reuse their personal data for their own purposes across different services: This is the correct answer and accurately defines data portability.

D . The ability of individuals to easily change to another similar service provider if fees are unlawfully being raised: While data portability might facilitate switching providers, it is not specifically tied to the issue of unlawful fee increases.

Reference from CIPP/US Materials:

GDPR Article 20: Provides the right to data portability in the EU.

CCPA Section 1798.100: Requires businesses to provide personal data in a readily usable format upon request.

IAPP CIPP/US Certification Textbook: Discusses data portability as part of consumer rights and privacy frameworks.

Question: 177

Which of the following is NOT a common challenge large organizations face when implementing data portability?

A. The presence of third-party data in the data to be ported.
B. Technically compatible systems for transmission feasibility
C. Security considerations in relation to the transfer of the data.
D. The technical skillsets available in the transmitting organization.

Answer: D

Explanation:

When implementing data portability, organizations often face significant challenges due to the complexity of managing data transfers. These challenges commonly include concerns about third- party data, technical compatibility for data transmission, and security considerations. However, the technical skillsets available in the transmitting organization is NOT typically identified as a primary challenge because most organizations have or can acquire the necessary technical expertise through training or by outsourcing.

Explanation of Options:

A . The presence of third-party data in the data to be ported: This is a valid challenge, as the inclusion of third-party data can raise legal and contractual concerns about ownership and transferability.

B . Technically compatible systems for transmission feasibility: Ensuring that data can be transferred between systems in compatible formats is a critical and common challenge.

C . Security considerations in relation to the transfer of the data: Data transfers must be secure to prevent unauthorized access or breaches, making this a valid challenge.

D . The technical skillsets available in the transmitting organization: While technical skills are important, organizations usually have the ability to address this issue through hiring, training, or outsourcing, making this the least common challenge.

Reference from CIPP/US Materials:

IAPP CIPP/US Certification Textbook: Discusses operational challenges related to data portability, including system compatibility, data security, and third-party involvement.
NIST Privacy Framework: Addresses organizational readiness and data transfer risks.

Question: 178

Under the EU-US Data Privacy Framework, what must participating organizations provide to individuals in regard to complaints and disputes?

A. An independent recourse mechanism.
B. A copy 01 the individual's personal data
C. A description of the organization's data processing policies
D. A means of communicating with the organization's privacy team.

Answer: A

Explanation:
Under the EU-US Data Privacy Framework (DPF), organizations that participate in the framework must provide individuals with a way to resolve complaints and disputes about how their personal data is handled. Specifically, organizations are required to offer an independent recourse mechanism to ensure compliance with the principles of the framework. This mechanism enables individuals to bring their complaints forward and have them addressed through an impartial and accessible process.
The independent recourse mechanism is critical to the DPF as it reinforces accountability and builds trust in cross-border data transfers. Organizations must select a third-party dispute resolution provider (such as an alternative dispute resolution body or a regulatory body) and disclose this mechanism in their privacy policies. The mechanism must be provided free of charge to the individual.
Explanation of Options:
A . An independent recourse mechanism: This is the correct answer, as it is explicitly required under the EU-US Data Privacy Framework for resolving disputes and complaints related to data privacy.
B . A copy of the individual's personal data: While data access rights are part of broader privacy regulations (e.g., GDPR), this is not specific to the EU-US DPF's requirements regarding complaint handling.
C . A description of the organization's data processing policies: While transparency about data processing is an important requirement under the DPF, it does not address the need for a formal dispute resolution mechanism.
E. A means of communicating with the organization's privacy team: While communication channels are essential, they do not meet the requirement for an independent recourse mechanism as stipulated by the DPF.
Reference from CIPP/US Materials:
EU-US Data Privacy Framework Principles: Specifically, the "Recourse, Enforcement, and Liability" principle requires participating organizations to provide an independent recourse mechanism for complaints.
IAPP CIPP/US Certification Textbook: Discusses dispute resolution and redress mechanisms as a cornerstone of international data transfer agreements.
US Department of Commerce Privacy Shield Program Website: Similar requirements under the now- replaced Privacy Shield have been carried over to the DPF, ensuring individuals have access to independent redress mechanisms.

Question: 179

SCENARIO

Please use the following to answer the next question;

Miraculous Healthcare is a large medical practice with multiple locations in California and Nevad a. Miraculous normally treats patients in person, but has recently decided to start offering telehealth appointments, where patients can have virtual appointments with on-site doctors via a phone app. For this new initiative. Miraculous is considering a product built by MedApps. a company that makes quality telehealth apps for healthcare practices and licenses them to be used with the practices" branding. MedApps provides technical support for the app. which it hosts in the cloud MedApps also offers an optional benchmarking service for providers who wish to compare their practice to others using the service

Riya is the Privacy Officer at Miraculous, responsible for the practice s compliance with HIPAA and other applicable laws, and she works with the Miraculous procurement team to get vendor agreements in place. She occasionally assists procurement in vetting vendors and inquiring about their own compliance practices. as well as negotiating the terms of vendor agreements Riya is currently reviewing the suitability of the MedApps app from a pnvacy perspective

Riya has also been asked by the Miraculous Healthcare business operations team to review the MedApps' optional benchmarking service. Of particular concern is the requirement that Miraculous Healthcare upload information about the appointments to a portal hosted by MedApps

Which of the following would accurately describe the relationship of the parties if they enter into a contract for use of the app?

A. Miraculous Healthcare would be the covered entity because Us name and branding are on the app. MedApps would be a business associate because it Is hosting the data that supports the app B. MedApps would be the covered entity because it built and hosts the app and all the data. Miraculous Healthcare would be a business associate because it only provides its brand on the app. C. Miraculous Healthcare would be a covered entity because it is the healthcare provider; MedApps would also be a covered entity because the data in the app is being shared with it.

D. Miraculous Healthcare would be the covered entity because it is the healthcare provider; MedApps would be a business associate because it is providing a service to support Miraculous.

Answer: D

Explanation:

Under the Health Insurance Portability and Accountability Act (HIPAA), entities involved in the handling of protected health information (PHI) are classified as either covered entities or business associates based on their roles and activities.

Definitions Under HIPAA:

Covered Entity (CE):

A healthcare provider, health plan, or healthcare clearinghouse that creates, receives, maintains, or transmits PHI.

Miraculous Healthcare qualifies as a covered entity because it is a medical practice directly providing healthcare services to patients.

Business Associate (BA):

An organization or individual that performs functions, activities, or services involving the use or disclosure of PHI on behalf of a covered entity.

