EXAMTOPICS

-Expert Verified, Online, **Free**.



CERTIFICATION TEST

-CertificationTest.net - Cheap & Quality Resources With Best Support

Question #1 *Topic 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

Suggested Answer: *C*

Community vote distribution

C (100%)

Bhimesh Most Recent 1 year, 11 months ago

Courts have two different types of jurisdiction. Personal jurisdiction refers to the court's authority over a person being sued or charged with a crime. Subject matter jurisdiction refers to the court's authority to hear cases on a particular area of the law.

upvoted 1 times

Qwamer 3 years, 2 months ago

Private-Sector Privacy(2020): Jurisdiction: The authority of a court to hear a particular case. A court must have jurisdiction over both the type of dispute (“subject matter jurisdiction”) and the parties (“personal jurisdiction”). Government agencies have jurisdictional limits also.

upvoted 4 times

Question #2 *Topic 1*

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

Suggested Answer: *B*

Community vote distribution

B (100%)

Bhimesh Most Recent 1 year, 11 months ago

The NAI is one example of an industry self-regulatory framework, but there are others that are broad in nature or that apply to specific industries. For example, the Better Business Bureau operates a self-regulatory program for organizations that advertise to children.

upvoted 1 times

Bhimesh 1 year, 11 months ago

The Network Advertising Initiative (NAI) is a self-regulatory program focused on digital marketing. Businesses involved in the distribution of online advertising participate in NAI as members, and NAI claims that almost every Internet ad displayed in the United States uses the technology of one of its members. The NAI publishes a code of conduct that contains detailed requirements describing how its members must provide notice of their privacy practices, offers consumers the ability to opt out of information processing, and describes how they must implement procedures for data security, transfer, and quality. The NAI conducts compliance reviews of its members and has the authority to sanction them and refer noncompliant companies to the Federal Trade Commission or other regulators for possible enforcement action.

upvoted 1 times

Question #3 *Topic 1*

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

Suggested Answer: *A*

Community vote distribution

C (100%)

Bhimesh Most Recent 1 year, 11 months ago

For enforcement under Section 5 of the FTC Act or state UDAP laws, self-regulation only occurs at the quasi-legislative stage (i.e., voluntary industry rulemaking). A company writes its own privacy policy, or an industry group drafts a code of conduct that companies agree to follow. Under Section 5, the FTC can then decide whether to bring an enforcement action, and adjudication can occur in front of an ALJ, with appeal to federal court. The NAI(self-regulation) publishes a code of conduct that contains detailed requirements describing how its members must provide notice of their privacy practices separation-of-powers components: legislation, enforcement and adjudication. Enforcement refers to the question of who should initiate enforcement actions. Adjudication refers to the question of who should decide whether a company has violated the privacy rules, and with what penalties

upvoted 1 times

Romeokton 2 years, 1 month ago

Definitely C

upvoted 1 times

smp175 2 years, 8 months ago

See IAPP book, Section 3.10, paragraph 2.

upvoted 2 times

Question #4 *Topic 1*

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

Suggested Answer: *A*

Community vote distribution

A (100%)

Bhimesh 1 year, 11 months ago

Selected Answer: A

Five priority areas listed by the FTC in its 2012 report Do Not Track industry has made significant progress in implementing Do Not Track. The browser vendors have developed tools that consumers can use to signal that they do not want to be tracked Mobile The Commission calls on companies providing mobile services to work toward improved privacy protections, including the development of short, meaningful disclosures.

upvoted 1 times

Bhimesh 1 year, 11 months ago

Five priority areas listed by the FTC in its 2012 report Do Not Track industry has made significant progress in implementing Do Not Track. The browser vendors have developed tools that consumers can use to signal that they do not want to be tracked Mobile The Commission calls on companies providing mobile services to work toward improved privacy protections, including the development of short, meaningful disclosures.Data Brokers: To address the invisibility of, and consumers' lack of control over, data brokers' collection and use of consumer information, the Commission supports targeted legislation Large Platform Providers: To the extent that large platforms, such as Internet Service Providers, operating systems, browsers, and social media seek, to comprehensively track consumers' online activities, it raises heightened privacy concerns. Promoting Enforceable Self-Regulatory Codes: The Department of Commerce, with the support of key industry stakeholders, is undertaking a project to facilitate the development of sector-specific codes of conduct.

upvoted 1 times

Bhimesh **Most Recent** 1 year, 11 months ago

Data Brokers: To address the invisibility of, and consumers' lack of control over, data brokers' collection and use of consumer information, the Commission supports targeted legislation Large Platform Providers: To the extent that large platforms, such as Internet Service Providers, operating systems, browsers, and social media seek, to comprehensively track consumers' online activities, it raises heightened privacy concerns. Promoting Enforceable Self-Regulatory Codes: The Department of Commerce, with the support of key industry stakeholders, is undertaking a project to facilitate the development of sector-specific codes of conduct.

upvoted 1 times

Question #5 *Topic 1*

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

A. The 1974 Privacy Act

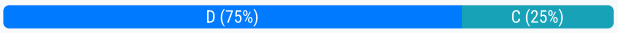
B. Common law principles

C. European Union Directive

D. Traditional fair information practices

Suggested Answer: *C*

Community vote distribution



impchoi Highly Voted 3 years, 3 months ago

The IAPP book states: "he 2012 White House Report contains a preface signed by President Obama and defines the “Consumer Privacy Bill of Rights” based on traditional fair information practices (FIPs)."

upvoted 7 times

Bhimesh Most Recent 1 year, 11 months ago

D - Traditional fair information practices

upvoted 1 times

Bhimesh 2 years, 1 month ago

C - Traditional fair information practices - Obama administration issued a report proposing a Consumer Privacy Bill of Rights. Derived from traditional fair information practices, this document aimed to empower consumers by giving them more control over how businesses handle their data, by restricting collection of their personal data, and by ensuring that their data will only be used for the agreed purpose. The Consumer Privacy Bill of Rights doesn't have the force of law, and compliance is voluntary. It formed the backbone for a proposed approach to new privacy legislation from the Obama administration in 2015, but that legislation stalled. Subsequent federal legislation derived from these principles have continued to flounder in Congress. After Obama's term in office ended, the Consumer Privacy Bill of Rights was removed from the White House website by the new administration. (The 2012 White House Report contains a preface signed by President Obama and define the “Consumer Privacy Bill of Rights” based on traditional fair information practices (FIPs).)Correction - D - Traditional fair information practices

upvoted 1 times

Bhimesh 2 years, 1 month ago

C - Traditional fair information practices - Obama administration issued a report proposing a Consumer Privacy Bill of Rights. Derived from traditional fair information practices, this document aimed to empower consumers by giving them more control over how businesses handle their data, by restricting collection of their personal data, and by ensuring that their data will only be used for the agreed purpose. The Consumer Privacy Bill of Rights doesn't have the force of law, and compliance is voluntary. It formed the backbone for a proposed approach to new privacy legislation from the Obama administration in 2015, but that legislation stalled. Subsequent federal legislation derived from these principles have continued to flounder in Congress. After Obama's term in office ended, the Consumer Privacy Bill of Rights was removed from the White House website by the new administration. (The 2012 White House Report contains a preface signed by President Obama and define the “Consumer Privacy Bill of Rights” based on traditional fair information practices (FIPs).)

upvoted 1 times

Bhimesh 1 year, 11 months ago

Correction - D - Traditional fair information practices

upvoted 1 times

IT_Dude_Err405 2 years, 5 months ago

Google Bard

upvoted 1 times

PrivacyICU 2 years, 6 months ago

It's D since that's what the government briefings say and the IAPP book reads. FIPPs (1970's and 1980s) existed long before the EU Data Protection Directive (1995) did.

upvoted 2 times

Savaage 2 years, 11 months ago

According to the IAPP book, it should be D as well as other sources including Nimo 53rd Edition Publication

upvoted 2 times

Supp2023 3 years ago

Option C "European Union Directive" is actually a valid answer, as the Consumer Privacy Bill of Rights was partially inspired by the European Union's Data Protection Directive. Therefore, both options C and D could be considered correct.

upvoted 1 times

Lupey 3 years ago

This is an incorrect answer. The correct answer is D.

upvoted 2 times

Question #6 *Topic 1*

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

Suggested Answer: *A*

Community vote distribution

A (100%)

Bhimesh 1 year, 11 months ago

Selected Answer: A

Consent Decrees A consent decree is a judgment entered by consent of the parties whereby the defendant agrees to stop alleged illegal activity, typically without admitting guilt or wrongdoing.[8] This legal document is approved by a judge and formalizes an agreement reached between a federal (or state) agency and an adverse party. The consent decree describes the actions the defendant will take, and the decree itself may be subject to a public comment period. Once approved, the consent decree has the efect of a court decision.

upvoted 1 times

Bhimesh 1 year, 11 months ago

Consent Decrees A consent decree is a judgment entered by consent of the parties whereby the defendant agrees to stop alleged illegal activity, typically without admitting guilt or wrongdoing.[8] This legal document is approved by a judge and formalizes an agreement reached between a federal (or state) agency and an adverse party. The consent decree describes the actions the defendant will take, and the decree itself may be subject to a public comment period. Once approved, the consent decree has the efect of a court decision.Consent Decree A judgment entered by consent of the parties. Typically, the defendant agrees to stop alleged illegal activity and pay a fine, without admitting guilt or wrongdoing. This legal document is approved by a judge and formalizes an agreement reached between a U.S. federal or state agency and an adverse party.

upvoted 1 times

Bhimesh **Most Recent** 1 year, 11 months ago

Consent Decree A judgment entered by consent of the parties. Typically, the defendant agrees to stop alleged illegal activity and pay a fine, without admitting guilt or wrongdoing. This legal document is approved by a judge and formalizes an agreement reached between a U.S. federal or state agency and an adverse party.

upvoted 1 times

Question #7 *Topic 1*

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

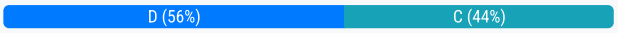
B. Implied consent

C. Opt-in

D. Opt-out

Suggested Answer: *B*

Community vote distribution



mab487 Most Recent 1 year, 8 months ago
The answer is definitely D
upvoted 1 times

Bhimesh 1 year, 11 months ago
What type of legal choice DOES NOT notice provide? The term opt-in means an affirmative indication of choice based on an express act of the person giving the consent. For example, a person opts in if they say yes when asked, "May we share your information?" Failure to answer would result in the information not being shared.
upvoted 4 times

PrivacyICU 2 years, 6 months ago
Answer is D. Opt-out is discussed in "Choice" in IAPP TEXT 2.3.2. Only 2 choices based on the text: Opt-In and Opt-Out. Consent is implied if you do not choose to opt-out, but that's not the question.
upvoted 3 times

Deatherage 2 years, 7 months ago
I say D because of the term used in the question "Legal Choice". B could work, but I wouldn't consider it the "legal" choice, it is more of the decision made by the website if you dont take action to refuse cookies.
upvoted 1 times

smp175 2 years, 8 months ago
Seems the answer should be C. C and D are mutually exclusive, and B and D are largely the same.
upvoted 1 times

Question #8 *Topic 1*

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 customers' 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 worries 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)

Suggested Answer: *C*

Community vote distribution



Bhimesh Most Recent 1 year, 11 months ago

C. It will increase the security of customers' personal information (PI)
upvoted 1 times

Question #9 *Topic 1*

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 customers' 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 worries 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

Suggested Answer: *A*

Community vote distribution

A (100%)

Bhimesh 1 year, 11 months ago

Selected Answer: A

Should be A...

A. Leaving the company susceptible to violations by setting unrealistic goals

upvoted 1 times

Bhimesh 1 year, 11 months ago

Should be A... A. Leaving the company susceptible to violations by setting unrealistic goalsIf the policy is not strict enough, then consumers,regulators, and the press may criticize the company for its failure to protect privacy. If a policy is too strict, then open-ended statements or overly ambitious security promises can result in legal penalties or reputational problems if the organization cannot satisfy its promises. An organization should not finalize a privacy policy without legal consultation followed by executive approval.

upvoted 1 times

Bhimesh **Most Recent** 1 year, 11 months ago

If the policy is not strict enough, then consumers,regulators, and the press may criticize the company for its failure to protect privacy. If a policy is too strict, then open-ended statements or overly ambitious security promises can result in legal penalties or reputational problems if the organization cannot satisfy its promises. An organization should not finalize a privacy policy without legal consultation followed by executive approval.

upvoted 1 times

Question #10 *Topic 1*

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 customers' 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 worries 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.

Suggested Answer: *B*

Community vote distribution



Bhimesh Most Recent 1 year, 11 months ago
Should be B B. The policy might not be implemented consistency across departments.
upvoted 1 times

Question #11 *Topic 1*

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 customers' 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 worries 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

Suggested Answer: *B*

Community vote distribution



Bhimesh Most Recent 1 year, 11 months ago

B. Spending more time understanding the company's information goals
upvoted 2 times

Question #12 *Topic 1*

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

Suggested Answer: *C*

Community vote distribution

C (100%)

Supp2023 Highly Voted 3 years ago

The main goal of Privacy by Design, according to the FTC Report of 2012, is to incorporate privacy protections throughout the development process. Therefore, the answer is C.

upvoted 5 times

Bhimesh Most Recent 1 year, 11 months ago

PRIVACY BY DESIGN Baseline Principle: Companies should promote consumer privacy throughout their organizations and at every stage of the development of their products and services. The preliminary staff report called on companies to promote consumer privacy throughout their organizations and at every stage of the development of their products and services.

upvoted 3 times

Question #13 *Topic 1*

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

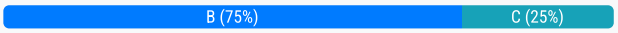
B. Industries may not be strict enough in the creation and enforcement of rules

C. A new business owner may not understand the regulations

D. Human rights may be disregarded for the sake of privacy

Suggested Answer: *B*

Community vote distribution



talilu Most Recent 1 year, 11 months ago

"Industries may not be strict enough in the creation and enforcement of rules" (from the textbook) Privacy advocates and supporters of the European approach to data protection often express concern that industries are not strict enough when creating, adhering to, and enforcing privacy rules or codes of conduct. European regulators, for instance, say that privacy is a fundamental human right, and data protection authorities (DPAs) should be involved in defining and protecting that right.

upvoted 3 times

Bhimesh 1 year, 11 months ago

It is important to note that self-regulation is controversial Privacy advocates and supporters of the European approach to data protection often express concern that industries are not strict enough when creating, adhering to, and enforcing privacy rules or codes of conduct.

upvoted 1 times

MDedon 2 years, 6 months ago

IAPP US Private Sector Privacy 3E Section 3.10, Paragraph 6

upvoted 1 times

Question #14 *Topic 1*

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

Suggested Answer: *A*

Community vote distribution

A (100%)

Bhimesh Most Recent 1 year, 11 months ago

The GPEN aims to promote cross-border information sharing as well as investigation and enforcement cooperation among privacy authorities around the world

upvoted 3 times

PrivacyICU 2 years, 6 months ago

A. Just google it.

upvoted 1 times

Question #15 *Topic 1*

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

Suggested Answer: *A*

Community vote distribution

A (100%)

twiny Most Recent 2 years ago

The correct answer is A. Scanning emails sent to and received by students. Reference: The IAPP textbook, U.S. Private-Sector Privacy, 4th Edition, 2024, Section 10.5.1: "In 2014, students in California who used Apps for Education sued Google, accusing the company of scanning millions of emails sent to and received by students."

upvoted 2 times

Bhimesh 2 years, 5 months ago

Google's Apps for Education Google, for example, developed free Apps for Education a suite of tools that included Gmail, Google Calendar, Google Docs, and Google Classroom In 2014, students in California who used Apps for Education sued Google, accusing the company of scanning millions of emails sent to and received by the students

upvoted 1 times

PrivacyICU 2 years, 12 months ago

Answer is A. Scanning e-mails to get analytics for targeted marketing was a Google practice at the time of the action.

upvoted 1 times

Question #16 *Topic 1*

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

Suggested Answer: *B*

Community vote distribution

B (100%)

twiny Most Recent 2 years ago

The correct answer is B. An online merchant's free shipping offer. Reference: The IAPP textbook, U.S. Private-Sector Privacy, 4th Edition, 2024, Section 5.3.1 FTC Jurisdiction: "Because Section 5 of the FTC Act refers to unfair and deceptive practices "in commerce," this means that nonprofit organizations are not covered. Also, under the FTC Act, the commission's powers do not extend to certain industries, including banks and other federally regulated financial institutions, as well as common carriers, such as the transportation and communications industries."

upvoted 2 times

Bhimesh 2 years, 5 months ago

Section 5 of the FTC Act applies to unfair and deceptive practices "in commerce," and does not apply to nonprofit organizations. The commission's powers also do not extend to certain industries, including banks, other federally regulated financial institutions, and common carriers such as the transportation and communications industries.

upvoted 1 times

PrivacyICU 2 years, 12 months ago

Answer is B through the simple process of elimination and the right answer remains. A and D are local issues (FTC), so federal commerce jurisdiction. FTC doesn't have jurisdiction over banks, so eliminate C. B fits because it is interstate commerce that affects potentially anyone, anywhere in the US. Keep in mind it's only asking what "venture" is subject to FTC regulation, not what venture violated FTC regulations so don't bother trying to figure out if the venture did something wrong.

upvoted 2 times

Question #17 *Topic 1*

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.