MedApps qualifies as a business associate because it is providing a telehealth app service to Miraculous, which involves hosting and maintaining PHI (e.g., appointment details, patient information).

Analysis of the Relationship:

Miraculous Healthcare: As the healthcare provider, it is responsible for patient care and compliance with HIPAA. Since it directly provides healthcare services to patients, it is the covered entity in this scenario.

MedApps: Although MedApps designed, hosts, and supports the telehealth app, it is providing these services on behalf of Miraculous Healthcare. As such, MedApps is a business associate under HIPAA. This designation requires MedApps to comply with HIPAA regulations through a Business Associate Agreement (BAA), ensuring that it appropriately safeguards the PHI it handles on behalf of Miraculous Healthcare.

Consideration of the Benchmarking Service:

The optional benchmarking service also reinforces MedApps' role as a business associate. Miraculous Healthcare would need to assess whether the PHI uploaded for benchmarking meets HIPAA's minimum necessary standard and that MedApps implements appropriate safeguards for PHI used for benchmarking. The BAA would need to address these specific uses.

Explanation of Options:

A . Miraculous Healthcare would be the covered entity because its name and branding are on the app. MedApps would be a business associate because it is hosting the data that supports the app: While this is close, it oversimplifies the reasoning by focusing solely on branding. The covered entity designation is determined by the healthcare services provided, not just branding.

B . MedApps would be the covered entity because it built and hosts the app and all the data. Miraculous Healthcare would be a business associate because it only provides its brand on the app: This is incorrect because MedApps is not directly providing healthcare services. Hosting and maintaining PHI does not make it a covered entity but rather a business associate.

C . Miraculous Healthcare would be a covered entity because it is the healthcare provider; MedApps would also be a covered entity because the data in the app is being shared with it: This is incorrect because MedApps does not independently provide healthcare services to patients. Its role is solely as a service provider to Miraculous.

D . Miraculous Healthcare would be the covered entity because it is the healthcare provider; MedApps would be a business associate because it is providing a service to support Miraculous: This is the correct answer. Miraculous is the covered entity, and MedApps, by hosting the telehealth app and handling PHI on Miraculous' behalf, is a business associate.

Reference from CIPP/US Materials:

HIPAA Privacy Rule (45 CFR § 160.103): Defines covered entities and business associates.

Business Associate Agreements (BAAs): HIPAA requires a BAA between covered entities and business associates to ensure PHI is appropriately protected.

IAPP CIPP/US Certification Textbook: Provides detailed examples of covered entities and business associates, along with their roles and responsibilities under HIPAA.

Question: 180

SCENARIO

Please use the following to answer the next question;

Miraculous Healthcare is a large medical practice with multiple locations in California and Nevad a. Miraculous normally treats patients in person, but has recently decided to start offering teleheaith appointments, where patients can have virtual appointments with on-site doctors via a phone app For this new initiative. Miraculous is considering a product built by MedApps, a company that makes quality teleheaith apps for healthcare practices and licenses them to be used with the practices' branding. MedApps provides technical support for the app. which it hosts in the cloud MedApps also offers an optional benchmarking service for providers who wish to compare their practice to others using the service

Riya is the Privacy Officer at Miraculous, responsible for the practice's compliance with HIPAA and other applicable laws, and she works with the Miraculous procurement team to get vendor agreements in place. She occasionally assists procurement in vetting vendors and inquiring about their own compliance practices. as well as negotiating the terms of vendor agreements Riya is currently reviewing the suitability of

the MedApps app from a privacy perspective.

Riya has also been asked by the Miraculous Healthcare business operations team to review the MedApps' optional benchmarking service. Of particular concern is the requirement that Miraculous Healthcare upload information about the appointments to a portal hosted by MedApps What is the most practical action Riya can take to minimize the privacy risks of using an app for telehealth appointments?

A. Prevent MedApps from using copies of the patient data.
B. Require MedApps to obtain consent from all patients.
C. Require MedApps to submit a SOC2 report.
D. Engage in active oversight of MedApps

Answer: D

Explanation:

When handling sensitive data, such as protected health information (PHI) in compliance with HIPAA, it is crucial for covered entities, such as Miraculous Healthcare, to ensure that their business associates (e.g., MedApps) appropriately safeguard the data they process. While contracts like Business Associate Agreements (BAAs) establish the obligations of business associates, active oversight by the covered entity is a practical and necessary step to mitigate privacy risks and ensure compliance.

Why Active Oversight is the Best Option:

Active oversight involves regular monitoring, audits, and reviews of MedApps' practices to ensure they comply with the agreed-upon privacy and security obligations.

This approach allows Miraculous Healthcare to confirm that MedApps is implementing appropriate technical and organizational safeguards, such as encryption, secure access controls, and breach notification processes.

It also ensures that MedApps remains compliant with HIPAA requirements over time, even if there are changes to the app, its services, or legal requirements.

Explanation of Options:

A. Prevent MedApps from using copies of the patient data:

While restricting MedApps from creating unnecessary data copies could reduce some risks, it is often impractical, especially for troubleshooting, app hosting, and support purposes. HIPAA does not require outright prevention of data copies, as long as PHI is appropriately safeguarded and used solely for permissible purposes.

B. Require MedApps to obtain consent from all patients:

Under HIPAA, covered entities (not business associates) are primarily responsible for obtaining patient consent or authorization where required. MedApps, as a business associate, processes PHI on behalf of Miraculous Healthcare and is not in a position to obtain consent directly from patients. C. Require MedApps to submit a SOC2 report:

A SOC 2 (Service Organization Control 2) report can provide valuable assurance regarding MedApps' security, availability, and confidentiality practices. However, this action alone does not mitigate all risks, as SOC 2 reports are point-in-time assessments and may not reflect ongoing compliance or address specific HIPAA requirements.

D. Engage in active oversight of MedApps:

This is the most practical and comprehensive approach. Active oversight includes reviewing MedApps' privacy practices, conducting periodic assessments, and monitoring compliance with the Business Associate Agreement (BAA). It ensures that MedApps continues to protect PHI appropriately and addresses any privacy risks proactively.

Additional Context:

In the context of the optional benchmarking service, Riya should ensure:

The uploaded data is de-identified or aggregated to comply with HIPAA's de-identification standard (45 CFR § 164.514) if possible.

The use of PHI for benchmarking is explicitly addressed in the BAA or a separate agreement.

Reference from CIPP/US Materials:

HIPAA Privacy Rule (45 CFR § 160.103 and 164.504): Describes the responsibilities of covered entities and business associates, including the need for BAAs and safeguards for PHI.