Suggested Answer: *B*

Community vote distribution

B (100%)

Bhimesh Most Recent 1 year, 11 months ago

the Privacy Shield requires participating companies to name a compliance third party

upvoted 2 times

MDedon 2 years, 6 months ago

This question is out of date, the EU-US Privacy shield was ruled invalid in 2020 in the Schrems II case.

upvoted 2 times

Question #18 *Topic 1*

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

Suggested Answer: *C*

Community vote distribution

C (100%)

twiny Most Recent 2 years ago

The correct answer is C. The Department of Health and Human Services. Reference: The IAPP textbook, U.S. Private-Sector Privacy, 4th Edition, 2024, Section 9.2.1 The Disposal Rule: "Enforcement of the Disposal Rule is by the FTC, the federal banking regulators, and the CFPB."

upvoted 3 times

Bhimesh 2 years, 5 months ago

Disposal of information. Appropriate destruction of data or information in any format or media is a key component of information management for both the contracting organization and its vendors. The Disposal Rule under the Fair and Accurate Credit Transactions Act(FACTA) of 2003 sets forth required disposal protections for Financial Institutions. The Disposal Rule requirements provide a good baseline for the disposal of personal information more generally. FACTA enacted a number of consumer protections. It required truncation of credit and debit card numbers, so that receipts do not reveal the full credit or debit card number.

upvoted 2 times

Question #19 *Topic 1*

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 data. 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

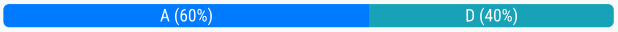
B. The text of the original complaint

C. The company's data privacy policies

D. Prevailing regulation on this subject

Suggested Answer: *D*

Community vote distribution



d654514 Most Recent 1 year, 9 months ago
At this stage of the investigation, the data privacy leader should review A. Available data flow diagrams.
upvoted 1 times

fightingpotato 1 year, 11 months ago
At this stage of the investigation, the data privacy leader should review A. Available data flow diagrams. This will help identify all personal data received from the EU-based retailer, understand how that data is processed and stored, and ensure compliance with the supervisory authority's request. Understanding the data flows is crucial for responding effectively to the investigation and mitigating potential risks.
upvoted 2 times

twiny 2 years ago
All options are plausible correct answers. However, the key to answering this question lies in the following sentence: "The letter closes with an urgent request: 'Please act immediately by identifying all personal data received from our company.'" And the question explicitly asks about the "first" step: "At this stage of the investigation, what should the data privacy leader review first?" Therefore, to help their European retailer/partner, reviewing the available data flow diagrams would be the first step for the data privacy leader. By reviewing the data flows, the data privacy leader will be able to identify the data received from the partner and respond to them accordingly, thus addressing the point asked by the question.
upvoted 3 times

Bhimesh 2 years, 5 months ago
Should be D. Prevailing regulation on this subject
upvoted 1 times

Buki007 2 years, 8 months ago
The answer is D. If you look at A, what if we review the Data flows and later find out that the regulation does not apply to us?
upvoted 1 times

jjjrbm 2 years, 10 months ago
B makes sense as well. Several of the options are reasonable
upvoted 3 times

PrivacyICU 2 years, 12 months ago

D makes sense because you want to understand the law before you apply it to your case.

upvoted 1 times

smp175 3 years, 2 months ago

Does anyone have any additional information on why the answer is D and not A? It seems that identifying categories of PII received would be fine, and therefore reviewing data flows would be the first step. Is it because the prompt specifically states "identifying all personal data", which implies such data would not be anonymized, and therefore prevailing regulation should be reviewed before providing such PII?

upvoted 2 times

Question #20 *Topic 1*

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 data. 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

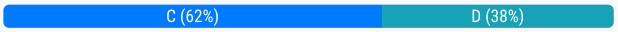
B. Database schemas held by the retailer

C. Lists of all customers, sorted by country

D. Interviews with key marketing personnel

Suggested Answer: *C*

Community vote distribution



BrianVelasquez Most Recent 3 months ago
When the documented data inventory is obsolete, lists of customers sorted by country provide the most concrete, actionable insight to determine which users are affected by the retailer's cross-border data flows, enabling the company to efficiently locate, identify, and delete the complainant's personal data.
upvoted 2 times

gghadid 1 year, 1 month ago
I will choose D. Cuz listing customers would not tell the categories, source, use, third parties which are key to the the data information. however, marketing personnel may exactly know how the data was processed which is helpful for the investigation.
upvoted 3 times

Bhimesh 1 year, 11 months ago
Should be C. Lists of all customers, sorted by country
upvoted 3 times

Question #21 *Topic 1*

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 data. 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

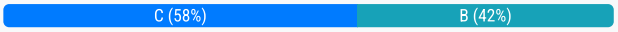
B. As a data processor

C. As a data controller

D. As a data manager

Suggested Answer: *A*

Community vote distribution



Supp2023 Highly Voted 3 years, 6 months ago
"Data supervisor" is not a recognized term under the GDPR. The correct answer is C: as a data controller. The GDPR defines a data controller as the entity that determines the purposes, conditions, and means of the processing of personal data. In the given scenario, the US-based startup company is selling a new gaming application and would likely be considered a data controller as it determines the purposes and means of processing personal data of its users.
upvoted 10 times

twiny Highly Voted 2 years ago
The biggest problem with this question is the wording of its scenario, specifically the first sentence: "A US-based startup company is selling a new gaming application", with the word "selling" being the biggest cause of confusion. However, reading the rest of the scenario, one can infer that the startup is not actually "selling" the game (or the gaming application). It's the European retailer/partner who is selling the game. The US-based startup develops the game and sells it through its retailers, one of which is in Europe. So, the US startup does not collect any customer data. It's the EU retailer who does that and transfers it to the US startup. Therefore, the EU retailer is the data controller, and the US startup is the data processor. Hence, the correct answer is "B. As a data processor." The answer provided by the author, "A. As a data supervisor", is incorrect because "Data supervisor" is not a term used in the GDPR. GDPR is very strict in its language; therefore, assuming that Supervisor and Controller can be used interchangeably shows poor judgment.
upvoted 5 times

BrianVelasquez Most Recent 3 months ago
Under the General Data Protection Regulation (GDPR), a data controller is the entity that determines the purposes and means of processing personal data. By designing the gaming application, collecting user information for it, and deciding its core data strategies, the startup dictates how and why data is handled. In this scenario, the retailer is also a data controller who gathered the user's data and shared it with you. Because your organization autonomously uses that information to run and operate your application, you are acting as an independent controller, not a processor acting strictly on someone else's instructions.
upvoted 1 times

mab487 1 year, 8 months ago
they are a processor
upvoted 1 times

447bcdc 1 year, 9 months ago

b. As a data processor Under the GDPR, a data processor is an entity that processes personal data on behalf of a data controller. In this scenario, the US-based startup company is likely processing personal data (such as user data) on behalf of the EU-based retailer. The retailer, as the entity determining the purposes and means of processing personal data, would be classified as the data controller. Therefore, the US-based startup company, while handling personal data, is doing so under the instructions of the EU-based retailer, making it a data processor.

upvoted 1 times

Bhimesh 2 years, 5 months ago

Selected Answer: B

The answer should be B: The controller is an EU-based retail partner and their letter says " The letter closes with an urgent request: “Please act immediately by identifying all personal data received from our company.”

upvoted 2 times

fightingpotato 1 year, 11 months ago

Under the General Data Protection Regulation (GDPR), the U.S.-based startup company would most likely be classified as C. As a data controller. This is because the startup determines the purposes and means of processing personal data received from the EU-based retailer. Even though the retailer is also involved, the startup's role in handling that data typically aligns with that of a data controller.

upvoted 2 times

Bhimesh 2 years, 5 months ago

The answer should be B: The controller is an EU-based retail partner and their letter says " The letter closes with an urgent request: “Please act immediately by identifying all personal data received from our company.”Correction - Option C

upvoted 2 times

Bhimesh 2 years, 5 months ago

Correction - Option C

upvoted 1 times

BM9904 2 years, 7 months ago

Data controller is an organization that has the authority to decide how and why personal information is to be processed. This entity is the focus of most obligations under privacy and data protection laws

upvoted 2 times

Buki007 2 years, 7 months ago

Under the GDPR the company would be determined as a controller since they control the means and the use of the personal data that is collected and shared with their retail partner.

upvoted 1 times

Romeokton 2 years, 7 months ago

Also think is C

upvoted 2 times

jjjrbm 2 years, 10 months ago

Correct answer is C. Data Controller

upvoted 2 times

PrivacyICU 2 years, 12 months ago

Processor is the answer and correct based on the fact that the EU retailer was collecting consents and sending data internationally to US. The distractor of lack of consent and the instruction somehow implied that it now needs to be adhered to by the processor despite controller EU Retailer messing up should be mindfully sidestepped. Supervisor and Controller are synonymous with both terms used in the GDPR. Data manager is not a term used in GDPR.

upvoted 1 times

testaking917 3 years ago

Must be processor because they do not collect the data directly but the retailer does that

upvoted 3 times

Savaage 3 years, 5 months ago

The prompt says that the video game company received data from the retail, making it the Data Processor.

upvoted 4 times

Robb17 3 years, 6 months ago

Data processor

upvoted 2 times

Lisawood 3 years, 7 months ago

there is no data supervisor under GDPR

upvoted 1 times

cpr14 3 years, 6 months ago

So what's the correct answer?

upvoted 2 times

Lisawood 3 years, 7 months ago

there is no data supervisor under GDPRIs the suggested answer valid although no equivalent role under GDPR but does apply to US?

upvoted 1 times

Testtaker719 3 years, 7 months ago

Is the suggested answer valid although no equivalent role under GDPR but does apply to US?

upvoted 1 times

Question #22 *Topic 1*

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 data. 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

Suggested Answer: *B*

Community vote distribution

D (100%)

Bhimesh Most Recent 1 year, 11 months ago
Should be D. Right to Be Forgotten...
upvoted 1 times

8ab5356 2 years, 1 month ago
Also known as the right to erasure, the GDPR gives individuals the right to ask organizations to delete their personal data. Therefore, it could be A or D
upvoted 1 times

Romeokton 2 years, 1 month ago
Answer should be D
upvoted 1 times

PrivacyICU 2 years, 6 months ago
The answer is D. GDPR doesn't use the term "removal", so don't be fooled. The wording in the law is everything on this exam. GDPR uses the right of modification or erasure. Erasure has come to mean colloquially as the right to be forgotten under GDPR. So although not in the law the right choice in the GDPR has a colloquial answer.
upvoted 1 times

PrivacyICU 2 years, 6 months ago
GDPR doesn't use the term "removal", so don't be fooled. The wording in the law is everything on this exam. GDPR uses the right of modification or erasure. Erasure has come to mean colloquially as the right to be forgotten under GDPR. So although not in the law the right choice in the GDPR has a colloquial answer.
upvoted 1 times

Supp2023 3 years ago

The term "Right of Removal" is not a specific right granted under the GDPR. However, the Right to be Forgotten is often described as a right to request the removal or erasure of personal data, so it is possible that "Right of Removal" is being used as another term for the Right to be Forgotten. In any case, in the scenario you described, the complainant's request is specifically for the deletion or removal of her personal data, which is consistent with the Right to be Forgotten. So while the term "Right of Removal" may not be an official term used in the GDPR, it could potentially refer to the Right to be Forgotten in this context.

upvoted 3 times

Lisawood 3 years, 1 month ago

Right to removal/erasure is the same as right to be forgotten under GDPRWould the correct answer be D since it is asking under GDPR?

upvoted 2 times

Lisawood 3 years, 1 month ago

Right to removal/erasure is the same as right to be forgotten under GDPR

upvoted 2 times

Testtaker719 3 years, 1 month ago

Would the correct answer be D since it is asking under GDPR?

upvoted 3 times

Question #23 *Topic 1*

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

Suggested Answer: *D*

Community vote distribution

D (100%)

Bhimesh Most Recent 1 year, 11 months ago

“no consumer choice,” or “no option,” is expected in a range of situations. The 2010 preliminary FTC staff report, Protecting Consumer Privacy in an Era of Rapid Change, called these situations “commonly accepted practices.” In such situations, an organization has been given implied authority to share personal information. For example, a consumer who orders a product online expects their personal information to be shared with the shipping company, the credit card processor, and others who are engaged in fulfilling the transactions. The consumer does not expect to have to sign an opt-in or be offered an opt-out option for the shipping company to learn the address. In addition to product fulfillment, other examples provided by the FTC include “internal operations such as improving services offered, fraud prevention, legal compliance and First-party marketing” by the seller to the customer

upvoted 1 times

Bhimesh 1 year, 11 months ago

Should be D. When a customer’s street address is shared with a shipping company If the shipping company has to deliver the parcel, there is no option / no choice to opt-out and no further consent is required...

upvoted 1 times

PrivacyICU 2 years, 6 months ago

The shipper is given access to the data needed to complete the transaction, so the buyer (you) give implied consent to the shipper when buying on Amazon (be it Amazon that ships or a 3rd party that does the service that is implied in the contract of buying online to be shipped to your house).

upvoted 1 times

RSkye 2 years, 11 months ago

“For example, a consumer who orders a product online expects their personal information to be shared with the shipping company, the credit card processor, and others who are engaged in fulfilling the transactions. The consumer does not expect to have to sign an opt-in or be offered an opt-out option for the shipping company to learn the address” Excerpt From IAPP_US_TB_US-Private-Sector-Privacy-3E_1.0

upvoted 3 times

Question #24 *Topic 1*

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

Suggested Answer: *C*

Community vote distribution



Bhimesh Most Recent 1 year, 11 months ago

Should be C Effective management of user preferences can become quite challenging, especially for organizations that interact with their customers with multiple channels and for multiple products. The following are some of these challenges: The scope of an opt-out or another user preference can vary. As mentioned above, financial institutions must provide an opt-out by law prior to sharing personal information with third parties, but sharing with affliates can be done without offering such an opt-out. An organization must decide how broadly an opt-out or another user preference will apply.

upvoted 2 times

MDedon 2 years, 6 months ago

As far as I am able to tell, this answer was determined by the the following from IAPP US Private Sector Privacy 3E Section 4.6.2: "Effective management of user preferences can become quite challenging, especially for organizations that interact with their customers with multiple channels and for multiple products." Nowhere does it state that this is the most challenging task businesses face. This is a subjective answer.

upvoted 1 times

smp175 2 years, 8 months ago

C seems like a technical challenge that is likely easily addressed. In contrast, D requires a legal determination of whether the information can be shared under the FCRA. Additionally, C is not unique to financial institutions...

upvoted 1 times

Question #25 *Topic 1*

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

Suggested Answer: *B*

Community vote distribution

C (100%)

twiny Most Recent 2 years ago

The correct answer is clearly C. The vendor's employee retention rates. Reference: The IAPP textbook, U.S. Private-Sector Privacy, 4th Edition, 2024, Section 4.2.2 Vendor/Third-Party Risk Assessments. The factors to consider are as Bhimesh mentioned in his comment. The vendor's employee retention rates are not mentioned in the textbook as one of the factors. Regardless, while employee retention is important for any business, of the answer choices provided, it is the least directly relevant to the vendor's ability to manage personal information securely and effectively.

upvoted 2 times

Bhimesh 2 years, 5 months ago

Vendor Due Diligence A procuring organization may have specific standards and processes for vendor selection. A prospective vendor should be evaluated against these standards. Standards for selecting vendors may include: 1. Reputation 2. Financial condition and insurance 3. Information security controls 4. Point of transfer 5. Disposal of information 6. Employee training and user awareness 7. Vendor incident response 8. Audit rights.

upvoted 3 times

Romeokton 2 years, 7 months ago

Agree with C

upvoted 2 times

jjjrbm 2 years, 10 months ago

Agree. Answer should be C

upvoted 2 times

Privaceeeeee9876 3 years, 4 months ago

The reason I considered vendor employee retention rate at an important factor is if employees at the vendor have access to PI and are constantly leaving that opens a possibility for the employees that have left to disclose PI.

upvoted 1 times

Supp2023 3 years, 6 months ago

Agree. Option C, the vendor's employee retention rates, is the least important factor for the company to consider when selecting a vendor to manage Personal Information (PI). While it is important for a company to consider the reputation and financial health of a vendor, as well as their employee training program, the retention rates of the vendor's employees are not a direct indicator of the vendor's ability to protect personal information. It is important for the company to ensure that the vendor has appropriate security measures in place to protect personal information, such as access controls, encryption, and data breach response procedures. The company should also consider the vendor's compliance with applicable privacy and data protection laws, as well as their experience working with sensitive personal information. Overall, while employee retention rates may indirectly reflect the quality of the vendor's services, they are not a direct factor in assessing the vendor's ability to manage personal information.

upvoted 4 times

Qwamer 3 years, 6 months ago

The answer should be C. On page 90-91 of the book, Section 4.7.2 Vendor Due Diligence, employee retention rate was not mentioned.

upvoted 2 times

Question #26 *Topic 1*

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

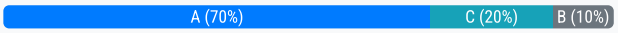
B. An online retailer subscribes new customers to an e-mail list by default

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

Suggested Answer: *A*

Community vote distribution



gghadid Most Recent 1 year, 1 month ago

B. subscribes by default is the mechanism of opt-out, and is not equal to implied consent

upvoted 1 times

fightingpotato 1 year, 11 months ago

A company is operating under the assumption of implied consent in the situation where B. An online retailer subscribes new customers to an e-mail list by default. Implied consent generally occurs when a person's actions or circumstances suggest that they agree to a certain use of their information, such as subscribing them to an email list without explicit consent.Option A, where an employer contacts the professional references provided on an applicant's resume, is typically considered a situation where explicit consent is implied. The applicant generally provides references with the understanding that the employer will contact them to verify information or gain insights about their qualifications. This expectation is part of the application process and is often seen as part of the implied agreement when a candidate submits their references. In contrast, option B involves a situation where the retailer assumes consent by default without the customer's explicit action to agree, which aligns more closely with the concept of implied consent in data handling practices.