NIST Privacy Framework and NIST SP 800-53: Provides guidance on implementing oversight mechanisms for third-party risk management.

IAPP CIPP/US Certification Textbook: Discusses the importance of vendor management and active oversight in ensuring privacy compliance.

Conclusion:

Requiring MedApps to submit a SOC 2 report or restricting data use might address specific concerns but would not provide the comprehensive, ongoing protection necessary to reduce risks effectively. Engaging in active oversight is the most practical and effective action to minimize privacy risks while maintaining compliance with HIPAA.

Question: 181

SCENARIO

Please use the following to answer the next question;

Miraculous Healthcare is a large medical practice with multiple locations in California and Nevad a. Miraculous normally treats patients in person, but has recently decided to start offering tliehealth appointments, where patients can have virtual appointments with on-site doctors via a phone app For this new initiative. Miraculous is considering a product built by MedApps, a company that makes quality teleheaith apps for healthcare practices and licenses them to be used with the practices" branding. MedApps provides technical support for the app. which it hosts in the cloud. MedApps also offers an optional benchmarking service for providers who wish to compare their practice to others using the service

Riya is the Privacy Officer at Miraculous, responsible for the practice's compliance with HIPAA and other applicable laws, and she works with the Miraculous procurement team to get vendor agreements in place She occasionally assists procurement in vetting vendors and inquiring about their own compliance practices. as well as negotiating the terms of vendor agreements. Riya is currently reviewing the suitability of the MedApps app from a privacy perspective.

Riya has also been asked by the Miraculous Healthcare business operations team to review the MedApps' optional benchmarking service. Of particular concern is the requirement that Miraculous Healthcare upload information about the appointments to a portal hosted by MedAppsa

If MedApps receives an access request under CCPAfrom a California-based app user, how should It handle the request?

A. MedApps should immediately begin deleting the user's data.
B. MedApps should provide the privacy notice in an easily readable format
C. MedApps should decline the request because MedApps is not based In California.
D. MedApps should promptly forward the request to Miraculous for instructions on handling.

Answer: D

Explanation:

Under the California Consumer Privacy Act (CCPA), businesses are required to respond to consumer requests for access, deletion, or information about how their data is processed. However, the responsibilities differ depending on whether the entity is acting as a business or a service provider under the CCPA.

Key CCPA Definitions:

Business:
The entity that determines the purposes and means of processing personal information.
In this scenario, Miraculous Healthcare is the business because it determines how the app and its associated data are used to deliver healthcare services.
Service Provider:
The entity that processes personal information on behalf of the business pursuant to a contractual agreement.
MedApps acts as a service provider because it is hosting and managing the app and the data on behalf of Miraculous Healthcare.
As a service provider, MedApps is restricted in how it can handle consumer data and must follow the instructions of the business (Miraculous Healthcare) for any data-related requests. Therefore, if MedApps receives an access or deletion request from a California-based user, it must forward the request to Miraculous Healthcare, which is responsible for determining how to respond in compliance with the CCPA.
Explanation of Options:
A. MedApps should immediately begin deleting the user's data:
This is incorrect because MedApps cannot act independently in responding to access or deletion requests under CCPA. As a service provider, it must follow the instructions of the business (Miraculous Healthcare).
B. MedApps should provide the privacy notice in an easily readable format:
This is irrelevant to the question. While providing a privacy notice in a readable format is a CCPA requirement, it does not address how to handle an access request.
C. MedApps should decline the request because MedApps is not based in California:
This is incorrect. CCPA applies to businesses and service providers that collect or process personal data of California residents, regardless of whether the entity itself is physically located in California. D. MedApps should promptly forward the request to Miraculous for instructions on handling: This is correct. Under CCPA, service providers are required to cooperate with the business and must forward consumer requests to the business for guidance and action. MedApps' role as a service provider obligates it to defer to Miraculous Healthcare's instructions.
Relevant Reference from CIPP/US Materials:
CCPA Section 1798.140(v): Defines a service provider and outlines its obligations to process personal information only on behalf of the business and in accordance with contractual terms.
CCPA Section 1798.105(c): States that service providers are not required to delete personal information unless instructed to do so by the business.
IAPP CIPP/US Certification Textbook: Discusses the roles of businesses and service providers under the CCPA and their respective responsibilities regarding consumer requests.
Practical Considerations:
Riya, as the Privacy Officer at Miraculous Healthcare, should ensure that the Business Associate Agreement (BAA) and any CCPA-specific contract provisions with MedApps clearly define: The process for handling consumer requests under CCPA.
The requirement for MedApps to promptly notify and defer to Miraculous Healthcare for any such requests.
Conclusion:
MedApps, as a service provider, is not authorized to respond to CCPA access or deletion requests independently. It must forward the request to Miraculous Healthcare for instructions.

Question: 182

What consumer protection did the Fair and Accurate Credit Transactions Act (FACTA) require?

A. The ability to correct inaccurate credit report information

B. The truncation of account numbers on credit card receipts
C. The right to request removal from email lists.
D. The issuing of notice when third-party data is used in an adverse decision

Answer: B

Explanation:
The Fair and Accurate Credit Transactions Act (FACTA) is a U.S. federal law enacted in 2003 that amended the Fair Credit Reporting Act (FCRA). It introduced a variety of provisions designed to combat identity theft and protect consumer information. One of the key consumer protections required by FACTA is the truncation of credit and debit card numbers on receipts to prevent identity theft.
Details of the Truncation Requirement:
FACTA Section 113 (15 U.S.C. § 1681c(g)):
Retailers are prohibited from printing more than the last five digits of a credit or debit card number on electronically generated receipts. Additionally, the card's expiration date must also be excluded. This requirement applies to point-of-sale and other electronically printed receipts and aims to reduce the risk of credit card fraud and identity theft.
Explanation of Options:
A. The ability to correct inaccurate credit report information:
This right is protected under the Fair Credit Reporting Act (FCRA), not FACTA specifically.
B. The truncation of account numbers on credit card receipts:
This is correct, as it is one of the most notable protections introduced by FACTA to prevent identity theft.
C. The right to request removal from email lists:
This right is not provided under FACTA but may be addressed by other laws, such as the CAN-SPAM Act.
D. The issuing of notice when third-party data is used in an adverse decision:
This requirement is a provision of the FCRA, not FACTA.
Reference from CIPP/US Materials:
FACTA Section 113 (15 U.S.C. § 1681c(g)): Details the truncation requirements for credit and debit card receipts.
IAPP CIPP/US Certification Textbook: Highlights FACTA's measures to protect consumer financial information and prevent identity theft.

Question: 183

Which of the following would best provide a sufficient consumer disclosure under the Fair Credit Reporting Act (FCRA) prior to a consumer report being obtained for employment purposes?

A. A verbal notice provided with a conditional offer of employment
B. A notice provision in an electronic employment application.
C. A notice provision in a mailed offer letter.
D. A standalone notice document.

Answer: D

Explanation:
Under the Fair Credit Reporting Act (FCRA), employers are required to provide a clear and conspicuous disclosure in a standalone document before obtaining a consumer report (e.g., a background check) for employment purposes. This requirement ensures that the individual is fully aware that a consumer report will be obtained and consents to the process.

Requirements for a Sufficient Consumer Disclosure:

Clear and Conspicuous Disclosure:

Employers must inform the individual, in writing, that a consumer report may be obtained for employment purposes.

Standalone Document:

The disclosure must be provided in a separate document not combined with other materials, such as an employment application. This ensures the individual's attention is focused on the notice.

Written Authorization:

Employers must obtain written authorization from the individual before procuring the consumer report.

Explanation of Options:

A. A verbal notice provided with a conditional offer of employment:

Verbal notice is insufficient under FCRA, which requires a written, standalone disclosure.

B. A notice provision in an electronic employment application:

Embedding the disclosure in an employment application would not meet the FCRA requirement for a standalone document and could be legally invalid.

C. A notice provision in a mailed offer letter:

Including the disclosure in an offer letter does not satisfy the requirement for a separate, standalone document.

D. A standalone notice document:

This is the correct answer, as the FCRA explicitly requires the disclosure to be in a separate document to ensure clarity and compliance.

Reference from CIPP/US Materials:

FCRA Section 604(b) (15 U.S.C. § 1681b(b)): Requires a clear and conspicuous standalone disclosure before obtaining a consumer report for employment purposes.

IAPP CIPP/US Certification Textbook: Explains the FCRA requirements for employment-related consumer reports, including the disclosure and authorization process.

Question: 184

SCENARIO

Please use the following to answer the next question;

Jane is a U.S. citizen and a senior software engineer at California-based Jones Labs, a major software supplier to the U.S. Department of Defense and other U.S. federal agencies Jane's manager, Patrick, is a French citizen who has been living in California for over a decade. Patrick has recently begun to suspect that Jane is an insider secretly transmitting trade secrets to foreign intelligence. Unbeknownst to Patrick, the FBI has already received a hint from anonymous whistleblower, and jointly with the National Secunty Agency is investigating Jane's possible implication in a sophisticated foreign espionage campaign

Ever since the pandemic. Jane has been working from home. To complete her daily tasks she uses her corporate laptop, which after each togin conspicuously provides notice that the equipment belongs to Jones Labs and may be monitored according to the enacted privacy policy and employment handbook Jane also has a corporate mobile phone that she uses strictly for business, the terms of which are defined in her employment contract and elaborated upon in her employee handbook. Both the privacy policy and the employee handbook are revised annually by a reputable California law firm specializing in privacy law. Jane also has a personal iPhone that she uses for private purposes only.

Jones Labs has its primary data center in San Francisco, which is managed internally by Jones Labs engineers The secondary data center, managed by Amazon AWS. is physically located in the UK for disaster recovery purposes. Jones Labs' mobile devices backup is managed by a mid-sized mobile delense company located in Denver, which physically stores the data in Canada to reduce costs. Jones Labs MS Office documents are securely stored in a Microsoft Office 365 data

When storing Jane's fingerprint for remote authentication. Jones Labs should consider legality issues under which of the following9

A. The Privacy Rule of the HITECH Act.
B. The California loT Security Law (SB 327).
C. The applicable state law such as Illinois BIPA
D. The federal Genetic Information Nondiscrimination Act (GINA).

Answer: C

Explanation:

When storing biometric data, such as fingerprints, organizations in the U.S. must comply with statespecific biometric privacy laws if they operate in states that regulate biometric information. The most prominent of these laws is the Illinois Biometric Information Privacy Act (BIPA), but similar laws also exist or are developing in other states, such as Texas and Washington.

Key Considerations for Storing Biometric Data:

Illinois Biometric Information Privacy Act (BIPA):

BIPA (740 ILCS 14) is a leading and highly influential state law regulating the collection, storage, and use of biometric information. It requires organizations to:

Obtain informed, written consent before collecting biometric data.

Establish a publicly available policy governing the retention and destruction of biometric data.

Use a reasonable standard of care to protect biometric data from unauthorized access or use. Prohibit the sale or transfer of biometric data without consent.

California and Biometric Data:

While California's California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA) provide general protections for personal information, including biometric data, they do not have the specific consent and handling requirements that BIPA does. Nevertheless, California residents have rights related to access, deletion, and the sale of biometric information.

Explanation of Options:

A. The Privacy Rule of the HITECH Act:

The HITECH Act applies to the protection of protected health information (PHI) under HIPAA. While the Privacy Rule regulates healthcare-related information, it does not apply to Jane’s biometric data used for remote authentication unless it is tied to PHI. This scenario is unrelated to healthcare, so this answer is incorrect.

B. The California IoT Security Law (SB 327):

California's IoT Security Law primarily focuses on ensuring security requirements for connected devices. It does not regulate the collection or storage of biometric information. This is not relevant to the question.

C. The applicable state law such as Illinois BIPA:

This is correct. State biometric privacy laws, such as Illinois BIPA, explicitly govern the collection, storage, and use of biometric data like fingerprints. Organizations like Jones Labs must ensure compliance with such laws, including obtaining consent and properly securing and destroying biometric information.

D. The federal Genetic Information Nondiscrimination Act (GINA):

GINA prohibits discrimination based on genetic information in employment and health insurance. However, it does not regulate the storage of biometric data like fingerprints. This is not applicable to this scenario.

Best Practices for Compliance:

Jones Labs should:

Understand the applicable state biometric laws: If Jane resides in Illinois or other states with biometric laws, Jones Labs must comply with those specific legal requirements.

Obtain informed consent: Ensure that employees like Jane sign a written consent form before storing their

fingerprints for authentication.
Secure biometric data: Use strong encryption and other security measures to protect the biometric information.
Define retention and destruction policies: Clearly establish how long biometric data will be stored and how it will be destroyed after its purpose is fulfilled.
Reference from CIPP/US Materials:
Illinois Biometric Information Privacy Act (BIPA): Sets the standard for biometric privacy regulations in the U.S.
California Consumer Privacy Act (CCPA): Protects personal information but does not specifically regulate biometric data like fingerprints with the same rigor as BIPA.
IAPP CIPP/US Certification Textbook: Discusses the emergence of state-specific biometric privacy laws and their applicability in different scenarios.