upvoted 1 times

fightingpotato 1 year, 11 months ago

Selected Answer: B

A company is operating under the assumption of implied consent in the situation where B. An online retailer subscribes new customers to an e-mail list by default. Implied consent generally occurs when a person's actions or circumstances suggest that they agree to a certain use of their information, such as subscribing them to an email list without explicit consent.

upvoted 1 times

fightingpotato 1 year, 11 months ago

Option A, where an employer contacts the professional references provided on an applicant's resume, is typically considered a situation where explicit consent is implied. The applicant generally provides references with the understanding that the employer will contact them to verify information or gain insights about their qualifications. This expectation is part of the application process and is often seen as part of the implied agreement when a candidate submits their references. In contrast, option B involves a situation where the retailer assumes consent by default without the customer's explicit action to agree, which aligns more closely with the concept of implied consent in data handling practices.

upvoted 1 times

examdj101j 2 years, 5 months ago

I think there should be more discussion into whether B maybe the correct choice, my book CIPP/US (Sybex Version) doesn't really cover implied consent, but by definition, B - looks to be more of the right answer. I have never seen a situation where an employer called references without your verbal/written consent even though the references are listed. Online applications may enlist your specific consent to send reference emails to your references upon the submitting of your application (Teacher Applications most known for this).

upvoted 2 times

Bhimesh 2 years, 5 months ago

Should be A - an organization has been given implied authority by an applicant...

upvoted 2 times

Stevenciu 2 years, 6 months ago

I think it's C. Contacting references provided by an applicant is generally considered as having explicit consent rather than implied, because the act of listing references on a resume or application is a direct indication that the applicant expects and authorizes the employer to contact those references.

upvoted 2 times

Boats 3 years, 4 months ago

Agreed but A is the better answer.

upvoted 4 times

Supp2023 3 years, 5 months ago

Both A and B are right in this instance.B is not correct because the error of the retailer does not justify anything.

upvoted 1 times

Supp2023 3 years, 5 months ago

Both A and B are right in this instance.

upvoted 1 times

PrivacyICU 2 years, 12 months ago

B is not correct because the error of the retailer does not justify anything.

upvoted 3 times

Question #27 *Topic 1*

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

Suggested Answer: *D*

Community vote distribution

B (100%)

impchoi Highly Voted 3 years, 3 months ago

The answer is B. That is part of Build. The others are part of Discover.

upvoted 9 times

Zhenyuan Highly Voted 2 years, 11 months ago

The correct answer is B. However, B is required by the evolve, not build.

upvoted 5 times

e38c357 Most Recent 1 year, 5 months ago

B according to Gemini and the fact that B is more about building or implementation

upvoted 1 times

Bhimesh 1 year, 11 months ago

Phase 1: Discover Before DRAFTING OR UPDATING A PRIVACY POLICY, consider the company’s environment, information goals, and corporate culture. What laws regulate the company’s collection or use of information? Does the company wish to be AGGRESSIVE in its use of information? Does the company instead plan to be more cautious in its use of personal information to reduce legal and reputational risks or perhaps to achieve a competitive advantage as a privacy-sensitive leader? These goals serve as the foundation upon which the company’s policies are built. The successful privacy professional forges honest and open relationships with individuals ACROSS DEPARTMENTS. The participation of a range of departments, including legal, compliance, customer service, marketing, IT, HR, and sales is often BENEFICIAL in the creation of an information plan. The team should have the knowledge base and influence in the organization to determine and articulate the company’s current practices and future goals.

upvoted 2 times

Romeokton 2 years, 1 month ago

As explained by impchoi

upvoted 1 times

jjjrbm 2 years, 4 months ago

Correct answer is "A".

upvoted 1 times

Question #28 *Topic 1*

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

Suggested Answer: *A*

Community vote distribution

A (100%)

Bhimesh Most Recent 1 year, 11 months ago

Should be A. Being more closely scrutinized for any breaches of policy

upvoted 2 times

Question #29 *Topic 1*

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

Suggested Answer: *D*

Community vote distribution

D (100%)

HWAYUNGLE Most Recent 1 year, 1 month ago

To transfer personal data to a third party acting as an agent, organizations must: Accountability for Onward Transfer... (i) Transfer such data only for limited and specified purposes; (ii) Ascertain that the agent is obligated to provide at least the same level of privacy protection as is required by the Principles; (iii) Take 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; (iv) Require 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; (v) Upon notice, including under (vi) Take reasonable and appropriate steps to stop and remediate unauthorized processing; and (vii) Provide a summary or a representative copy of the relevant privacy provisions of its contract with that agent to the Department upon request.

upvoted 2 times

Bhimesh 1 year, 11 months ago

Selected Answer: D

To transfer personal data to a third party acting as an agent, organizations must: Accountability for Onward Transfer... (i) Transfer such data only for limited and specified purposes; (ii) Ascertain that the agent is obligated to provide at least the same level of privacy protection as is required by the Principles; (iii) Take 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; (iv) Require 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; (v) Upon notice, including under (vi) Take reasonable and appropriate steps to stop and remediate unauthorized processing; and (vii) Provide a summary or a representative copy of the relevant privacy provisions of its contract with that agent to the Department upon request.

upvoted 1 times

Bhimesh 1 year, 11 months ago

To transfer personal data to a third party acting as an agent, organizations must: Accountability for Onward Transfer... (i) Transfer such data only for limited and specified purposes; (ii) Ascertain that the agent is obligated to provide at least the same level of privacy protection as is required by the Principles; (iii) Take 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; (iv) Require 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; (v) Upon notice, including under (vi) Take reasonable and appropriate steps to stop and remediate unauthorized processing; and (vii) Provide a summary or a representative copy of the relevant privacy provisions of its contract with that agent to the Department upon request.Accountability for onward transfer / vendor agreements Privacy Shield expands regulation of and accountability for third party personal data transfers. A Privacy Shield certified organization must specify in third party contracts that transferred personal data "may only be processed for limited and specified purposes consistent with" the data subject's consent. Third parties must agree to "provide the same level of protection as the Principles." Where the third party is acting as an agent, such as a vendor, the organization must in addition "take reasonable and appropriate steps" to ensure the agent upholds the Principles A Privacy Shield certified organization must even provide the DOC with relevant third party contractual provisions, which place some restrictions on contractual confidentiality.

upvoted 2 times

Bhimesh 1 year, 11 months ago

Accountability for onward transfer / vendor agreements Privacy Shield expands regulation of and accountability for third party personal data transfers. A Privacy Shield certified organization must specify in third party contracts that transferred personal data “may only be processed for limited and specified purposes consistent with” the data subject’s consent. Third parties must agree to “provide the same level of protection as the Principles.” Where the third party is acting as an agent, such as a vendor, the organization must in addition “take reasonable and appropriate steps” to ensure the agent upholds the Principles A Privacy Shield certified organization must even provide the DOC with relevant third party contractual provisions, which place some restrictions on contractual confidentiality.

upvoted 1 times

Question #30 *Topic 1*

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

A. To ensure privacy rights of U.S. citizens

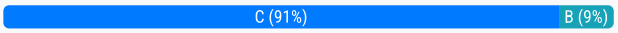
B. To protect consumers

C. To enforce antitrust laws

D. To negotiate consent decrees with companies violating personal privacy

Suggested Answer: *B*

Community vote distribution



scoobi Highly Voted 3 years, 8 months ago

IT'S ORIGINAL PURPOSE WAS TO ENFORCE ANTITRUST LAWS

upvoted 10 times

smp175 Highly Voted 3 years, 2 months ago

IAPP book, Section 3.3, first sentence. "The FTC was founded in 1914 to enforce antitrust laws, and its general consumer protection mission was established by a statutory change in 1938." In particular in considering this answer, note that the FTC Act was initially passed in 1914.

upvoted 6 times

BrianVelasquez Most Recent 3 months ago

Signed into law in 1914 by President Woodrow Wilson, the Federal Trade Commission Act was originally created to enforce antitrust laws, bust corporate trusts, and prevent unfair methods of competition in the marketplace. Its primary goal was to regulate the market by maintaining a competitive economy for the benefit of consumers.

upvoted 1 times

HWAYUNGLE 1 year, 1 month ago

IAPP book, Section 3.3, first sentence. "The FTC was founded in 1914 to enforce antitrust laws, and its general consumer protection mission was established by a statutory change in 1938

upvoted 1 times

Bhimesh 2 years, 5 months ago

Selected Answer: B

The FTC enforces federal consumer protection laws that prevent fraud, deception and unfair business practices. The Commission also enforces federal antitrust laws that prohibit anticompetitive mergers and other business practices that could lead to higher prices, fewer choices, or less innovation.

Whether combating telemarketing fraud, Internet scams or price-fixing schemes, the FTC's mission is to protect consumers and promote competition.

upvoted 1 times

twiny 2 years ago

I just realized that there is a voting comment option where you can select the answer choice letter. Apologies for duplicating my comment. The question is asking about the ORIGINAL purpose of the Federal Trade Commission Act. The original purpose of the Federal Trade Commission Act was to enforce antitrust laws and prevent unfair competition in the marketplace. Over time, the FTC's role has expanded to include consumer protection and privacy enforcement, but these were not its initial focus. Here is how the IAPP textbook puts it: "The FTC was founded in 1914 to enforce antitrust laws, and its general consumer protection mission was established by a statutory change in 1938." Therefore, the correct answer is C. To enforce antitrust laws. Reference: The IAPP textbook, U.S. Private-Sector Privacy, 4th Edition, 2024, Section 5.3.

upvoted 2 times

twiny 2 years ago

The question is asking about the ORIGINAL purpose of the Federal Trade Commission Act. The original purpose of the Federal Trade Commission Act was to enforce antitrust laws and prevent unfair competition in the marketplace. Over time, the FTC's role has expanded to include consumer protection and privacy enforcement, but these were not its initial focus. Here is how the IAPP textbook puts it: "The FTC was founded in 1914 to enforce antitrust laws, and its general consumer protection mission was established by a statutory change in 1938." Therefore, the correct answer is C. To enforce antitrust laws. Reference: The IAPP textbook, U.S. Private-Sector Privacy, 4th Edition, 2024, Section 5.3.

upvoted 1 times

Bhimesh 2 years, 5 months ago

The FTC enforces federal consumer protection laws that prevent fraud, deception and unfair business practices. The Commission also enforces federal antitrust laws that prohibit anticompetitive mergers and other business practices that could lead to higher prices, fewer choices, or less innovation. Whether combating telemarketing fraud, Internet scams or price-fixing schemes, the FTC's mission is to protect consumers and promote competition.The future of federal enforcement will continue to build on core directives of the FTC to protect consumers and encourage competition. According to the FTC's "Comment on the Future of Privacy" in 2018, the FTC sees a future of continued enforcement of unfair and deceptive trade practices with respect to privacy and security.

upvoted 1 times

Bhimesh 2 years, 5 months ago

The future of federal enforcement will continue to build on core directives of the FTC to protect consumers and encourage competition. According to the FTC's "Comment on the Future of Privacy" in 2018, the FTC sees a future of continued enforcement of unfair and deceptive trade practices with respect to privacy and security.

upvoted 1 times

ph2022 3 years, 6 months ago

per the FTC Board, it was do protect the consumer.

upvoted 2 times

Question #31 *Topic 1*

SCENARIO -
Please use the following to answer the next question:
Matt went into his son's bedroom one evening and found him stretched out on his bed typing on his laptop.
"Doing your homework?" Matt asked hopefully.
"No," the boy said. "I'm filling out a survey."
Matt looked over his son's shoulder at his computer screen. "What kind of survey?"
"It's asking questions about my opinions."
"Let me see," Matt said, and began reading the list of 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.

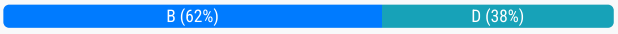
B. Collecting information from a child under the age of thirteen.

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

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

Suggested Answer: *D*

Community vote distribution



impchoi Highly Voted 3 years, 9 months ago
B is correct.
upvoted 6 times

BrianVelasquez Most Recent 3 months ago
Option B is correct because the scenario directly involves a violation of the Children's Online Privacy Protection Act (COPPA), which is enforced by the Federal Trade Commission (FTC). COPPA strictly regulates how commercial websites and online services collect personal information from children under the age of 13. Matt's son is only ten years old, and the marketer collected his name, address, telephone number, and date of birth without obtaining verifiable parental consent first. Option D is incorrect because the FTC enforces federal laws and federal regulations, not industry self-regulatory guidelines or private "privacy policies of the marketing industry."
upvoted 1 times

twiny 2 years ago
Here is why choice D is incorrect: While the company's actions may have violated best practices for children's marketing, the legal violation here is specifically about collecting personal data from a child under 13 without parental consent, as regulated by COPPA, and, therefore, will be enforced by the FTC.
upvoted 4 times

twiny 2 years ago

The key to answering this question is the word VIOLATION: "Based on the incident, the FTC's enforcement actions against the marketer would most likely include what violation?" The correct answer is B. Collecting information from a child under the age of thirteen. Here is why: 1. The Children's Online Privacy Protection Act (COPPA) is a U.S. law that places strict requirements on how companies can collect and use personal information from children under the age of 13. According to COPPA, companies must obtain verifiable parental consent before collecting personal information from children under 13, and they must clearly disclose their data collection practices. 2. In this scenario, the marketer collected personal information from Matt's 10-year-old son (name, address, date of birth, etc.) without apparent parental consent. This would be a clear VIOLATION of COPPA.

upvoted 3 times

examdj101j 2 years, 5 months ago

Collecting information from a child under 13 is not a violation, The violation would be failure to obtain parent consent when collecting information from a child under 13. My choice is D.

upvoted 1 times

Bhimesh 2 years, 5 months ago

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

upvoted 2 times

jjjrbm 2 years, 10 months ago

answer is B

upvoted 1 times

smp175 3 years, 2 months ago

Nothing in the prompt suggests that the marketer undertakes to comply with any self-regulatory policies. In contrast, based on the prompt there was clearly no parental consent. B due to a violation of COPPA is the answer.

upvoted 1 times

Privaceeeeee9876 3 years, 4 months ago

D: The question is asking about violations marketer. If the question were to ask about the FTC's enforcement actions in violation of COPPA then the answer would be B

upvoted 1 times

Supp2023 3 years, 5 months ago

B may be ok with parental consent. D, however may be the right answer here because the question is specifically asking based on the incident, the FTC's enforcement actions against the marketer would most likely include what violation and D is the only best option here.

upvoted 1 times

Question #32 *Topic 1*

SCENARIO -
Please use the following to answer the next question:
Matt went into his son's bedroom one evening and found him stretched out on his bed typing on his laptop.
"Doing your homework?" Matt asked hopefully.
"No," the boy said. "I'm filling out a survey."
Matt looked over his son's shoulder at his computer screen. "What kind of survey?"
"It's asking questions about my opinions."
"Let me see," Matt said, and began reading the list of 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

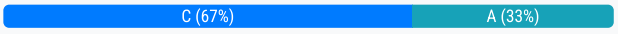
B. The marketer did not provide evidence that the prize books were appropriate for children

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

Suggested Answer: *A*

Community vote distribution



Lisawood Highly Voted 3 years, 7 months ago
Te answer is C. Must obtain parental consent.
upvoted 6 times

twiny Most Recent 2 years ago
The correct answer is C. The marketer seems to have distributed his son's information without Matt's permission. Here is why choice A is incorrect: COPPA does require parental notification; however, the scenario does not indicate that the marketer attempted to provide any information to Matt at all. The issue is not the inadequacy of the attempt but the lack of parental consent and the collection of the child's personal information without the parent's knowledge. While the scenario does not explicitly indicate that the marketer has distributed Matt's son's information without Matt's permission, the fact Matt noticed several other commercial emails from marketers advertising products for children in his son's inbox implies the original marketer has distributed Matt's son's information, making choice C the best answer to the question asked.
upvoted 2 times

examdj101j 2 years, 5 months ago
C is a specific violation of COPPA, A is vague and can mean a lot of different things, so I am going with C on this one.
upvoted 2 times

Bhimesh 2 years, 5 months ago

C. The marketer seems to have distributed his son's information without Matt's permission The COPPA Rule, 16 CFR part 312, issued pursuant to the Children's Online Privacy Protection Act ("COPPA" or "COPPA statute"), 15 U.S.C. 6501 et seq., became effective on April 21, 2000. The Rule imposes certain requirements on operators of Web sites or online services directed to children under 13 years of age, and on operators of other Web sites or online services that have actual knowledge that they are collecting personal information online from a child under 13 years of age (collectively, "operators"). Among other things, the Rule requires that operators provide notice to parents and obtain verifiable parental consent prior to collecting, using, or disclosing personal information from children under 13 years of agel agree, Matt states that his son received more emails from marketers advertising products to him.

upvoted 2 times

Bhimesh 2 years, 5 months ago

Selected Answer: C

C. The marketer seems to have distributed his son's information without Matt's permission

The COPPA Rule, 16 CFR part 312, issued pursuant to the Children's Online Privacy Protection Act ("COPPA" or "COPPA statute"), 15 U.S.C. 6501 et seq., became effective on April 21, 2000.

The Rule imposes certain requirements on operators of Web sites or online services directed to children under 13 years of age, and on operators of other Web sites or online services that have actual knowledge that they are collecting personal information online from a child under 13 years of age (collectively, "operators").