Question: 185

SCENARIO
Please use the following to answer the next question;
Jane is a U.S. citizen and a senior software engineer at California-based Jones Labs, a major software supplier to the U.S. Department of Defense and other U.S. federal agencies Jane's manager, Patrick, is a French citizen who has been living in California for over a decade. Patrick has recently begun to suspect that Jane is an insider secretly transmitting trade secrets to foreign intelligence. Unbeknownst to Patrick, the FBI has already received a hint from anonymous whistleblower, and jointly with the National Secunty Agency is investigating Jane's possible implication in a sophisticated foreign espionage campaign
Ever since the pandemic. Jane has been working from home. To complete her daily tasks she uses her corporate laptop, which after each togin conspicuously provides notice that the equipment belongs to Jones Labs and may be monitored according to the enacted privacy policy and employment handbook Jane also has a corporate mobile phone that she uses strictly for business, the terms of which are defined in her employment contract and elaborated upon in her employee handbook. Both the privacy policy and the employee handbook are revised annually by a reputable California law firm specializing in privacy law. Jane also has a personal iPhone that she uses for private purposes only.
Jones Labs has its primary data center in San Francisco, which is managed internally by Jones Labs engineers The secondary data center, managed by Amazon AWS. is physically located in the UK for disaster recovery purposes. Jones Labs' mobile devices backup is managed by a mid-sized mobile delense company located in Denver, which physically stores the data in Canada to reduce costs. Jones Labs MS Office documents are securely stored in a Microsoft Office 365 data Under Section 702 of F1S
A. the NSA may do which of the following without a Foreign Intelligence Surveillance Court warrant? A. Compel AWS to disclose Jane's email communications with a Taiwanese national residing in Taiwan.
B. Compel AWS to disclose email communications between two Chinese nationals residing in the EU. C. Compel Microsoft to disclose Patnck's Skype calls with a Brazilian national living in Peru.
D. Compel Jane to disclose the PIN code for her corporate mobile phone.

Answer: B

Explanation:
Under Section 702 of the Foreign Intelligence Surveillance Act (FISA), the National Security Agency (NSA) is authorized to collect and analyze communications of non-U.S. persons located outside the United States for foreign intelligence purposes. Section 702 allows the NSA to compel U.S.-based service providers, such as AWS or Microsoft, to provide access to data without requiring a warrant from the Foreign Intelligence Surveillance

Court (FISC) if certain criteria are met.

Key Aspects of Section 702:

Scope of Surveillance:

Section 702 applies to non-U.S. persons located outside the United States. It cannot be used to target U.S. citizens or individuals located within the United States, even if they communicate with non-U.S. persons.

Provider Obligations:

The NSA can compel U.S.-based service providers (e.g., AWS, Microsoft) to disclose information about communications involving foreign individuals if the data is relevant to foreign intelligence purposes.

Explanation of the Options:

A. Compel AWS to disclose Jane's email communications with a Taiwanese national residing in Taiwan: Incorrect. Jane is a U.S. citizen, and Section 702 cannot be used to directly target U.S. persons or their communications, even if the other party in the communication is a non-U.S. person.

B. Compel AWS to disclose email communications between two Chinese nationals residing in the EU: Correct. Section 702 allows the NSA to target non-U.S. persons located outside the U.S. without a warrant, even if their communications are hosted by a U.S.-based service provider like AWS. This scenario falls directly under the scope of Section 702.

C. Compel Microsoft to disclose Patrick's Skype calls with a Brazilian national living in Peru: Incorrect. Patrick is a U.S. resident, even though he is a French citizen. Section 702 cannot be used to target individuals who are lawfully residing in the United States.

D. Compel Jane to disclose the PIN code for her corporate mobile phone:

Incorrect. Section 702 applies to electronic communications data held by service providers, not to individuals. Compelling an individual to disclose a PIN code would require a different legal authority, such as a court-issued subpoena or warrant.

Legal Framework:

Section 702 of FISA: Provides the NSA with the authority to compel U.S.-based service providers to assist in collecting data on non-U.S. persons located outside the U.S. for foreign intelligence purposes.

Targeting Limitations: Section 702 cannot be used to intentionally target U.S. persons or anyone located within the United States.

Service Providers: Examples include U.S.-based companies such as Amazon AWS, Microsoft, and Google.

Practical Considerations for Jones Labs:

Jones Labs should be aware that:

Data stored with U.S.-based providers (even if located in the EU) may still be subject to Section 702 requests.

International data transfer compliance may require careful consideration of Standard Contractual Clauses (SCCs) or other safeguards to align with EU privacy regulations, such as the GDPR, in light of the extraterritorial nature of U.S. surveillance laws.

Reference from CIPP/US Materials:

FISA Section 702 (50 U.S.C. § 1881a): Outlines the legal authority for targeting non-U.S. persons located outside the United States.

IAPP CIPP/US Certification Textbook: Discusses Section 702 and its implications for U.S.-based service providers handling international data.

Schrems II Decision: Highlights conflicts between U.S. surveillance laws and EU privacy laws, particularly for data stored by U.S. companies overseas.

Question: 186

According to the Family Educational Rights and Privacy Act (FERPA). when can a school disclose records without a student's consent?

A. If the disclosure Is not to be conducted through email to the third party
B. If the disclosure would not reveal a student's student identification number
C. If the disclosure is made to practitioners who are involved in a student's hearth care.
D. If the disclosure is for the purpose of providing transcripts to a school where a student intends to enroll.

Answer: D

Explanation:
The Family Educational Rights and Privacy Act (FERPA) is a federal law that protects the privacy of student education records. FERPA generally requires that schools obtain written consent from students (or their parents if the student is a minor) before disclosing personally identifiable information from education records. However, FERPA allows specific exceptions where disclosures can be made without consent.
One of these exceptions is when a school discloses education records to another school where the student seeks or intends to enroll. This allows educational institutions to share information for legitimate educational purposes, such as transferring transcripts between schools when a student moves or applies for enrollment elsewhere.
Explanation of Options:
A. If the disclosure is not to be conducted through email to the third party:
FERPA does not prohibit disclosures via email as long as the recipient is authorized and the disclosure meets FERPA requirements. The medium of disclosure is not a determining factor.
B. If the disclosure would not reveal a student's student identification number:
FERPA restricts the disclosure of personally identifiable information but does not specifically regulate disclosures based on whether a student ID number is included unless the number itself compromises the student's privacy.
C. If the disclosure is made to practitioners who are involved in a student's health care:
FERPA does not specifically provide an exception for health care practitioners unless the disclosure falls under the "health and safety emergency" exception, which does not apply to general health care.
D. If the disclosure is for the purpose of providing transcripts to a school where a student intends to enroll:
This is correct and aligns with one of the exceptions outlined in FERPA. Schools are permitted to share student records with other educational institutions where a student seeks or intends to enroll without requiring consent.
Reference from CIPP/US Materials:
FERPA (20 U.S.C. § 1232g): Governs the disclosure of student education records and details specific exceptions to the consent requirement.
IAPP CIPP/US Certification Textbook: Explains FERPA's consent requirements and exceptions, including disclosures for enrollment purposes.