Among other things, the Rule requires that operators provide notice to parents and obtain verifiable parental consent prior to collecting, using, or disclosing personal information from children under 13 years of age

upvoted 1 times

examdj101j 2 years, 5 months ago

I agree, Matt states that his son received more emails from marketers advertising products to him.

upvoted 1 times

fdnsup 2 years, 5 months ago

Answer C "adequate attempt" is not enough under COPPA the parent needs to provide his consent

upvoted 1 times

jjjrbm 2 years, 10 months ago

Answer is C

upvoted 2 times

Boats 3 years, 4 months ago

Make reasonable efforts (taking into account available technology) to provide direct notice to parents of the operator's practices with regard to the collection, use, or disclosure of personal information from persons under 13, including notice of any material change to such practices to which the parents have previously consented;

upvoted 3 times

Supp2023 3 years, 5 months ago

A is the best option here, because we don't know if the other commercial emails were a result of distribution from this particular marketer. A is likely the best choice here.

upvoted 2 times

Question #33 *Topic 1*

SCENARIO -
Please use the following to answer the next question:
Matt went into his son's bedroom one evening and found him stretched out on his bed typing on his laptop.
"Doing your homework?" Matt asked hopefully.
"No," the boy said. "I'm filling out a survey."
Matt looked over his son's shoulder at his computer screen. "What kind of survey?"
"It's asking questions about my opinions."
"Let me see," Matt said, and began reading the list of 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

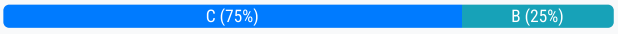
B. By making a COPPA privacy notice available on website

C. By participating in an approved self-regulatory program

D. By regularly assessing the security risks to consumer privacy

Suggested Answer: *A*

Community vote distribution



impchoi Highly Voted 3 years, 9 months ago
C: Safe harbor indicates participation in a self-regulatory program.
upvoted 5 times

twiny Most Recent 2 years ago
The correct answer is C. By participating in an approved self-regulatory program. Here is why: COPPA includes a Safe Harbor provision, which allows companies to meet COPPA's requirements by participating in an FTC-approved self-regulatory program. These programs are designed to ensure compliance with COPPA's requirements, including obtaining verifiable parental consent before collecting personal information from children under the age of 13. Companies that participate in these programs are subject to oversight and audits, which help ensure that they are following COPPA regulations. Here is whyA is incorrect: The FTC does not specifically approve the content of individual marketing emails. The issue in the scenario is not about the content of the emails but the collection of children's personal data without proper parental consent. Here is why B is incorrect: While having a COPPA-compliant privacy notice on the website is necessary, it is not sufficient on its own to meet COPPA's Safe Harbor requirements.
upvoted 3 times

Bhimesh 2 years, 5 months ago
COPPA Safe Harbor Program The Children's Online Privacy Protection Act (COPPA) includes a provision enabling industry groups or others to submit for Commission approval self-regulatory guidelines that implement the protections of the Commission's final Rule. The COPPA Rule requires the Commission to act on a request for "safe harbor" treatment within 180 days of the filing of the request, and after the proposed guidelines have been subject to notice and comment. Section 312.10 of the final Rule sets out the criteria for approval of guidelines and the materials that must be submitted as part of a safe harbor application.
upvoted 2 times

Aremu1 2 years, 9 months ago

"A" is the most probable answer as the question is asking about meeting COPPA “Safe Harbor” requirements

upvoted 1 times

jjjrbm 2 years, 10 months ago

answer is C

upvoted 1 times

cja1002 2 years, 11 months ago

COPPA safe harbor programs comprise industry groups that self-regulate their member-operators and establish their own guidelines and requirements that must guarantee the same or greater protection for children as the standards set forth in the COPPA rule.

upvoted 1 times

smp175 3 years, 2 months ago

FTC COPPA Safe Harbor applies to approval of self-regulatory programs, not something as specific as individual email contents. Therefore C is the best answer.

upvoted 2 times

Boats 3 years, 4 months ago

https://www.ftc.gov/business-guidance/resources/childrens-online-privacy-protection-rule-six-step-compliance-plan-your-business Step 2: Post a Privacy Policy that Complies with COPPA. Assuming you’re covered by COPPA, the next step is to post a privacy policy. It must clearly and comprehensively describe how personal information collected online from kids under 13 is handled. The notice must describe not only your practices, but also the practices of any others collecting personal information on your site or service — for example, plug-ins or ad networks.

upvoted 3 times

Supp2023 3 years, 5 months ago

A is likely the best choice here. Safe Harbor self-regulatory approvals require submitting the request to FTC for pre-approval https://www.ftc.gov/system/files/2012-31341.pdf

upvoted 1 times

Question #34 *Topic 1*

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

Suggested Answer: *A*

Community vote distribution

A (100%)

twiny Most Recent 2 years ago

The correct answer is supported more directly in section 8.2.4 Electronic Health Records, where the IAPP textbook reads, "The $19 billion in funding in HITECH created important incentives for health providers to use electronic health records (EHRs) more extensively. Providers who make "meaningful use" of EHRs can qualify for these funds."

upvoted 2 times

twiny 2 years ago

The correct answer is A. Make electronic health records (EHRs) part of regular care. Reference: The IAPP textbook, U.S. Private-Sector Privacy, 4th Edition, 2024, Section 8.2

upvoted 1 times

Bhimesh 2 years, 5 months ago

Selected Answer: A

The Health Information Technology for Economic and Clinical Health Act (HITECH) was enacted as part of the American Recovery and Reinvestment Act of 2009 to promote the adoption and meaningful use of health information technology. HITECH codified and funded the office of the National Coordinator for Health Information Technology and provided $19 billion in INCENTIVES FOR HEALTHCARE PROVIDERS TO ADOPT ELECTRONIC HEALTH RECORDS and develop a national electronic health information exchange. HITECH also strengthened HIPAA to address the privacy impacts of the expanded use of electronic health records

upvoted 2 times

Bhimesh 2 years, 5 months ago

The Health Information Technology for Economic and Clinical Health Act (HITECH) was enacted as part of the American Recovery and Reinvestment Act of 2009 to promote the adoption and meaningful use of health information technology. HITECH codified and funded the office of the National Coordinator for Health Information Technology and provided $19 billion in INCENTIVES FOR HEALTHCARE PROVIDERS TO ADOPT ELECTRONIC HEALTH RECORDS and develop a national electronic health information exchange. HITECH also strengthened HIPAA to address the privacy impacts of the expanded use of electronic health recordsThe $19 billion in funding in HITECH created important incentives for health providers to use Electronic Health Records (EHRs) more extensively. Providers who make “meaningful use” of EHRs can qualify for these funds.

upvoted 2 times

Bhimesh 2 years, 5 months ago

The $19 billion in funding in HITECH created important incentives for health providers to use Electronic Health Records (EHRs) more extensively. Providers who make “meaningful use” of EHRs can qualify for these funds.

upvoted 2 times

Boats 3 years, 4 months ago

What funding did the HITECH Act provide healthcare? The Department of Health & Human Services (HHS) was given a budget in excess of $25 billion to achieve the goals of the HITECH Act. The HHS used some of that budget to fund the Meaningful Use program – a program that incentivized care providers to adopt certified EHRs by offering monetary incentives

upvoted 2 times

Question #35 *Topic 1*

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

Suggested Answer: *B*

Community vote distribution

B (100%)

twiny Most Recent 2 years ago

The correct answer is B. Pharmaceutical companies. Reference: The IAPP textbook, U.S. Private-Sector Privacy, 4th Edition, 2024, Section 8.1 The Health Insurance Portability and Accountability Act of 1996. The textbook reads: "Entities that are directly covered under HIPAA include: - Health care providers (e.g., doctors' offices, hospitals) that conduct certain transactions in electronic form - Health plans (e.g., health insurers) - Health care clearinghouses (e.g., third-party organizations that host, handle, or process medical information)" Pharmaceutical companies are not on the list of HIPPA-covered entities, making choice B the best answer to the question asked.

upvoted 3 times

Bhimesh 2 years, 5 months ago

A Covered Entity is one of the following: A Health Care Provider A Health Plan A Health Care Clearinghouse A Health Care Provider includes... Doctors Clinics Psychologists Dentists Chiropractors Nursing Homes Pharmacies ...but only if they transmit any information in an electronic form in connection with a transaction for which HHS has adopted a standard. A Health Plan - This includes: Health insurance companies HMOs Company health plans Government programs that pay for health care, such as Medicare, Medicaid, and the military and veterans health care programs A Health Care Clearinghouse- This includes entities that process nonstandard health information they receive from another entity into a standard (i.e., standard electronic format or data content), or vice versa.

upvoted 3 times

Bhimesh 2 years, 5 months ago

The purpose of the 21st Century Cures Act ("Cures Act") is to expedite the research process for new medical devices and prescription drugs, speed up the process for drug approval, and reform mental health treatment. Although the initial version of the bill raised concerns that PHARMACEUTICAL COMPANIES would be able to purchase individually identifiable health information that was deemed to have research or public health purposes, the final bill addressed these potential pitfalls. Information blocking prohibited but HIPAA's protection of PHI remains. The Cures Act prohibits providers, health information technology (HIT) providers, health information exchanges (HIEs). This requirement must be balanced with HIPAA's requirements concerning PHI.HITECH itself, along with providing funding for greater use of EHRs, made certain changes to HIPAA's legal treatment of EHRs. Covered entities must provide individuals with a copy of their EHR on request and must account for all nonoral disclosures made within three years on the request. Additionally, covered entities may not sell EHRs without the consent of the patient, and covered entities cannot receive payment for certain marketing plans

upvoted 1 times

Bhimesh 2 years, 5 months ago

Selected Answer: B

The purpose of the 21st Century Cures Act ("Cures Act") is to expedite the research process for new medical devices and prescription drugs, speed up the process for drug approval, and reform mental health treatment.

Although the initial version of the bill raised concerns that PHARMACEUTICAL COMPANIES would be able to purchase individually identifiable health information that was deemed to have research or public health purposes, the final bill addressed these potential pitfalls.

Information blocking prohibited but HIPAA's protection of PHI remains. The Cures Act prohibits providers, health information technology (HIT) providers, health information exchanges (HIEs). This requirement must be balanced with HIPAA's requirements concerning PHI.

upvoted 1 times

Bhimesh 2 years, 5 months ago

HITECH itself, along with providing funding for greater use of EHRs, made certain changes to HIPAA's legal treatment of EHRs. Covered entities must provide individuals with a copy of their EHR on request and must account for all nonoral disclosures made within three years on the request. Additionally, covered entities may not sell EHRs without the consent of the patient, and covered entities cannot receive payment for certain marketing plans

upvoted 1 times

Question #36 *Topic 1*

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

Suggested Answer: *D*

Community vote distribution

D (100%)

twiny Most Recent 2 years ago

Typo in my last sentence. Should read, "making choice D the BEST answer to the question asked." (not the "next" answer).

upvoted 1 times

twiny 2 years ago

The correct answer is D. Medical providers. Reference: The IAPP textbook, U.S. Private-Sector Privacy, 4th Edition, 2024, Section 8.2.1 Notice of Breach: "If there is a high probability that the security or privacy of the information (financial, reputational, or other) has been compromised, a covered entity must notify individuals within 60 days of discovery. If the breach affects more than 500 people, the covered entity must notify the HHS immediately, and if the breach affects 500 or more in the same jurisdiction, it must notify the media." Medical providers are not among those to whom the covered entity should report the breach, making choice D the next answer to the question asked.

upvoted 3 times

Bhimesh 2 years, 5 months ago

Selected Answer: D

Breach Notification Requirements Following a breach of unsecured protected health information, covered entities must provide notification of the breach to affected individuals, the Secretary, and, in certain circumstances, to the media. In addition, business associates must notify covered entities if a breach occurs at or by the business associate.

Individual Notice Covered entities must notify affected individuals following the discovery of a breach of unsecured protected health information.

Media Notice Covered entities that experience a breach affecting more than 500 residents of a State or jurisdiction are, in addition to notifying the affected individuals, required to provide notice to prominent media outlets serving the State or jurisdiction.

upvoted 1 times

Bhimesh 2 years, 5 months ago

Breach Notification Requirements Following a breach of unsecured protected health information, covered entities must provide notification of the breach to affected individuals, the Secretary, and, in certain circumstances, to the media. In addition, business associates must notify covered entities if a breach occurs at or by the business associate. Individual Notice Covered entities must notify affected individuals following the discovery of a breach of unsecured protected health information. Media Notice Covered entities that experience a breach affecting more than 500 residents of a State or jurisdiction are, in addition to notifying the affected individuals, required to provide notice to prominent media outlets serving the State or jurisdiction.Notice to the Secretary (notify the Secretary by visiting the HHS website) In addition to notifying affected individuals and the media (where appropriate), covered entities must notify the Secretary of breaches of unsecured protected health information. Covered entities will notify the Secretary by visiting the HHS website and filling out and electronically submitting a breach report form. If a breach affects 500 or more individuals, covered entities must notify the Secretary without unreasonable delay and in no case later than 60 days following a breach. If, however, a breach affects fewer than 500 individuals, the covered entity may notify the Secretary of such breaches on an annual basis. Reports of breaches affecting fewer than 500 individuals are due to the Secretary no later than 60 days after the end of the calendar year in which the breaches are discovered

upvoted 1 times

Bhimesh 2 years, 5 months ago

Notice to the Secretary (notify the Secretary by visiting the HHS website) In addition to notifying affected individuals and the media (where appropriate), covered entities must notify the Secretary of breaches of unsecured protected health information. Covered entities will notify the Secretary by visiting the HHS website and filling out and electronically submitting a breach report form. If a breach affects 500 or more individuals, covered entities must notify the Secretary without unreasonable delay and in no case later than 60 days following a breach. If, however, a breach affects fewer than 500 individuals, the covered entity may notify the Secretary of such breaches on an annual basis. Reports of breaches affecting fewer than 500 individuals are due to the Secretary no later than 60 days after the end of the calendar year in which the breaches are discovered

upvoted 2 times

Boats 3 years, 4 months ago

https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html Following a breach of unsecured protected health information, covered entities must provide notification of the breach to affected individuals, the Secretary, and, in certain circumstances, to the media. In addition, business associates must notify covered entities if a breach occurs at or by the business associate.

upvoted 1 times

Question #37 *Topic 1*

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

Suggested Answer: *A*

Community vote distribution

B (100%)

Qwamer Highly Voted 3 years ago

FACTA amended FCRA, which already had a right to correct inaccurate reporting. The answer is B, on page 227 of the book the first consumer protection listed is truncation if credit and debit card numbers on receipts.

upvoted 5 times

Shaza123 Highly Voted 3 years ago

The correct answer is B.

upvoted 5 times

Bhimesh 1 year, 11 months ago

The Fair and Accurate Credit Transactions Act FACTA enacted a number of consumer protections. It required truncation of credit and debit card numbers, so that receipts do not reveal the full credit or debit card number. It gave consumers new rights to an explanation of their credit scores. It also gave individuals the right to request a free annual credit report from each of the three national consumer credit agencies Equifax, Experian and TransUnion. Along with other identity theft protections, FACTA required regulators to promulgate a Disposal Rule and a Red Flags Rule.All merchants are required to partially mask credit card numbers on receipts and transaction records, and Social Security numbers must be similarly redacted by consumer request. Any users of credit records must dispose of paper and electronic records when no longer needed. FACTA also requires higher standards and more disclosure from CRAs to ensure that information is accurate and to tell consumers specifically how they calculate credit scores.

upvoted 2 times

Bhimesh 1 year, 11 months ago

Selected Answer: B

The Fair and Accurate Credit Transactions Act

FACTA enacted a number of consumer protections.

It required truncation of credit and debit card numbers, so that receipts do not reveal the full credit or debit card number.

It gave consumers new rights to an explanation of their credit scores.

It also gave individuals the right to request a free annual credit report from each of the three national consumer credit agencies Equifax, Experian and TransUnion.