Question: 187

A software company wants to use web scraping to collect personal data from professional networking websites in order to train an artificial intelligence program to evaluate Job applications. The company has identified several actions for limiting their potential legal liability regarding affected data subjects and professional networking websites. Which of the following would be the least effective action for helping them do this?

A. Following the terms of use posted on professional networking websites that are scraped.
B. Adding a notice to the company website's terms of use disclosing the use of web scraping
C. Limiting the amount of the personally identifiable information they collect

D. Decertifying the scraped data before selling it to any third parties.

Answer: B

Explanation:

Web scraping to collect personal data can pose significant legal and ethical risks, particularly when it involves professional networking sites or other platforms where terms of service (ToS) explicitly prohibit such activity. To limit liability, the software company must take proactive measures to comply with applicable laws (such as privacy laws) and contractual obligations (e.g., terms of use on the scraped websites).

Adding a notice to the company website's terms of use would be the least effective action, as it does not address the legal and ethical issues associated with scraping data from third-party websites. Simply adding a notice about the company's use of scraping does not mitigate liability for violating the ToS of professional networking websites or violating privacy rights under laws like the GDPR or CCPA.

Explanation of Options:

A. Following the terms of use posted on professional networking websites that are scraped:

This is one of the most effective ways to limit legal liability. Violating ToS can result in lawsuits or legal penalties, so adhering to them is critical.

B. Adding a notice to the company website's terms of use disclosing the use of web scraping: This is the least effective action. Including this notice on the company's own website does not address potential violations of third-party website ToS or the privacy rights of affected individuals. C. Limiting the amount of the personally identifiable information they collect: Minimizing the amount of data collected aligns with data protection principles, such as data minimization under the GDPR, and can reduce privacy risks.

D. Deidentifying the scraped data before selling it to any third parties:

Deidentifying or anonymizing data is a critical step for reducing legal liability and complying with privacy laws. However, the company should also ensure that the deidentification is robust and irreversible.

Reference from CIPP/US Materials:

GDPR Article 5: Establishes principles such as data minimization and accountability for data processing.

IAPP CIPP/US Certification Textbook: Highlights the risks of web scraping and the importance of adhering to contractual obligations and privacy laws.

Question: 188

Due to cookie deprecation, businesses will be required to simplify their tracking practices by doing what?

A. Ensuring only registered users are tracked.
B. Running analytics only in dedicated sandboxes
C. Purging existing IDs that identify visitors by browser.
D. Deleting their existing data sets of any third-party cookies

Answer: D

Explanation:

With the impending deprecation of third-party cookies, businesses must simplify their tracking practices and shift to more privacy-conscious technologies. Third-party cookies are being phased out by major web browsers, such as Google Chrome, to improve user privacy and reduce cross-site tracking.

One of the most critical actions businesses need to take is deleting existing data sets of third-party cookies, as they will soon become obsolete. This action ensures compliance with emerging privacy standards and helps organizations transition to alternative methods of tracking, such as first-party data collection or consent-

based tracking mechanisms.

Explanation of Options:

A. Ensuring only registered users are tracked:

While focusing on registered users might simplify tracking, it does not address the broader privacy concerns surrounding third-party cookies.

B. Running analytics only in dedicated sandboxes:

Sandboxing analytics tools may enhance security, but it does not directly relate to the transition away from third-party cookies.

C. Purging existing IDs that identify visitors by browser:

Browser IDs are not inherently tied to third-party cookies. Purging them might be part of broader privacy compliance efforts but is not the primary issue with cookie deprecation.

D. Deleting their existing data sets of any third-party cookies:

This is correct. Deleting existing third-party cookie data is a necessary step to align with the move away from third-party cookies, ensuring businesses are prepared for the shift to new tracking technologies.

Reference from CIPP/US Materials:

IAPP CIPP/US Certification Textbook: Discusses cookie deprecation and the shift towards first-party data and privacy-conscious tracking.

California Consumer Privacy Act (CCPA): Regulates the use of cookies and other tracking technologies, emphasizing user consent and transparency.

Question: 189

The Clarifying Lawful Overseas Use of Data (CLOUD) Act is primarily intended to do which of the following?

A. Codify a treaty with the EU that permits the cross-border transfer of personal information from the EU to the United States in compliance with the General Data Protection Regulation (GDPR).

B. Update the legal mechanisms through which federal law enforcement may obtain data that service providers maintain in a foreign country

C. Establish baseline pnvacy obligations that US companies must comply with for personal information, even if stored in a foreign country

D. Prohibit foreign companies from using the personal Information of US. citizens without their consent

Answer: B

Explanation:

The Clarifying Lawful Overseas Use of Data (CLOUD) Act, enacted in 2018, updates the legal framework for federal law enforcement to access electronic data held by U.S. service providers, even when the data is stored outside the United States. The act resolves jurisdictional issues that arise in cross-border data requests and facilitates international cooperation for law enforcement purposes. Key Provisions of the CLOUD Act:

Data Access for Law Enforcement:

The CLOUD Act allows U.S. federal law enforcement to compel U.S.-based service providers (e.g., Microsoft, Google) to provide access to data stored abroad using a valid warrant or subpoena, provided the request complies with applicable laws.

International Data Sharing Agreements:

The CLOUD Act enables the U.S. to establish bilateral agreements with other countries to streamline access to data for law enforcement purposes. These agreements ensure that U.S. and foreign law enforcement can access data without violating each other's sovereignty or privacy laws.

Conflict with Foreign Laws:

The act includes mechanisms for providers to challenge data requests that conflict with the laws of the country where the data is stored, providing safeguards for compliance with foreign privacy laws like the General Data Protection Regulation (GDPR).

Explanation of Options:

A. Codify a treaty with the EU that permits the cross-border transfer of personal information from the EU to the United States in compliance with the GDPR:

This is incorrect. The CLOUD Act is not specific to the EU or GDPR compliance. Instead, it focuses on law enforcement access to data stored abroad.