Along with other identity theft protections, FACTA required regulators to promulgate a Disposal Rule and a Red Flags Rule.

upvoted 2 times

Bhimesh Most Recent 1 year, 11 months ago

All merchants are required to partially mask credit card numbers on receipts and transaction records, and Social Security numbers must be similarly redacted by consumer request. Any users of credit records must dispose of paper and electronic records when no longer needed. FACTA also requires higher standards and more disclosure from CRAs to ensure that information is accurate and to tell consumers specifically how they calculate credit scores.

upvoted 1 times

jjjrbm 2 years, 4 months ago

Correct answer is B

upvoted 1 times

Privaceeeeee9876 2 years, 10 months ago

I chose A since the act is the fair and ACCURATE credit transactions act. Therefore, a consumer should be able to correct INACCURATE information

upvoted 3 times

Question #38 *Topic 1*

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

Suggested Answer: *D*

Community vote distribution

D (100%)

twiny Most Recent 2 years ago

The correct answer is D. The Consumer Financial Protection Bureau. This answer is supported in several sections of the IAPP textbook, U.S. Private-Sector Privacy, 4th Edition, 2024, such as: 5.4.3, "Until the creation of the CFPB, the FTC issued rules and guidance for the FCRA, as amended by the Fair and Accurate Credit Transactions Act (FACTA) of 2003. The CFPB now has authority to issue rules for those areas." 9, "The CFPB now has rulemaking authority for the FCRA, as updated by FACTA, as well as for most financial institutions under GLBA..." 9.4, "The CFPB has assumed rulemaking authority for specific existing laws related to financial privacy and other consumer issues, such as the FCRA, GLBA, and Fair Debt Collection Practices Act." Initially, I selected B, because the FTC previously had rulemaking and enforcement authority for these laws before the CFPB was created. While the FTC still has some enforcement responsibilities, the CFPB now holds primary rulemaking authority.

upvoted 2 times

Bhimesh 2 years, 5 months ago

In 2010, Congress passed the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act), which granted "rule-making authority" under FCRA (except for Section 615(e) (red flag guidelines and regulation) and Section 628 (disposal of records) to the Consumer Financial Protection Bureau (CFPB). Congress substantively amended the FCRA upon the passage of the Fair and Accurate Credit Transactions Act of 2003 (FACT Act). The FACT Act created many new responsibilities for consumer reporting agencies and users of consumer reports. It contained many new consumer disclosure requirements as well as provisions to address identity theft. In addition, it provided free annual consumer report rights for consumers and improved access to consumer report information to help increase the accuracy of data in the consumer reporting system.

upvoted 1 times

Romeokton 2 years, 7 months ago

Answer is D

upvoted 1 times

Boats 3 years, 4 months ago

https://www.consumerfinance.gov/compliance/supervision-examinations/fair-credit-reporting-act-fcra-examination-procedures/ In 2010, Congress passed the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act), which granted rule-making authority under FCRA (except for Section 615(e) (red flag guidelines and regulation) and Section 628 (disposal of records) to the Consumer Financial Protection Bureau (CFPB). The Dodd-Frank Act also amended two provisions of the FCRA to require the disclosure of a credit score and related information when a credit score is used in taking an adverse action or in risk-based pricing.

upvoted 3 times

Supp2023 3 years, 5 months ago

FTC also has significant rule making authority over FCRA and FACTA. Could B also be the right choice here?

upvoted 1 times

Question #39 *Topic 1*

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

Suggested Answer: *C*

Community vote distribution

A (100%)

impchoi Highly Voted 3 years, 9 months ago

The answer should be A: "The Disposal Rule requires any individual or entity that uses a consumer report, or information derived from a consumer report, for a business purpose to dispose of that consumer information in a way that prevents unauthorized access and misuse of the data. Consumer reports can be electronic or written. The rule applies to both small and large organizations, including consumer reporting agencies, lenders, employers, insurers, landlords, car dealers, attorneys, debt collectors, and government agencies." and "Examples of acceptable, reasonable measures include developing and complying with policies to: Burn, pulverize or shred papers containing consumer report information so that the information cannot be read or reconstructed Destroy or erase electronic files or media containing consumer report information so that the information cannot be read or reconstructed Conduct due diligence and hire a document destruction contractor to dispose of material specifically identified as consumer report information consistent with the rule"

upvoted 12 times

twiny Most Recent 2 years ago

The correct answer is A. To follow the Disposal Rule by having the reports shredded. Reference: The IAPP textbook, U.S. Private-Sector Privacy, 4th Edition, 2024, Section 9.2.1 The Disposal Rule: "Consumer reports can be electronic or written. The rule applies to both small and large organizations, including consumer reporting agencies, lenders, employers, insurers, landlords, car dealers, attorneys, debt collectors, and government agencies." The correct answer, according to the author, is C. To follow the Privacy Rule by notifying customers that the reports are being stored. Here is why it's incorrect: The Privacy Rule, under the Gramm-Leach-Bliley Act (GLBA), deals with how financial institutions handle customer privacy and the disclosure of personal information, but it does not specifically address the storage of credit reports in the way described in the scenario. Therefore, of the choices provided, following the Disposal Rule by having the reports shredded is a better answer to the question asked.

upvoted 2 times

Bhimesh 2 years, 5 months ago

The Disposal Rule requires any individual or entity that uses a consumer report, or information derived from a consumer report, for a business purpose to dispose of that consumer information in a way that prevents unauthorized access and misuse of the data. Consumer reports can be electronic or written. The rule applies to both small and large organizations, including consumer reporting agencies, lenders, employers, insurers, landlords, “CAR DEALERS”, attorneys, debt collectors, and government agencies.Disposal” includes any discarding, abandonment, donation, sale or transfer of information. The standard for disposal requires practices that are “reasonable” to protect against unauthorized access to or use of the consumer data. Factors to consider include the sensitivity of information being disposed of, the costs and benefits of various disposal methods, and available technology. Examples of acceptable, reasonable measures include developing and complying with policies to: Burn, pulverize or shred papers containing consumer report information so that the information cannot be read or reconstructed. Destroy or erase electronic files or media containing consumer report information so that the information cannot be read or reconstructed. Conduct due diligence and hire a document destruction contractor to dispose of material specifically identified as consumer report information consistent with the rule

upvoted 1 times

Bhimesh 2 years, 5 months ago

Selected Answer: A

The Disposal Rule requires any individual or entity that uses a consumer report, or information derived from a consumer report, for a business purpose to dispose of that consumer information in a way that prevents unauthorized access and misuse of the data. Consumer reports can be electronic or written. The rule applies to both small and large organizations, including consumer reporting agencies, lenders, employers, insurers, landlords, “CAR DEALERS”, attorneys, debt collectors, and government agencies.

upvoted 1 times

Bhimesh 2 years, 5 months ago

Disposal" includes any discarding, abandonment, donation, sale or transfer of information. The standard for disposal requires practices that are "reasonable" to protect against unauthorized access to or use of the consumer data. Factors to consider include the sensitivity of information being disposed of, the costs and benefits of various disposal methods, and available technology. Examples of acceptable, reasonable measures include developing and complying with policies to: Burn, pulverize or shred papers containing consumer report information so that the information cannot be read or reconstructed. Destroy or erase electronic files or media containing consumer report information so that the information cannot be read or reconstructed. Conduct due diligence and hire a document destruction contractor to dispose of material specifically identified as consumer report information consistent with the rule

upvoted 1 times

Judyhuang 2 years, 9 months ago

the answer is A

upvoted 1 times

jjjrbm 2 years, 10 months ago

Correct answer is A

upvoted 1 times

Privaceeeeee9876 3 years, 4 months ago

The answer is A

upvoted 3 times

Boats 3 years, 4 months ago

https://www.shrednations.com/articles/facta-compliance/ Proper Disposal of Sensitive Information Lastly, FACTA requires creditors and financial institutions to take "reasonable measures to protect against unauthorized access to or use of consumer information" by means of proper disposal. To ensure private information is not compromised it required that reasonable steps be taken to destroy private information beyond a doubt before it leaves the hands of any financial institution.

upvoted 1 times

Shaza123 3 years, 6 months ago

The correct answer is A.

upvoted 3 times

Question #40 *Topic 1*

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.

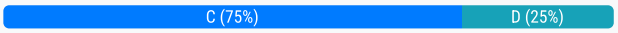
B. After disclosing marketing practices to customers and after giving them an opportunity to opt in.

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.

Suggested Answer: *C*

Community vote distribution



twiny Most Recent 2 years ago

The correct answer is C. After disclosing information-sharing practices to customers and after giving them an opportunity to opt out. Reference: The IAPP textbook, U.S. Private-Sector Privacy, 4th Edition, 2024, Section 9.3.2 The GLBA Privacy Rule: "In addition, other than for defined exceptions, a financial institution may also share consumer information with nonaffiliated companies and other third parties, but only after disclosing information-sharing practices to customers and providing them with the opportunity to opt out."

upvoted 1 times

Bhimesh 2 years, 5 months ago

The Gramm-Leach-Bliley Act seeks to protect consumer financial privacy. Its provisions limit when a "financial institution" may disclose a consumer's "nonpublic personal information" to nonaffiliated third parties. The law covers a broad range of financial institutions, including many companies not traditionally considered to be financial institutions because they engage in certain "financial activities." Financial institutions must notify their customers about their information-sharing practices and tell consumers of their right to "opt-out" if they don't want their information shared with certain nonaffiliated third parties. In addition, any entity that receives consumer financial information from a financial institution may be restricted in its reuse and redisclosure of that information.Note: While the GLB Act does not require you to provide an opt-out notice if you only disclose NPI to affiliates, if you share certain information with your affiliates, you may have an obligation to provide an opt-out notice under the Fair Credit Reporting Act. That opt-out notice must be included in your GLB privacy notice

upvoted 1 times

Bhimesh 2 years, 5 months ago

Selected Answer: C

The Gramm-Leach-Bliley Act seeks to protect consumer financial privacy. Its provisions limit when a "financial institution" may disclose a consumer's "nonpublic personal information" to nonaffiliated third parties. The law covers a broad range of financial institutions, including many companies not traditionally considered to be financial institutions because they engage in certain "financial activities." Financial institutions must notify their customers about their information-sharing practices and tell consumers of their right to "opt-out" if they don't want their information shared with certain nonaffiliated third parties. In addition, any entity that receives consumer financial information from a financial institution may be restricted in its reuse and redisclosure of that information.

upvoted 1 times

Bhimesh 2 years, 5 months ago

Note: While the GLB Act does not require you to provide an opt-out notice if you only disclose NPI to affiliates, if you share certain information with your affiliates, you may have an obligation to provide an opt-out notice under the Fair Credit Reporting Act. That opt-out notice must be included in your GLB privacy notice

upvoted 1 times

Z1682009 2 years, 7 months ago

A financial institution may also share consumer information with nonaffiliated companies and other third parties, but only after disclosing information-sharing practices to customers and providing them with the opportunity to opt out. IAPP 9.3.2 (page 233). The correct answer is C.

upvoted 1 times

jjjrbm 2 years, 10 months ago

Correct Answer is C. information with nonaffiliated companies and other third parties, but only after disclosing information-sharing practices to customers and providing them with the opportunity to opt out.

upvoted 1 times

Ambulocetus 3 years, 1 month ago

https://www.ftc.gov/business-guidance/resources/how-comply-privacy-consumer-financial-information-rule-gramm-leach-bliley-act "If you share their NPI with nonaffiliated third parties outside of three exceptions (see "Exceptions"), you must give your consumers and customers an "opt-out notice" that clearly and conspicuously describes their right to opt out of the information being shared. An opt-out notice must be delivered with a privacy notice, and it can be part of the privacy notice."

upvoted 1 times

Boats 3 years, 4 months ago

https://www.ecfr.gov/current/title-12/chapter-X/part-1022/subpart-C Example. A consumer has a homeowner's insurance policy with an insurance company. The insurance company furnishes eligibility information about the consumer to its affiliated creditor. Based on that eligibility information, the creditor wants to make a solicitation to the consumer about its home equity loan products. The creditor does not have a pre-existing business relationship with the consumer and none of the other exceptions apply. The creditor is prohibited from using eligibility information received from its insurance affiliate to make solicitations to the consumer about its home equity loan products unless the consumer is given a notice and opportunity to opt out and the consumer does not opt out.§ 1022.21 Affiliate marketing opt-out and exceptions. (i) It is clearly and conspicuously disclosed to the consumer in writing or, if the consumer agrees, electronically, in a concise notice that you may use eligibility information about that consumer received from an affiliate to make solicitations for marketing purposes to the consumer; (ii) The consumer is provided a reasonable opportunity and a reasonable and simple method to “opt out,” or prohibit you from using eligibility information to make solicitations for marketing purposes to the consumer; andHey boats. Love your responses in general, but I think you're off here. You're (correctly) addressing a situation in which the third party is *affiliated*. Here, the prompt states the the third party is *not* affiliated.

upvoted 1 times

Boats 3 years, 4 months ago

Selected Answer: D

https://www.ecfr.gov/current/title-12/chapter-X/part-1022/subpart-C

Example. A consumer has a homeowner's insurance policy with an insurance company. The insurance company furnishes eligibility information about the consumer to its affiliated creditor. Based on that eligibility information, the creditor wants to make a solicitation to the consumer about its home equity loan products. The creditor does not have a pre-existing business relationship with the consumer and none of the other exceptions apply. The creditor is prohibited from using eligibility information received from its insurance affiliate to make solicitations to the consumer about its home equity loan products unless the consumer is given a notice and opportunity to opt out and the consumer does not opt out.

upvoted 1 times

Boats 3 years, 4 months ago

§ 1022.21 Affiliate marketing opt-out and exceptions.

(i) It is clearly and conspicuously disclosed to the consumer in writing or, if the consumer agrees, electronically, in a concise notice that you may use eligibility information about that consumer received from an affiliate to make solicitations for marketing purposes to the consumer;

(ii) The consumer is provided a reasonable opportunity and a reasonable and simple method to “opt out,” or prohibit you from using eligibility information to make solicitations for marketing purposes to the consumer; and

upvoted 1 times

Boats 3 years, 4 months ago

§ 1022.21 Affiliate marketing opt-out and exceptions. (i) It is clearly and conspicuously disclosed to the consumer in writing or, if the consumer agrees, electronically, in a concise notice that you may use eligibility information about that consumer received from an affiliate to make solicitations for marketing purposes to the consumer; (ii) The consumer is provided a reasonable opportunity and a reasonable and simple method to “opt out,” or prohibit you from using eligibility information to make solicitations for marketing purposes to the consumer; andHey boats. Love your responses in general, but I think you're off here. You're (correctly) addressing a situation in which the third party is *affiliated*. Here, the prompt states the the third party is *not* affiliated.

upvoted 1 times

FDFDSFDSF 3 years, 1 month ago

Hey boats. Love your responses in general, but I think you're off here. You're (correctly) addressing a situation in which the third party is *affiliated*. Here, the prompt states the the third party is *not* affiliated.

upvoted 2 times

Supp2023 3 years, 5 months ago

Consumers must opt-in before a financial institution may share financial information with a non-affiliated third party. A is right answer. Can someone confirm?

upvoted 1 times

Question #41 *Topic 1*

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

Suggested Answer: *D*

Community vote distribution

D (100%)

twiny Most Recent 2 years ago

The correct answer is D. Offer an Opt-Out before transferring PI to an unaffiliated third party for the latter's own use. Reference: The IAPP textbook, U.S. Private-Sector Privacy, 4th Edition, 2024, Section 9.3.2 The GLBA Privacy Rule: "In addition, other than for defined exceptions, a financial institution may also share consumer information with nonaffiliated companies and other third parties, but only after disclosing information-sharing practices to customers and providing them with the opportunity to opt out."

upvoted 1 times

Bhimesh 2 years, 5 months ago

D. Offer an Opt-Out before transferring PI to an unaffiliated third party for the latter's own use Section 502 describes "Obligations with Respect to Disclosures of Personal Information." The GLBA requires that financial institutions share their privacy policies and practices with consumers in writing. Also, if the financial institution wants to share consumer nonpublic personal information(NPI) with nonaffiliated third parties, "the financial institution must give consumers the right to opt-out from the information sharing".The Gramm-Leach-Bliley Act requires financial institutions – companies that offer consumers financial products or services like loans, financial or investment advice, or insurance – to explain their information-sharing practices to their customers and to safeguard sensitive data.What is a nonaffiliated third party? A party that is not related by common ownership or corporate control. Under the GLBA, financial institutions must give consumers and customers a privacy notice with opt-out rights if they want to share nonpublic personal information with nonaffiliated third parties.C. Provide consumers with the opportunity to opt out of receiving telemarketing phone calls It should be noted that the GLBA prohibits financial institutions from disclosing consumer account numbers to non-affiliated companies for purposes of ' TELEMARKETING AND DIRECT MAIL MARKETING ' (including through email), even if the consumer has not opted out of sharing the information for marketing purposesFinancial institution may share any information it has with its" AFFILIATED "companies and joint marketing partners, which are other financial institutions with whom the entity jointly markets a financial product or service Provided – Privacy notice standard is met What information the financial institution collects about its consumers and customers? With whom it shares the information? How it protects or safeguards the information? An explanation of how a consumer may opt out of

upvoted 1 times

Bhimesh 2 years, 5 months ago

Selected Answer: D

D. Offer an Opt-Out before transferring PI to an unaffiliated third party for the latter's own use

Section 502 describes "Obligations with Respect to Disclosures of Personal Information."

The GLBA requires that financial institutions share their privacy policies and practices with consumers in writing.

Also, if the financial institution wants to share consumer nonpublic personal information(NPI) with nonaffiliated third parties, "the financial institution must give consumers the right to opt-out from the information sharing".

upvoted 1 times

Bhimesh 2 years, 5 months ago

The Gramm-Leach-Bliley Act requires financial institutions – companies that offer consumers financial products or services like loans, financial or investment advice, or insurance – to explain their information-sharing practices to their customers and to safeguard sensitive data.

upvoted 1 times

Bhimesh 2 years, 5 months ago

What is a nonaffiliated third party? A party that is not related by common ownership or corporate control. Under the GLBA, financial institutions must give consumers and customers a privacy notice with opt-out rights if they want to share nonpublic personal information with nonaffiliated third parties.

upvoted 1 times

Bhimesh 2 years, 5 months ago

C. Provide consumers with the opportunity to opt out of receiving telemarketing phone calls It should be noted that the GLBA prohibits financial institutions from disclosing consumer account numbers to non-affiliated companies for purposes of ' TELEMARKETING AND DIRECT MAIL MARKETING ' (including through email), even if the consumer has not opted out of sharing the information for marketing purposes

upvoted 1 times

Bhimesh 2 years, 5 months ago

Financial institution may share any information it has with its" AFFILIATED "companies and joint marketing partners, which are other financial institutions with whom the entity jointly markets a financial product or service Provided – Privacy notice standard is met What information the financial institution collects about its consumers and customers? With whom it shares the information? How it protects or safeguards the information? An explanation of how a consumer may opt out of having their information shared through a reasonable 'OPT-OUT' process

upvoted 1 times

Question #42 *Topic 1*

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

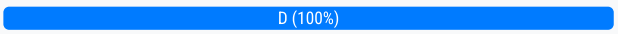
B. By speaking to a patient without prior authorization

C. By ignoring the conversation about a potential breach

D. By following through with his plans for his upcoming paper

Suggested Answer: *C*

Community vote distribution



impchoi Highly Voted 3 years, 9 months ago

Should be D: "Other than for treatment, covered entities must make reasonable efforts to limit the use and disclosure of PHI to the minimum necessary in order to accomplish the intended purpose." He isn't involved in the potential breach, which is why he isn't trained for it, and doesn't know all the facts of the situation. He has not obligation doesn't need to investigate any further based on anything that he heard.

upvoted 6 times

twiny Most Recent 2 years ago

The correct answer is D. By following through with his plans for his upcoming paper. HIPAA violations can occur when an individual's PHI is improperly disclosed without consent. In this scenario, Declan is planning to use John's name and information related to his medical situation for a paper, which would be a direct violation of HIPAA. Sharing patient information, especially identifying details like names, without explicit authorization is prohibited under HIPAA, unless certain exceptions apply (such as for treatment, payment, or healthcare operations). Since John has not given consent for his information to be shared (Declan did not even ask for it), Declan would be violating HIPAA by including this information in his paper.
According to the author, the correct answer is C. By ignoring the conversation about a potential breach. While reporting breaches is important and ignoring the conversation about a potential breach may be ethically concerning, it is not a direct HIPAA violation.

upvoted 2 times

Bhimesh 2 years, 5 months ago

What is the most likely way that Declan might “DIRECTLY” violate the Health Insurance Portability and Accountability Act (HIPAA)? Should be D. By following through with his plans for his upcoming paper - (Directly) • A. By being present when patients are checking in – it wont violate the HIPAA • B. By speaking to a patient without prior authorization – it wont hurt • C. By ignoring the conversation about a potential breach –INDIRECT – overheard, this would be considered hearsay, which is generally inadmissible • D. By following through with his plans for his upcoming paper - Directly A HIPAA violation refers to the failure to comply with HIPAA rules, which can include ‘Unauthorized access, use, or Disclosure ‘ of Protected Health Information (PHI),

upvoted 2 times

Supp2023 3 years, 5 months ago

In my opinion, C is still right- as a hospital employee, if he ignores the conversation about the breach, then he is equally responsible. Although, I believe the hospital would be at fault here, not each individual employee. Thoughts anyone?

upvoted 2 times

Question #43 *Topic 1*

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

Suggested Answer: *C*

Community vote distribution

D (100%)

impchoi Highly Voted 3 years, 9 months ago

D: "Privacy notices. The Privacy Rule generally requires a covered entity to provide a detailed privacy notice at the date of first service delivery. There are some defined exceptions to the notice requirements. For example, a privacy notice does not have to be provided when the healthcare provider has an "indirect treatment relationship" with the patient or in the case of medical emergencies. The rule is quite specific about elements that must be included in the notice, including detailed statements about individuals' rights with respect to their PHI."The correct answer is C. It is important for test takers to not add additional information to the prompt by assuming information. By choosing D, you are assuming that Declan will stay long enough in the position that he will personally see to it that every first time patient receives a privacy notice. By choosing C, you are answering the exact question by addressing the paper waste concern and complying with HIPAA which allows covered entities to post privacy notices on websites. Model Notices of Privacy Practices on the HHS website outlines two requirements: A covered entity must make its notice available to any person who asks for it (satisfies pointing the person in the direction of the covered entity website); A covered entity must prominently post and make available its notice on any web site it maintains that provides information about its customer services or benefits (satisfies pointing the person to the covered entity website to view privacy notice).

upvoted 7 times

impchoi Highly Voted 3 years, 9 months ago

D: "Privacy notices. The Privacy Rule generally requires a covered entity to provide a detailed privacy notice at the date of first service delivery. There are some defined exceptions to the notice requirements. For example, a privacy notice does not have to be provided when the healthcare provider has an “indirect treatment relationship” with the patient or in the case of medical emergencies. The rule is quite specific about elements that must be included in the notice, including detailed statements about individuals’ rights with respect to their PHI."

upvoted 7 times

[Removed] 3 years, 5 months ago

The correct answer is C. It is important for test takers to not add additional information to the prompt by assuming information. By choosing D, you are assuming that Declan will stay long enough in the position that he will personally see to it that every first time patient receives a privacy notice. By choosing C, you are answering the exact question by addressing the paper waste concern and complying with HIPAA which allows covered entities to post privacy notices on websites. Model Notices of Privacy Practices on the HHS website outlines two requirements: A covered entity must make its notice available to any person who asks for it (satisfies pointing the person in the direction of the covered entity website); A covered entity must prominently post and make available its notice on any web site it maintains that provides information about its customer services or benefits (satisfies pointing the person to the covered entity website to view privacy notice).

upvoted 4 times

BrianVelasquez Most Recent 3 months ago

The radiology department can address Declan's concern and reduce paper waste by confirming patients are provided the privacy notice only on their first visit, as HIPAA only requires providers to give the notice once (at the start of services) and make a good-faith effort to obtain written acknowledgment

upvoted 1 times

twiny 2 years ago

Initially, I selected C. However, after reading the IAPP textbook, I realized the correct answer was D. Confirm that patients are given the privacy notice on their first visit. Reference: The IAPP textbook, U.S. Private-Sector Privacy, 4th Edition, 2024, Section 8.1.1 The HIPAA Privacy Rule, " - Privacy notices. The Privacy Rule generally requires a covered entity to provide a detailed privacy notice at the date of first service delivery."

upvoted 1 times

Bhimesh 2 years, 5 months ago

Should be D - Privacy notices. The Privacy Rule generally requires a covered entity to provide a detailed privacy notice at the date of FIRST SERVICE DELIVERY.

upvoted 1 times

jjjrbm 2 years, 10 months ago

answer is D

upvoted 1 times

Question #44 *Topic 1*

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

Suggested Answer: *C*

Community vote distribution

C (100%)

twiny Most Recent 2 years ago

The correct answer is C. By pointing out that contracts are in place to help ensure the observance of minimum security standards. Reference: The IAPP textbook, U.S. Private-Sector Privacy, 4th Edition, 2024, Section 8.1.2 The HIPAA Security Rule, "The HIPPA Security Rule was finalized in February 2003 and modified in January 2013. It establishes minimum security requirements for PHI that a covered entity or a business associate receives, creates, maintains, or transmits in electronic form."

upvoted 1 times

Bhimesh 2 years, 5 months ago

Should be C. By pointing out that contracts are in place to help ensure the observance of minimum security standards The Minimum Information Security Standards is a standard for the minimum information security measures that any institution MUST put in place for sensitive or classified information to protect national security.

upvoted 2 times

Question #45 *Topic 1*

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

Suggested Answer: *D*

Community vote distribution

A (100%)

twiny Most Recent 2 years ago

The correct answer is A. For-profit organizations and for-profit telefunders regarding charitable solicitations. Reference: The IAPP textbook, U.S. Private-Sector Privacy, 4th Edition, 2024, Section 11.1.2.1 Exceptions to the DNC Rules: "DNC rules apply to for-profit organizations and cover charitable solicitations placed by for-profit telefunders. DNC rules do not apply to: - Nonprofits calling on their own behalf - Calls to customers with an existing relationship within the last 18 months - Inbound calls, provided that there is no “upsell” of additional products or services - Most business-to-business calls" I'm not sure why the author selected choice D as the correct answer. The TSR specifically applies to for-profit telemarketing activities. Not-for-profit organizations are generally not subject to the TSR, except when for-profit telefunders are involved.

upvoted 1 times

Bhimesh 2 years, 5 months ago

DNC rules apply to for-profit organizations and cover charitable solicitations placed by for-profit telefunders. Exceptions to the DNC Rules - DNC rules do not apply to: (i) Nonprofits calling on their own behalf (ii) Calls to customers with an existing relationship within the last 18 months (iii) Inbound calls, provided that there is no “upsell” of additional products or services (iv) Most business-to-business calls

upvoted 1 times

jjjrbm 2 years, 10 months ago

A is the right answer

upvoted 1 times

testaking917 3 years ago

Answer A is correct. IAPP book page 278

upvoted 1 times

fabianocamilos 3 years, 3 months ago

Some types of businesses are not covered by the TSR even though they conduct telemarketing campaigns that may involve some interstate telephone calls to sell goods or services. These three types of entities are not subject to the FTC’s jurisdiction, and are not covered by the TSR: 1. banks, federal credit unions, and federal savings and loans. 2. common carriers — such as long-distance telephone companies and airlines — when they are engaging in common carrier activity. 3. NON-PROFIT ORGANIZATIONS — those entities that are not organized to carry on business for their own, or their members’, profit. https://www.ftc.gov/business-guidance/resources/complying-telemarketing-sales-rule#comply

upvoted 2 times

Question #46 *Topic 1*

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 date and must state the times when calls can be made

Suggested Answer: *B*

Community vote distribution

C (100%)

impchoi Highly Voted 3 years, 9 months ago

C: "The TSR allows sellers and telemarketers to call consumers who consent to receive such calls. This consent must be in writing, must state the number to which calls may be made, and must include the consumer's signature. (A valid electronic signature is acceptable.)"

upvoted 8 times

twiny Most Recent 2 years ago

"The correct answer is C. The consent must be in writing, must contain the number to which calls can be made and must be signed. Reference: The IAPP textbook, U.S. Private-Sector Privacy, 4th Edition, 2024, Section 11.1.2.1 Exceptions to the DNC Rules: "Exception Based on Consent. The TSR allows sellers and telemarketers to call consumers who consent to receive such calls. This consent must be in writing, must state the number to which calls may be made, and must include the consumer's signature. A valid electronic signature is acceptable."

upvoted 1 times

Bhimesh 2 years, 5 months ago

Exception Based on Consent The TSR allows sellers and telemarketers to call consumers who consent to receive such calls. This consent must be in writing, must state the number to which calls may be made, and MUST include the consumer's signature. (A valid electronic signature is acceptable.) What must the written agreement contain? A written agreement need only contain: • unambiguous evidence that a call recipient is willing to receive telephone calls that deliver a prerecorded message by or on behalf of a specific seller; • the telephone number to which such messages may be delivered; and • the call recipient's signature.

upvoted 1 times

Boats 3 years, 4 months ago

https://www.ftc.gov/business-guidance/resources/complying-telemarketing-sales-rule#writtenagreement What must the written agreement contain? A written agreement need only contain: - unambiguous evidence that a call recipient is willing to receive telephone calls that deliver a - prerecorded message by or on behalf of a specific seller; the telephone number to which such messages may be delivered; and - the call recipient's signature.

upvoted 2 times

Question #47 *Topic 1*

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

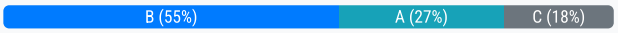
B. When the goods and services sold by its divisions are very similar

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

Suggested Answer: *C*

Community vote distribution



BrianVelasquez Most Recent 3 months ago

Under the FTC Telemarketing Sales Rule, an organization's divisions are generally considered separate entities unless there is substantial commonality between them. If a company's divisions sell very similar goods or services and share the same operational structure, a consumer's do-not-call request to one division is legally binding and must be shared across the related divisions.

upvoted 1 times

donisfattoo 1 year, 8 months ago

This is really tough....I think it could be A or B, but I'm leaning A based on the language cited in Twiny's answer "...a single seller without distinct corporate divisions may not call a consumer who asks not to be called again, even if the seller is offering a different good or service for sale." I think the lack of distinct corporate divisions is what makes it required for the entity specific DNC request to be shared throughout the corporation. Not the distinction on the goods being sold (whether similar or not). Obviously, its a close call

upvoted 2 times

twiny 2 years ago

Here is a citation from the FTC itself, published on it website: https://www.ftc.gov/business-guidance/resources/complying-telemarketing-sales-rule "What if a consumer asks a specific division of a corporation not to call? Does a call from a different division violate the TSR? Distinct corporate divisions generally are considered separate sellers under the TSR." "If a consumer tells one division of a company not to call again, a distinct corporate division of the same company may make another telemarketing call to that consumer. Nevertheless, a single seller without distinct corporate divisions may not call a consumer who asks not to be called again, even if the seller is offering a different good or service for sale." This implies that as long as the divisions of the organization are selling similar products or services, if a consumer asks not to be called, that request must apply across the entire organization and its affiliates to respect the consumer's preferences and avoid violating the Do-Not-Call (DNC) rules.

upvoted 3 times

joats245 2 years ago

Changing my answer....I'm going with B. The rule states that there needs to be diversity in operational structures, not that it has to be transparent. I think the fact that similar products are sold would trigger this requirement. In making a determination whether a corporate division is a separate entity for purposes of this rule, sellers must consider "whether there is substantial diversity between the operational structure of the divisions and whether the goods or services sold by the divisions are substantially different from each other."

upvoted 2 times

joats245 2 years ago

A or B? In making a determination whether a corporate division is a separate entity for purposes of this rule, sellers must consider "whether there is substantial diversity between the operational structure of the divisions and whether the goods or services sold by the divisions are substantially different from each other."

upvoted 1 times

Bhimesh 2 years, 5 months ago

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

upvoted 2 times

Question #48 *Topic 1*

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

Suggested Answer: *B*

Community vote distribution

B (100%)

twiny Most Recent 2 years ago

The correct answer is B. 10 days. References: 1. The IAPP textbook, U.S. Private-Sector Privacy, 4th Edition, 2024, Section 11.3 Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003: The CAN-SPAM Act "Prohibits sending commercial email (following a grace period of 10 business days) to an individual who has asked not to receive future email." 2. The IAPP textbook, U.S. Private-Sector Privacy, 4th Edition, 2024, Section 11.3.2 Express Prior Authorization: "The FCC rule maintains the CAN-SPAM-mandated 10-business-day grace period following a revoked authorization, after which messages cannot be sent."

upvoted 1 times

Bhimesh 2 years, 5 months ago

Honor opt-out requests promptly. Any opt-out mechanism you offer must be able to process opt-out requests for at least 30 days after you send your message. You must honor a recipient's opt-out request" within 10 business days". You can't charge a fee, require the recipient to give you any personally identifying information beyond an email address, or make the recipient take any step other than sending a reply email or visiting a single page on an Internet website as a condition for honoring an opt-out request. Once people have told you they don't want to receive more messages from you, you can't sell or transfer their email addresses, even in the form of a mailing list

upvoted 1 times

Romeokton 2 years, 7 months ago

B it is.

upvoted 1 times

Question #49 *Topic 1*

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

Suggested Answer: *C*

Community vote distribution

C (100%)

Bhimesh Most Recent 1 year, 11 months ago

Should be C - Status of the Student on Their Parents' Tax Return Even after the rights under FERPA have transferred to the student, a school may disclose to the parents the educational records of the student - without the student's consent - in the circumstance where the student is a dependent for tax purposes...

upvoted 1 times

Boats 2 years, 10 months ago

https://es.vccs.edu/about/family-educational-rights-and-privacy-act-ferpa/ The disclosure is to a parent who legally declares the student as a dependent, as defined by 20 U.S.C. § 1232g. (NOTE: Regardless of the student's age, a parent seeking access to their son or daughter's educational record must present proof upon each request of their child's dependency to the Registrar's Office by way of the most recent year's federal tax return.)

upvoted 2 times

Question #50 *Topic 1*

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

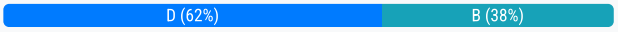
B. It requires the owner to implement an identity theft warning system

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

Suggested Answer: *A*

Community vote distribution



Bhimesh 1 year, 11 months ago

Should be D The Red Flag Program Clarification Act of 2010 was passed in response to concern that the definition of creditor extended to implicate unintended entities, such as attorneys and health providers, simply because they allow customers to pay their bills after the time of service . The clarification narrows the previously broad definition of creditor, as well as the circumstances under which they are covered by the rule. It eliminates entities that extend credit only “for expenses incidental to a service.” FACTA rule requires certain financial entities to develop and implement written identity theft detection programs that can identify and respond to the “red flags” that signal identity theft. Specifically, the rule applies to Financial institutions and creditors.“Financial institution” is defined as all banks, savings and loan associations and credit unions. It also includes all other entities that hold a “transaction account” belonging to a consumer. FACTA rule applies to entities that, regularly and in the course of business: Obtain or use consumer reports in connection with a credit transaction Furnish information to consumer reporting agencies in connection with a credit transaction Advance funds to or on behalf of someone, except for expenses incidental to a service provided by the creditor to that person The new law also authorizes regulations that apply the rule to businesses whose accounts should be “subject to a reasonably foreseeable risk of identity theft.”

upvoted 1 times

Bhimesh 1 year, 11 months ago

Selected Answer: D

Should be D The Red Flag Program Clarification Act of 2010 was passed in response to concern that the definition of creditor extended to implicate unintended entities, such as attorneys and health providers, simply because they allow customers to pay their bills after the time of service .

The clarification narrows the previously broad definition of creditor, as well as the circumstances under which they are covered by the rule. It eliminates entities that extend credit only “for expenses incidental to a service.”

FACTA rule requires certain financial entities to develop and implement written identity theft detection programs that can identify and respond to the “red flags” that signal identity theft. Specifically, the rule applies to Financial institutions and creditors.

upvoted 1 times

Bhimesh 1 year, 11 months ago

“Financial institution” is defined as all banks, savings and loan associations and credit unions. It also includes all other entities that hold a “transaction account” belonging to a consumer. FACTA rule applies to entities that, regularly and in the course of business: Obtain or use consumer reports in connection with a credit transaction Furnish information to consumer reporting agencies in connection with a credit transaction Advance funds to or on behalf of someone, except for expenses incidental to a service provided by the creditor to that person The new law also authorizes regulations that apply the rule to businesses whose accounts should be “subject to a reasonably foreseeable risk of identity theft.”

upvoted 1 times

Stevenciu 2 years ago

Selected Answer: B

Even though the grocery store might not be a traditional financial institution, FACTA's Red Flags Rule applies to them as a "creditor" because they offer money wire services, a form of credit under FACTA. This means they are required to have a program to identify and address potential red flags for identity theft.