B. Update the legal mechanisms through which federal law enforcement may obtain data that service providers maintain in a foreign country:

This is correct. The CLOUD Act directly addresses law enforcement's ability to compel data access from U.S. providers, regardless of the data's physical location.

C. Establish baseline privacy obligations that U.S. companies must comply with for personal information, even if stored in a foreign country:

This is incorrect. The CLOUD Act is focused on law enforcement access to data, not privacy obligations for companies.

D. Prohibit foreign companies from using the personal information of U.S. citizens without their consent:

This is incorrect. The CLOUD Act does not regulate foreign companies or impose consent requirements for using personal information.

Reference from CIPP/US Materials:

CLOUD Act (18 U.S.C. § 2713): Establishes legal mechanisms for cross-border data access and international agreements.

IAPP CIPP/US Certification Textbook: Discusses the CLOUD Act's impact on cross-border data requests and its interaction with global privacy laws.

Question: 190

Which of the following most accurately describes the regulatory status ot pandemic contact-tracing apps in the United States?

A. Contact tracing is covered exclusively under the Health Insurance Portability and Accountability Act (HIPAA).

B. Contact tracing is regulated by the U.S. Centers for Disease Control and Prevention (CDC).

C. Contact tracing is subject to a patchwork of federal and state privacy laws

D. Contact tracing is not regulated in the United States.

Answer: C

Explanation:

In the United States, pandemic contact-tracing apps are regulated under a patchwork of federal and state privacy laws, rather than a single, comprehensive framework. Contact-tracing initiatives often involve the collection and processing of sensitive data, including location and health information, which may fall under different legal regimes depending on the jurisdiction and type of data.

Key Regulations Affecting Contact-Tracing Apps:

State Privacy Laws:

States such as California (via the California Consumer Privacy Act - CCPA) and others have privacy

laws that may apply to contact-tracing apps, particularly when personal data is collected or shared. State-level health privacy laws may also govern how health-related data is collected and used.

HIPAA:

HIPAA (Health Insurance Portability and Accountability Act) applies only if the app is used by or on behalf of a covered entity (e.g., healthcare providers or health plans). If the app is operated by a private company without a connection to a HIPAA-covered entity, HIPAA likely does not apply. Federal Guidance:

The Federal Trade Commission (FTC) enforces general privacy protections under Section 5 of the FTC Act, which prohibits unfair or deceptive practices.

The FTC has also issued guidance on privacy considerations for health-related apps.

Other Federal and Sector-Specific Laws:

If the app collects health-related data, it could also trigger obligations under laws like the Americans with Disabilities Act (ADA) or sector-specific rules.

Explanation of Options:

A. Contact tracing is covered exclusively under the Health Insurance Portability and Accountability Act (HIPAA):

This is incorrect. HIPAA applies only to covered entities and their business associates, not broadly to all contact-tracing apps or initiatives.

B. Contact tracing is regulated by the U.S. Centers for Disease Control and Prevention (CDC):

This is incorrect. While the CDC provides guidance and recommendations for public health, it does not have regulatory authority over contact-tracing apps.

C. Contact tracing is subject to a patchwork of federal and state privacy laws:

This is correct. Contact-tracing apps in the U.S. are governed by various federal, state, and sectorspecific laws, creating a patchwork regulatory framework.

D. Contact tracing is not regulated in the United States:

This is incorrect. While there is no single regulatory framework for contact tracing, the practice is subject to multiple federal and state laws.

Reference from CIPP/US Materials:

IAPP CIPP/US Certification Textbook: Discusses the application of HIPAA, state privacy laws, and federal regulations to health-related technologies, including contact-tracing apps.

FTC Guidance on Health Apps: Details privacy considerations for app developers handling health- related data.

Question: 191

Which power was NOT granted to the California Privacy Protection Agency by the California Privacy Rights Act (CPRA)?

A. Adopting and updating CCPA regulations
B. Investigating possible violations of the CCPA on the agency's own initiative.
C. Overriding decisions of the Attorney General regarding CCPA enforcement
D. Imposing administrative fines for violations of the CCPA

Answer: C

Explanation:

The California Privacy Rights Act (CPRA), which amends the California Consumer Privacy Act (CCPA), created the California Privacy Protection Agency (CPPA). This agency has been granted significant

authority to regulate and enforce California privacy laws, but it does not have the authority to override decisions made by the California Attorney General regarding CCPA enforcement.

Powers Granted to the CPPA by the CPRA:

Adopting and Updating CCPA Regulations:

The CPPA has rulemaking authority, meaning it can adopt, amend, and update CCPA regulations to clarify obligations under the law.

This is explicitly stated in the CPRA.

Investigating Violations:

The CPPA can independently investigate potential violations of the CCPA, even without a complaint from a consumer.

Imposing Administrative Fines:

The CPPA has the authority to impose administrative fines for violations of the CCPA, which is critical for enforcing compliance.

Explanation of Option C:

While the CPPA has broad regulatory and enforcement powers, it cannot override decisions made by the Attorney General. The Attorney General retains certain oversight functions, particularly in transitioning enforcement authority to the CPPA. The CPPA's role is independent and complementary to that of the Attorney General, not one of supremacy.

Reference from CIPP/US Materials:

California Privacy Rights Act (CPRA): Specifies the creation, powers, and responsibilities of the CPPA. IAPP CIPP/US Certification Textbook: Discusses the CPPA's rulemaking and enforcement authority.

Question: 192

Which of the following data elements is most likely to be subject to comprehensive state data security and privacy laws?

A. Account holders' social security numbers, maintained by a bank.
B. Users' sexual orientations, maintained by a social media website
C. Individual drivers' license numbers, maintained by a state agency.
D. Contact details of individuals who report emergencies, maintained by local authorities

Answer: A

Explanation:

Social security numbers (SSNs) are one of the most sensitive types of personally identifiable information (PII) and are subject to comprehensive data security and privacy laws at both the federal and state levels. Banks, as financial institutions, are subject to strict regulations under laws like the Gramm-Leach-Bliley Act (GLBA) and state privacy laws regarding the safeguarding of sensitive data like SSNs.

Why Social Security Numbers are Most Likely to Be Covered:

SSNs are a high-value target for identity theft, making their protection a focus of numerous privacy and data security laws.

Federal laws like GLBA and the Fair Credit Reporting Act (FCRA) impose strict data security requirements on financial institutions.

State laws, such as those in California, often require businesses to protect SSNs and notify individuals in the event of a breach involving sensitive information.

Explanation of Options:

A. Account holders' social security numbers, maintained by a bank:

This is correct because SSNs are consistently protected under comprehensive laws at both the federal and state levels.