FACTA's definition of "creditor" is broader than the traditional definition and applies to businesses that regularly extend credit in connection with the offering or sale of a product or service. In this case, by offering money wire services, the grocery store is essentially extending credit (facilitating the transfer of funds) and falls under FACTA's definition of a creditor for the purposes of the Red Flags Rule.

upvoted 3 times

Stevenciu 2 years ago

Even though the grocery store might not be a traditional financial institution, FACTA's Red Flags Rule applies to them as a "creditor" because they offer money wire services, a form of credit under FACTA. This means they are required to have a program to identify and address potential red flags for identity theft. FACTA's definition of "creditor" is broader than the traditional definition and applies to businesses that regularly extend credit in connection with the offering or sale of a product or service. In this case, by offering money wire services, the grocery store is essentially extending credit (facilitating the transfer of funds) and falls under FACTA's definition of a creditor for the purposes of the Red Flags Rule.The logic is right, however the framing of question is tricky. The grocery owner in question "uses" a wire transfer service, doesn't "offer".I agree.

upvoted 3 times

workatfirst Most Recent 7 months ago

The logic is right, however the framing of question is tricky. The grocery owner in question "uses" a wire transfer service, doesn't "offer".

upvoted 1 times

examdj101j 1 year, 11 months ago

I agree.

upvoted 1 times

jjjrbm 2 years, 4 months ago

D is the correct answer

upvoted 2 times

Privaceeeeee9876 2 years, 10 months ago

I think it is D because the red flags rule revolves around protecting identity theft and the grocery store is not a financial entity

upvoted 2 times

Boats 2 years, 10 months ago

I don't think this business is covered by FACTA. This business does not have covered accounts. https://www.ftc.gov/business-guidance/resources/fighting-identity-theft-red-flags-rule-how-guide-business#who

upvoted 4 times

Qwamer 3 years ago

The answer should be B, on page 228 in section 9.2.2, under the "Red Flags Rule", "certain financial entities to develop and implement written identity detection programs that can identify and respond to the "red flags" that signal identity theft."

upvoted 4 times

Question #51 *Topic 1*

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

Suggested Answer: *B*

Community vote distribution

B (100%)

Bhimesh Most Recent 1 year, 11 months ago

Dodd-Frank Wall Street Reform and Consumer Protection Act Abusive practices are defined by Dodd–Frank and enforceable by the CFPB. An abusive practice is any act that "materially interferes with the ability of a consumer to understand a term or condition of a consumer financial product or service." Practices are also considered abusive if they exploit consumer misunderstanding, consumers who are unable to understand the terms, or a consumer relying on a third-party who may be exploiting them.

upvoted 1 times

Question #52 *Topic 1*

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

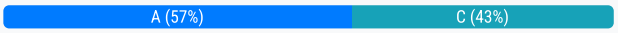
B. A university posts a public student directory that includes names, hometowns, e-mail addresses, and majors

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

Suggested Answer: *A*

Community vote distribution



BrianVelasquez Most Recent 3 months ago

While academic honors are public achievements, disclosing performance metrics (such as grades/honor rolls) along with specific identifying information from education records requires prior written consent from the parent or eligible student. Newspapers are third parties without consent.

upvoted 1 times

fightingpotato 1 year, 11 months ago

Option C, where a newspaper prints the names, grade levels, and hometowns of students who made the quarterly honor roll, does not typically violate FERPA because it is generally considered directory information. FERPA allows schools to designate certain information, such as names and honors, as directory information that can be disclosed without consent, provided the school has informed parents and students of their rights and the opportunity to opt out of such disclosures. However, the specifics can depend on the school's policy regarding directory information and whether the students have opted out. So, while C may raise concerns, it usually wouldn't violate FERPA unless the students' information was classified differently by the school. Option A, on the other hand, clearly violates FERPA as it involves disclosing identifiable student work without consent.

upvoted 2 times

6c5c57c 2 years ago

I agree with ianwayne14. It should be option A.

upvoted 2 times

ianwayne14 2 years, 1 month ago

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.

upvoted 3 times

Bhimesh 2 years, 5 months ago

FERPA -The statute generally prevents schools from divulging education record information, such as grades and behaviour, to parties other than the student without that student's consent • B. A university posts a public student directory that includes names, hometowns, e-mail addresses, and majors "Directory information" is broadly defined by FERPA to include information that would not generally be considered an invasion of privacy or harmful if disclosed • D. University police provide an arrest report to a student's hometown police, who suspect him of a similar crime The term education record has several important exceptions. The following record is not considered education records under FERPA: • Campus police records created and maintained by school campus police for law enforcement purposes

upvoted 2 times

YoshiYogi 2 years, 5 months ago

I would agree

upvoted 1 times

jjjrbm 2 years, 10 months ago

The act that violates the Family Educational Rights and Privacy Act of 1974 (FERPA) is: C. A newspaper prints the names, grade levels, and hometowns of students who made the quarterly honor roll. FERPA protects the privacy of students' educational records and generally prohibits the disclosure of personally identifiable information from those records without the student's consent. Options A, B, and D do not necessarily violate FERPA. Option A involves the use of a student's essay with permission. Option B involves public directory information, which can be disclosed under FERPA. Option D involves a potential law enforcement action and is not directly related to educational records disclosure.

upvoted 3 times

Question #53 *Topic 1*

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

Suggested Answer: *D*

Community vote distribution

D (100%)

Bhimesh Most Recent 1 year, 11 months ago

Disclosure to educational institutions in which a student seeks or intends to enroll, or is currently enrolled, when the disclosure is for a purpose related to the student's enrollment or transfer.

upvoted 1 times

Question #54 *Topic 1*

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

Suggested Answer: *D*

Community vote distribution

D (100%)

Bhimesh Most Recent 1 year, 11 months ago

The CAN-SPAM Act doesn't apply just to bulk email. It covers all commercial messages, which the law defines as "any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service," including email that promotes content on commercial websites. The law makes no exception for business-to-business email. That means all email – for example, a message to former customers announcing a new product line – must comply with the law.

upvoted 1 times

Question #55 *Topic 1*

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

Suggested Answer: *A*

Community vote distribution

A (100%)

Bhimesh 1 year, 11 months ago

Selected Answer: A

The Video Privacy Protection Act of 1988 (VPPA) was passed in response to the disclosure and publication of then-Supreme Court nominee Robert Bork's "video rental records". The disclosure was considered a gross invasion of his privacy

Videotape service providers are prohibited from disclosing customer personal information unless an enumerated exception applies.

The Video Privacy Protection Act (VPPA) was passed in 1988,back in the days when customers still went to video stores to rent movies to watch at home. The VPPA was designed to project an individual's video rental or purchase history from potentially embarrassing disclosure.

upvoted 1 times

Bhimesh 1 year, 11 months ago

The Video Privacy Protection Act of 1988 (VPPA) was passed in response to the disclosure and publication of then-Supreme Court nominee Robert Bork's "video rental records". The disclosure was considered a gross invasion of his privacy Videotape service providers are prohibited from disclosing customer personal information unless an enumerated exception applies. The Video Privacy Protection Act (VPPA) was passed in 1988,back in the days when customers still went to video stores to rent movies to watch at home. The VPPA was designed to project an individual's video rental or purchase history from potentially embarrassing disclosure.Video Privacy Protection Act of 1988 (VPPA) Scope VPPA applies to any PII collected from a consumer during transactions to rent, buy, or subscribe to the services or products of a videotape service provider. Such providers include anyone involved in providing audio/video materials for rental or purchase. Those who deliver audio video materials are also considered videotape service providers under the law.

upvoted 1 times

Bhimesh **Most Recent** 1 year, 11 months ago

Video Privacy Protection Act of 1988 (VPPA) Scope VPPA applies to any PII collected from a consumer during transactions to rent, buy, or subscribe to the services or products of a videotape service provider. Such providers include anyone involved in providing audio/video materials for rental or purchase. Those who deliver audio video materials are also considered videotape service providers under the law.

upvoted 1 times

Question #56 *Topic 1*

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

Suggested Answer: *C*

Community vote distribution

A (100%)

Qwamer Highly Voted 3 years ago

The answer should be A. In Section 11.5 of the book on page 288, "At the time entering into an agreement to provide cable services, and on an annual basis thereafter, cable service providers are required to give subscribers a privacy notice that "clearly and conspicuously" informs subscribers...".

upvoted 13 times

Bhimesh Most Recent 1 year, 11 months ago

The Cable Communications Policy Act of 1984 regulates the notice a cable television provider must furnish to customers, the ability of cable providers to collect personal information, the ability of cable providers to disseminate personal information and the retention and destruction of personal information by cable television providers. At the time of entering into an agreement to provide cable services, and on an annual basis thereafter, cable service providers are required to give subscribers a privacy notice that “clearly and conspicuously” informs subscribers of (1) the nature of the personal information collected, (2) how such information will be used, (3) the retention period of such information, and (4) the manner by which a subscriber can access and correct such information.

upvoted 2 times

Stevenciu 1 year, 12 months ago

The Cable Communications Policy Act of 1984 established guidelines to protect the privacy of cable television subscribers. One of its key provisions is the requirement for cable operators to provide subscribers with an annual notice. This notice must detail the nature of personally identifiable information collected, how it will be used, under what conditions it may be disclosed, and the rights of subscribers regarding this information. This act aims to ensure that subscribers are informed about their privacy rights and the use of their personal information by cable service providers.

upvoted 1 times

jjjrbm 2 years, 4 months ago

answer is A

upvoted 2 times

Question #57 *Topic 1*

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

Suggested Answer: *B*

Community vote distribution

B (100%)

Bhimesh Most Recent 1 year, 11 months ago

The FCC has rules in place to ban sending commercial advertising wirelessly to mobile phones without obtaining specific consent from a recipient in advance. These rules are designed to prevent advertisers from spamming cell phones with text messages, thus clogging cellular networks and incurring charges for mobile subscribers. This rule applies to messages sent directly to mobile phones using technologies like SMS text messaging. It does not apply, for example, to email messages that recipients may happen to read via email apps on their smartphones. But message senders need a way to know which domains these are so that they can avoid sending to those domains without prior consent. For this reason, the FCC created the Wireless Domain Registry of Internet domain names that are used to distribute messages to mobile devices, primarily as SMS text messages. Mobile service providers are required to submit updated domain names to the list and to report any updates or changes within 30 days.

upvoted 1 times

Romeokton 2 years, 1 month ago

One vote for B from me.

upvoted 2 times

Question #58 *Topic 1*

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

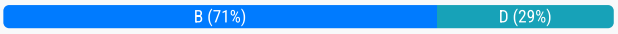
B. Because HealthCo did not conduct due diligence to verify or monitor CloudHealth's security measures

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

Suggested Answer: *B*

Community vote distribution



fightingpotato Most Recent 1 year, 11 months ago

The most significant reason that the U.S. Department of Health and Human Services (HHS) might impose a penalty on HealthCo is B. Because HealthCo did not conduct due diligence to verify or monitor CloudHealth's security measures. Under HIPAA, covered entities are responsible for ensuring that their business associates implement adequate security measures to protect ePHI. The failure to perform due diligence or audits to confirm that CloudHealth was compliant with security requirements could lead to significant penalties for HealthCo, as it indicates a lack of oversight and responsibility in protecting patient data.

upvoted 3 times

Bhimesh 2 years, 5 months ago

Should be D. Because CloudHealth violated its contract with HealthCo by not encrypting the ePHI What Constitutes a HIPAA Violation? A HIPAA violation is when a HIPAA-covered entity – or a business associate – fails to comply with one or more of the provisions of the HIPAA Privacy, Security, or Breach Notification Rules. A breach applies only to "unsecured" information, and a covered entity can avoid liability if it utilizes encryption Software to secure information

upvoted 2 times

BM9904 2 years, 7 months ago

"if the breach affects 500 or more in the same jurisdiction, it must notify the media. All breaches requiring notice must be reported to HHS at least annually. A breach applies only to "unsecured" information, and a covered entity can avoid liability if it utilizes encryption software to secure information." Section 8.2.1Sorry D here

upvoted 2 times

BM9904 2 years, 7 months ago

Selected Answer: B

“if the breach affects 500 or more in the same jurisdiction, it must notify the media. All breaches requiring notice must be reported to HHS at least annually. A breach applies only to “unsecured” information, and a covered entity can avoid liability if it utilizes encryption software to secure information.” Section 8.2.1

upvoted 2 times

BM9904 2 years, 5 months ago

Sorry D here

upvoted 1 times

Romeokton 2 years, 7 months ago

Might be also C here...

upvoted 1 times

Question #59 *Topic 1*

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

Suggested Answer: *A*

Community vote distribution



Bhimesh Most Recent 1 year, 11 months ago
Should be A. Training on techniques for identifying phishing attempts 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. What is the most effective kind of training CloudHealth could have given its employees to help PREVENT THIS TYPE OF DATA BREACH?
upvoted 1 times

Romeokton 2 years, 1 month ago
Definitely A
upvoted 1 times

Question #60 *Topic 1*

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

Suggested Answer: *D*

Community vote distribution

C (100%)

impchoi Highly Voted 3 years, 3 months ago

C: Administrative covers the phishing training. Technical covers the lack of encryption. Security safeguards are what we're talking about..and administrative and technical are important as mentioned above. The Physical safeguards are not important to how this breach occurred.

upvoted 10 times

Bhimesh 1 year, 11 months ago

Selected Answer: C

HealthCo wasn't in compliance with Administrative and Technical and hence Physical safeguards were not focused on during the investigation.

Safeguards.

The Privacy Rule requires that covered entities implement administrative, physical and technical safeguards to protect the confidentiality and integrity of all PHI.

The HIPAA Security Rule requires both covered entities and business associates to implement administrative, physical, and technical safeguards only for ePHI.

upvoted 1 times

Bhimesh 1 year, 11 months ago

HealthCo wasn't in compliance with Administrative and Technical and hence Physical safeguards were not focused on during the investigation. Safeguards. The Privacy Rule requires that covered entities implement administrative, physical and technical safeguards to protect the confidentiality and integrity of all PHI. The HIPAA Security Rule requires both covered entities and business associates to implement administrative, physical, and technical safeguards only for ePHI.The HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information. Covered entities Criminal penalties for HIPAA violations are directly applicable to covered entities (CE) including: Health plans Health care clearinghouses Health care providers who transmit claims in electronic form Medicare prescription drug card sponsors

upvoted 1 times

Bhimesh Most Recent 1 year, 11 months ago

The HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information. Covered entities Criminal penalties for HIPAA violations are directly applicable to covered entities (CE) including: Health plans Health care clearinghouses Health care providers who transmit claims in electronic form Medicare prescription drug card sponsors

upvoted 1 times

Deatherage 2 years, 7 months ago

A - In the scenario, HealthCo failed to conduct due diligence on CloudHealth, which indicates a lapse in administrative safeguards. B - In the scenario, it's mentioned that the PHI was not encrypted by CloudHealth, which pertains to technical safeguards. C - These are physical measures, policies, and procedures to protect electronic information systems and related buildings and equipment from natural and environmental hazards, and unauthorized intrusion. The scenario doesn't specifically mention any issues related to physical access or environmental threats to the ePHI. D - Security safeguard is not required by the HIPPA Security Rule so this option would be eliminated

upvoted 2 times

smp175 2 years, 8 months ago

The other comments are correct. See the prompt - "Of the safeguards required . . ." That wording rules out D, because it is not one of the safeguards. Rather, it is a red herring answer choice.

upvoted 2 times

Privaceeeeee9876 2 years, 10 months ago

C: Section 8.1.2 of the textbook lists the Security Rule Safeguards as admin, technical and physical. Security safeguards are not considered one of the three categories.

upvoted 2 times

Question #61 *Topic 1*

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

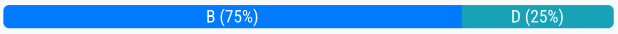
B. Respond with a request for satisfactory assurances such as a qualified protective order

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

Suggested Answer: *C*

Community vote distribution



joats245 Most Recent 2 years ago
From HHS comments: Covered entities may also disclose protected health information in response to a subpoena, discovery request, or other lawful process without a court order, but only if the covered entity receives satisfactory assurances that the party seeking disclosure has made reasonable efforts to ensure that the individual has been notified of the request or that reasonable efforts have been made by the party seeking the information to secure a qualified protective order. Additionally, a covered entity may disclose protected health information in response to a subpoena, discovery request, or other lawful process without a satisfactory assurance if it makes reasonable efforts to provide the individual with such notice or to seek a qualified protected order itself.
upvoted 1 times

7cae8a8 2 years, 2 months ago
No its actually A. Here's why: PHI may not be disclosed, except to the individual patient; as part of treatment, payment, or healthcare operations; as incident to other permitted or required disclosures; or under valid authorization from the individual.
upvoted 1 times

Bhimesh 2 years, 5 months ago

Selected Answer: B

The HIPAA Privacy Rule - the standards for a “qualified protective order” (QPO), which applies in state courts that are not covered by the Federal Rules of Civil Procedure. A QPO 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.

It also requires the return to the covered entity or destruction of the protected health information (including copies) at the end of the litigation.