B. Users' sexual orientations, maintained by a social media website:

While sexual orientation may be considered sensitive data under certain laws (e.g., GDPR in the EU), U.S. privacy laws do not consistently regulate this information.

C. Individual drivers' license numbers, maintained by a state agency:

While some states regulate drivers' license data, this information is not comprehensively covered under state privacy laws.

D. Contact details of individuals who report emergencies, maintained by local authorities:

This information is regulated in limited circumstances (e.g., Freedom of Information Act or public records laws) but is not subject to comprehensive state privacy laws.

Reference from CIPP/US Materials:

GLBA and FCRA: Highlight the importance of safeguarding sensitive financial information such as SSNs.

State Data Breach Notification Laws: Many states explicitly list SSNs as a protected data element.

Question: 193

More than half of U S. states require telemarketers to do which of the following?

A. Identify themselves at the beginning of a call
B. Obtain written consent from potential customers
C. Register with the state before conducting business.
D. Provide written contracts for customer transactions

Answer: C

Explanation:

More than half of U.S. states require telemarketers to register with the state before conducting telemarketing activities. These registration requirements are part of state-level consumer protection laws aimed at regulating telemarketing practices to prevent fraud and abusive practices.

Why State Registration is Required:

Telemarketing registration requirements allow states to monitor and regulate telemarketers operating within their jurisdiction.

Registration ensures that telemarketers comply with state-specific rules, such as "Do Not Call" list regulations or prohibitions on deceptive practices.

States like Florida, New York, and California are examples of jurisdictions with telemarketing registration laws.

Explanation of Options:

A. Identify themselves at the beginning of a call:

This is a requirement under the Federal Trade Commission's (FTC) Telemarketing Sales Rule (TSR), but it is not unique to state requirements.

B. Obtain written consent from potential customers:

While obtaining consent may be required in specific situations (e.g., under the Telephone Consumer Protection Act - TCPA for autodialed calls), it is not the most common state-level requirement.

C. Register with the state before conducting business:

This is correct. Registration with the state is one of the most common requirements for telemarketers under state laws.

D. Provide written contracts for customer transactions:

Written contracts are not universally required for telemarketing; this depends on the type of product or service being sold.

Reference from CIPP/US Materials:

FTC Telemarketing Sales Rule (TSR): Covers general telemarketing rules but acknowledges additional state-specific requirements, such as registration.

State Telemarketing Laws: Examples include Florida's Telemarketing Act, which requires state registration.

Question: 194

In the US, II is a best practice (and in some states a requirement) to conduct a data protection assessment in which instance?

A. When a background check is used as part of the hiring process
B. When any information is processed by a corporation.
C. When trade secrets are shared with a third party.
D. When technology is used to monitor employees.

Answer: D

Explanation:

In the U.S., it is a best practice and, in some states, a requirement to conduct a data protection impact assessment (DPIA) or similar evaluation when technology is used to monitor employees. This practice aligns with privacy principles aimed at ensuring that monitoring practices are proportionate, necessary, and lawful, while minimizing potential harm to employees' privacy.

Why Conduct a DPIA When Monitoring Employees?

Employee Privacy Risks: Monitoring technologies, such as video surveillance, keystroke logging, or location tracking, can significantly impact employees' privacy. Assessments help evaluate these risks and ensure compliance with applicable privacy laws.

State-Specific Requirements: Some states, like California under the California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA), require businesses to implement privacy safeguards, including assessments for high-risk activities involving sensitive data.

Best Practices: Even when not legally required, conducting a DPIA demonstrates accountability and helps mitigate risks associated with employee privacy violations.

Explanation of Options:

A. When a background check is used as part of the hiring process:

While background checks involve sensitive data and compliance with laws like the Fair Credit Reporting Act (FCRA), a DPIA is not typically required for this process. Instead, consent and notice are emphasized.

B. When any information is processed by a corporation:

This is too broad. DPIAs are generally reserved for high-risk activities involving sensitive data or technologies, not for all data processing activities.

C. When trade secrets are shared with a third party:

Sharing trade secrets involves contractual and confidentiality measures, but it does not usually necessitate a data protection assessment unless personal data is also involved.

D. When technology is used to monitor employees:

This is correct. Monitoring employees with technology poses significant privacy risks, making it a best practice (and sometimes a requirement) to assess the impacts on privacy and ensure compliance with state and

federal laws.

Reference from CIPP/US Materials:

California Privacy Rights Act (CPRA): Introduces risk assessments for certain data processing activities.

IAPP CIPP/US Certification Textbook: Discusses privacy risks associated with employee monitoring and the importance of impact assessments.

Question: 195

What is the purpose of a cure provision in a stale data privacy law?

A. To allow a business a limited timeframe to fix alleged violations before facing enforcement.
B. To allow consumers a period of time to discover their data has been mishandled
C. To allow a state to initiate formal enforcement actions for a fixed time period.
D. To allow certain provisions of a law to expire after a defined time period

Answer: A

Explanation:

A cure provision in state data privacy laws gives businesses an opportunity to remediate violations of the law within a specified timeframe after receiving notice of the alleged violation. This provision is intended to promote compliance rather than immediately imposing penalties or enforcement actions.

Key Aspects of Cure Provisions:

Notice and Cure Period:

Businesses are given a timeframe (e.g., 30 days) to address the alleged violation before formal enforcement actions are taken by state authorities.

Encouraging Compliance:

Cure provisions incentivize businesses to implement corrective actions and ensure compliance without incurring fines or penalties for minor or first-time violations.

State-Specific Examples:

The California Consumer Privacy Act (CCPA) initially included a 30-day cure provision, though it was later limited under the California Privacy Rights Act (CPRA).

Other state laws, such as Virginia's Consumer Data Protection Act (VCDPA), also include cure provisions.

Explanation of Options:

A. To allow a business a limited timeframe to fix alleged violations before facing enforcement:

This is correct. Cure provisions are specifically designed to give businesses an opportunity to address violations before facing enforcement actions.

B. To allow consumers a period of time to discover their data has been mishandled:

This describes consumer rights related to data breach notifications, not cure provisions.

C. To allow a state to initiate formal enforcement actions for a fixed time period:

Cure provisions delay enforcement actions rather than initiate them.

D. To allow certain provisions of a law to expire after a defined time period:

This describes sunset provisions, not cure provisions.

Reference from CIPP/US Materials:

CCPA and CPRA: Discuss the cure provisions and their role in enforcement.

IAPP CIPP/US Certification Textbook: Highlights the purpose and impact of cure provisions in state privacy laws.