If a QPO is in place, a covered entity complies with privacy requirements for disclosure in litigation or administrative proceedings

upvoted 1 times

Bhimesh 2 years, 5 months ago

The HIPAA Privacy Rule - the standards for a “qualified protective order” (QPO), which applies in state courts that are not covered by the Federal Rules of Civil Procedure. A QPO 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. It also requires the return to the covered entity or destruction of the protected health information (including copies) at the end of the litigation. If a QPO is in place, a covered entity complies with privacy requirements for disclosure in litigation or administrative proceedingsNot D. Respond with a redacted document only relative to the plaintiff A large amount of personal information may be disclosed to parties in the course of civil litigation. Courts can issue protective orders to prohibit disclosure of personal information revealed in litigation, and “Attorneys increasingly are required to Redact” Social Security numbers and other sensitive information when filing documents with the courts

upvoted 1 times

Bhimesh 2 years, 5 months ago

Not D. Respond with a redacted document only relative to the plaintiff A large amount of personal information may be disclosed to parties in the course of civil litigation. Courts can issue protective orders to prohibit disclosure of personal information revealed in litigation, and “Attorneys increasingly are required to Redact” Social Security numbers and other sensitive information when filing documents with the courts

upvoted 1 times

easyambition1046 2 years, 8 months ago

C is correct because it's asking about the individual's ePHI disclosed in the breach. An individual has a right to their ePHI under HIPAA/HITECH. A request for their records can be appropriately made through their attorney. You don't need a QPO and you can't redact records when you're sending it to the individual or their legal rep.

upvoted 1 times

smp175 3 years, 2 months ago

Best answer is B given the provided study material. D is not necessarily incorrect, but B more fully identifies the appropriate course of action.

upvoted 1 times

Boats 3 years, 4 months ago

By doing C the company would be putting themselves at risk for another data breach. I would go with D.

upvoted 1 times

Question #62 *Topic 1*

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 workplace injuries under OSHA requirements

D. Personal health information under the HIPAA Privacy Rule

Suggested Answer: *D*

Community vote distribution

D (100%)

Bhimesh Most Recent 1 year, 11 months ago

an organization "Generally NOT" be required to disclose to law enforcement... • D. Personal health information under the HIPAA Privacy Rule HIPAA - Disclosures Permitted by Law For some categories of information, an organization is permitted, BUT NOT REQUIRED(GENERALLY), to disclose personal information It permits (BUT DOES NOT REQUIRE) companies to disclose PHI when required to do so by another applicable law, such as the state laws that require reporting of medical information • C. Information about workplace injuries under OSHA requirements The U.S. Department of Labor's (DOL's) Occupational Health and Safety Administration (OSHA) requires compilation and reporting of information about certain workplace injuries and illnesses

upvoted 1 times

Bhimesh 1 year, 11 months ago

A. Information about medication errors under the Food, Drug and Cosmetic Act The U.S. Food and Drug Administration (FDA) requires health professionals and drug manufacturers to report serious adverse events, product problems, or medication errors suspected to be associated with the use of an FDA-regulated drug, biologic, device or dietary supplement under the Food, Drug and Cosmetic Act (FDCA). B. Money laundering information under the Bank Secrecy Act of 1970 Required Disclosure Under Anti-Money- Laundering Laws Financial institutions are also subject to a variety of requirements to retain records and, in some instances, disclose personal financial information to the government. Financial institutions in general have intricate accounting and control systems to document transactions and reduce the risk of fraud.

upvoted 1 times

tfnp 2 years, 4 months ago

It is D. For HIPAA even if there is a law enforcement request, the individual needs to be notified in case they want to appeal.

upvoted 1 times

Deatherage 2 years, 7 months ago

D - Under the HIPAA Privacy Rule, covered entities are not typically required to disclose personal health information (PHI) to law enforcement unless there is a specific reason as defined by the rule (e.g., a court order, warrant, or certain administrative requests). The other choices involve regulatory regimes where disclosures to law enforcement or other governmental authorities are generally expected when specific incidents or issues arise.

upvoted 1 times

Privaceeeeee9876 2 years, 10 months ago

The answer is not D. Textbook mentions "certain law enforcement activates" as a valid exception to the HIPAA privacy rule.

upvoted 1 times

Qwamer 3 years ago

This question should be "none of the above". On page 347, Section 13.1.1, all of the answers are listed as times when disclosures are required by law.

upvoted 3 times

Qwamer 3 years ago

This question should be "none of the above". On page 347, Section 13.1.1, all of the answers are listed as times when disclosures are required by law.D is correct it permits not required in page 347 and it also depends on state laws

upvoted 3 times

testaking917 2 years, 6 months ago

D is correct it permits not required in page 347 and it also depends on state laws

upvoted 1 times

Question #63 *Topic 1*

A law enforcement agency 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

Suggested Answer: *C*

Community vote distribution

C (100%)

Bhimesh Most Recent 1 year, 11 months ago

Selected Answer: C

D.CALEA The U.S. Communications Assistance to Law Enforcement Act of 1994 (CALEA), sometimes referred to as the "Digital Telephony Bill," lays out the duties of defined actors in the telecommunications industry to cooperate in the interception of communications for law enforcement and other needs relating to the security and safety of the public

It notably requires "telecommunications carriers" to design their products and services to ensure that they can carry out a lawful order to provide government access to communications

upvoted 1 times

Bhimesh 1 year, 11 months ago

D.CALEA The U.S. Communications Assistance to Law Enforcement Act of 1994 (CALEA), sometimes referred to as the "Digital Telephony Bill," lays out the duties of defined actors in the telecommunications industry to cooperate in the interception of communications for law enforcement and other needs relating to the security and safety of the public It notably requires "telecommunications carriers" to design their products and services to ensure that they can carry out a lawful order to provide government access to communicationsCALEA applies to telecommunications carriers, but not to other "information services." As enacted, therefore, the law was interpreted not to apply to internet services. In 2004, however, the U.S. Department of Justice (DOJ), the Federal Bureau of Investigation (FBI) and the Drug Enforcement Administration (DEA) petitioned to EXPAND THE INTERPRETATION OF THE SCOPE OF THE LEGISLATION. In 2005, the FCC issued an order that providers of broadband internet access and voiceover-internet protocol (VoIP) services were telecommunications services when they interconnect with traditional telephone services, and so they now operate under CALEA requirements

upvoted 1 times

Bhimesh 1 year, 11 months ago

CALEA applies to telecommunications carriers, but not to other "information services." As enacted, therefore, the law was interpreted not to apply to internet services. In 2004, however, the U.S. Department of Justice (DOJ), the Federal Bureau of Investigation (FBI) and the Drug Enforcement Administration (DEA) petitioned to EXPAND THE INTERPRETATION OF THE SCOPE OF THE LEGISLATION. In 2005, the FCC issued an order that providers of broadband internet access and voiceover-internet protocol (VoIP) services were telecommunications services when they interconnect with traditional telephone services, and so they now operate under CALEA requirements

upvoted 1 times

mojotheamazing 2 years, 4 months ago

In its own words, the purpose of CALEA is: To amend title 18, United States Code, to make clear a telecommunications carrier's duty to cooperate in the interception of communications for Law Enforcement purposes, and for other purposes.

upvoted 1 times

Question #64 *Topic 1*

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

Suggested Answer: *A*

Community vote distribution

A (100%)

Bhimesh Most Recent 1 year, 11 months ago

More generally, court rules today require REDACTION of certain personal information by the litigants themselves. REDACTION is the practice of identifying and removing or blocking information from documents being produced pursuant to a discovery request or as evidence in a court proceeding. The rule applies to both paper and electronic filings and to both parties and non-parties filing documents. Specifically, ATTORNEYS are required to REDACT documents.

upvoted 1 times

Question #65 *Topic 1*

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

Suggested Answer: *C*

Community vote distribution

A (100%)

impchoi Highly Voted 3 years, 3 months ago

The prohibition on interception has a number of exceptions, each of which may have its own nuances requiring an expert to analyze. Under federal law, interception is permitted if a person is the party to the call or if one of the parties has given consent.69

upvoted 6 times

Bhimesh Most Recent 1 year, 11 months ago

There are a few important categories of exceptions to the Electronic Communications Privacy Act of 1986 - Title 1 Wiretap Act: 1) The law provides an exception for communications service providers who unavoidably overhear some oral communications in the normal course of business. 2) Legal eavesdropping by the government is permitted as authorized by appropriate laws, such as the Foreign Intelligence Surveillance Act (FISA), discussed later in this chapter. 3) Law enforcement may also intercept communications with appropriate court orders, such as a warrant. 4) "Communications may be intercepted or recorded with the consent of only one party in the communication".

upvoted 2 times

jjjrbm 2 years, 4 months ago

answer is A

upvoted 1 times

mojotheamazing 2 years, 4 months ago

https://wyattfirm.com/the-electronic-communications-privacy-act-of-1986-tracking-the-productivity-of-work-from-home-employees/ "In other words, monitoring must be relevant to the business, recurring, and the employee must know about it." Here it is personal and there is no indication that the employee knew.

upvoted 1 times

Egofskam 2 years, 10 months ago

It is A - If one of the persons involved in the communication being intercepted has consented to the interception, it is not unlawful (i.e., the one-party consent rule). See 18 U.S.C. § 2511(2)(c)-(d).

upvoted 1 times

Privaceeeeee9876 2 years, 10 months ago

Answer should be A

upvoted 1 times

Supp2023 2 years, 11 months ago

In my opinion, C is the right answer. The question is asking what is an exception to the wiretap act, and interception of employee calls in a workplace is not subject to wiretap act.

upvoted 2 times

Question #66 *Topic 1*

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.

Suggested Answer: *A*

Community vote distribution

C (100%)

Bhimesh Most Recent 1 year, 11 months ago

Authorization for Specific Forms of Surveillance When FISA was first passed, it included rules to authorize the government to conduct electronic surveillance, such as wiretapping. In 1977, Senator Ted Kennedy introduced the Foreign Intelligence Surveillance Act (FISA) to provide a legal framework to manage government spying. FISA limits surveillance to appropriate foreign targets and sets legal processes for due process and oversight.

upvoted 2 times

erwingr 2 years, 3 months ago

See Supp2023

upvoted 1 times

Egofskam 2 years, 10 months ago

The correct answer is C

upvoted 2 times

Supp2023 2 years, 11 months ago

The original purpose of the Foreign Intelligence Surveillance Act (FISA) was to further define a framework for authorizing wiretaps by the executive branch for national security purposes under Article II of the Constitution. Therefore, option C is the correct answer. FISA establishes procedures for the physical and electronic surveillance and collection of foreign intelligence information between foreign powers and agents of foreign powers suspected of espionage or terrorism. It allows the government to obtain surveillance warrants from a special court, the Foreign Intelligence Surveillance Court (FISC), rather than from a regular court.

upvoted 3 times

Question #67 *Topic 1*

What practice does the USA FREEDOM Act NOT authorize?

A. Emergency exceptions that allow 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

D. The bulk collection of telephone data and internet metadata

Suggested Answer: *A*

Community vote distribution

D (100%)

impchoi Highly Voted 3 years, 3 months ago

"he USA FREEDOM Act ended bulk collection conducted under Section 215.154 Going forward, requests by government officials must be based upon specific selectors, such as a telephone number. Company officials are now permitted to release statistics about the number of such requests they receive in a given time period, and the government is required to report its numbers once a year.155 In 2018, government officials obtained 56 court orders for traditional business records and 14 court orders for call detail records.156"

upvoted 11 times

Bhimesh Most Recent 1 year, 11 months ago

Prohibited bulk data collection by requiring the request to list specific search parameters called “selection terms.” Selection terms narrow the request by naming criteria such as specific phone numbers, email addresses, or accounts. The USA FREEDOM Act ended bulk collection conducted under Section 215.

upvoted 1 times

erwingr 2 years, 3 months ago

See Impchoi

upvoted 1 times

jjjrbm 2 years, 4 months ago

Look section 13.3.3.4 Pen Register and Trap-and-Trace Orders

upvoted 1 times

Question #68 *Topic 1*

Why was the Privacy Protection Act of 1980 drafted?

A. To respond to police searches of newspaper facilities

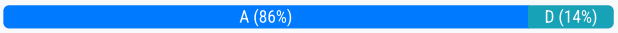
B. To assist prosecutors in civil litigation against newspaper companies

C. To assist in the prosecution of white-collar crimes

D. To protect individuals from personal privacy invasion by the police

Suggested Answer: *D*

Community vote distribution



Bhimesh Most Recent 1 year, 11 months ago

Media Records and the Privacy Protection Act The Privacy Protection Act of 1980 provides an extra layer of protection for members of the media and media organizations from government searches or seizures in the course of a criminal investigation. PPA was passed in the wake of the 1978 Supreme Court case of Zurcher v. Stanford Daily. In that case, police used a search warrant to look through a newspaper's unpublished photographs of a demonstration. Under PPA, government offcials engaging in criminal investigations are NOT permitted to search or seize media work products or documentary materials "reasonably believed to have a purpose to disseminate to the public a newspaper, book, broadcast or other similar form of public communication." In practice, rather than physically searching a newsroom, " The PPA effectively forces law enforcement to use subpoenas or voluntary cooperation to obtain evidence from those engaged in First Amendment activities

upvoted 2 times

Z1682009 2 years, 1 month ago

Page 367- PPA was drafted to respond to police physical searches of traditional newspaper facilities.

upvoted 1 times

Romeokton 2 years, 1 month ago

One more vote for A

upvoted 1 times

AdeyB 2 years, 5 months ago

If you go by the 'US Private Sector Privacy' learning material - then A is the right answer. As has been mentioned refer to Chapter 13, 13.3.7. Page 367

upvoted 3 times

testaking917 2 years, 6 months ago

A is correct. IN IAPP book page 367

upvoted 3 times

Ambulocetus 2 years, 7 months ago

Yes, the PPA protects individuals; however, the PPA was drafted in direct response to the Zurcher decision: In 1978, the U.S. Supreme Court ruled in the case of Zurcher v. Stanford Daily that law enforcement could obtain search warrants to search newsrooms for evidence related to criminal activities. This decision raised concerns that such searches could impede the ability of journalists to do their jobs and gather information without fear of government interference.

upvoted 2 times

smp175 2 years, 8 months ago

D is the right answer. A is worded to intentionally confuse. The PPA applies to any individual collecting information intended for public dissemination. Therefore a journalist's camera at the scene of a protect or rally is protected - the PPA is not so narrow to be initially intended to only apply to newsrooms. A newsroom search was merely the catalyst that led to its adoption.

upvoted 1 times

Boats 2 years, 10 months ago

The Privacy Protection Act of 1980 is legislation passed in the United States that protects journalists and newsrooms from search by government officials. The act protects "work products" and "documentary materials," which have been broadly interpreted.

upvoted 2 times

Supp2023 2 years, 11 months ago

D is the right answer. The Act was drafted to protect individuals and entities from unreasonable searches and seizures by the government in the course of obtaining materials for use in a criminal investigation. It establishes a higher standard for newsroom searches, but it should not be confused with what the question is asking -- WHY was it drafted.

upvoted 2 times

Lisawood 3 years, 1 month ago

The Privacy protection act protects journalists

upvoted 4 times

Question #69 *Topic 1*

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

Suggested Answer: *B*

Community vote distribution

B (100%)

Bhimesh Most Recent 1 year, 11 months ago

Managing e-discovery and privacy begins with a well-managed data retention program… In designing a retention policy, it should be remembered that electronically stored information (ESI) takes not only obvious forms such as email or word processing documents, but can also manifest itself as databases, web pages, server logs, instant messaging transcripts, voicemail systems, social networking records, thumb drives, or even the microSD cards found in smartphones. An important source of standards and best practices for managing electronic discovery compliance through data retention policies is the Sedona Conference

upvoted 1 times

AdeyB 2 years, 5 months ago

Page 346 of the learning material - ".....e-discovery rules, which require automated and large-scale production of emails and other corporate documents during the discovery process prior to trial".

upvoted 1 times

smp175 2 years, 8 months ago

Can anyone explain this further?One of the primary objectives of e-discovery rules is to prevent the loss or destruction of information that may be relevant to a legal matter. These rules impose obligations on organizations to properly retain and manage their electronic data to ensure its availability when needed for litigation or investigations

upvoted 1 times

smp175 2 years, 8 months ago

Can anyone explain this further?

upvoted 1 times

yoyo59 2 years, 8 months ago

One of the primary objectives of e-discovery rules is to prevent the loss or destruction of information that may be relevant to a legal matter. These rules impose obligations on organizations to properly retain and manage their electronic data to ensure its availability when needed for litigation or investigations

upvoted 2 times

Question #70 *Topic 1*

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

Suggested Answer: *A*

Community vote distribution

A (100%)

Bhimesh Most Recent 1 year, 11 months ago

A. They require employers not to discriminate against certain classes when employees use personal information The primary purpose of these laws is to prohibit discrimination in hiring and other employment decisions. A secondary effect, however, is that they often affect how interviews and other background screen activities are conducted. For instance, an employer risks possible discrimination claims for interview questions about national origin or race

upvoted 1 times

Romeokton 2 years, 1 month ago

Think A is right

upvoted 1 times

Question #71 *Topic 1*

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

Suggested Answer: *C*

Community vote distribution

C (100%)

Bhimesh Most Recent 1 year, 11 months ago

TWO EXCEPTIONS to the prohibition on interception often apply in the workplace. Under federal law, interception is permitted: 1. If a person is a party to a call or where one of the parties has given consent 2. The interception is done in the ordinary course of business An employer who provides communication services, such as a company telephone or email service, has the ability to intercept provided the interception occurs in the normal course of the user's business. An important distinction exists when an employer listens to an employee's purely personal call. In this instance, the employer risks violation of the wiretap laws. As courts have split on how broadly to define the "ordinary course of business," many employers rely on the consent exception for interception of telephone calls. Privacy professionals should be alert to the requirements of relevant state laws on recording phone calls, because some of these laws require ONE-PARTY CONSENT, while others mandate that ALL PARTIES TO THE CALL CONSENT.

upvoted 1 times

Question #72 *Topic 1*

SCENARIO -
Please use the following to answer the next question:
Larry has become increasingly dissatisfied with his telemarketing position at SunriseLynx, and particularly with his supervisor, Evan. Just last week, he overheard Evan mocking the state's Do Not Call list, as well as the people on it. "If they were really serious about not being bothered," Evan said, "They'd be on the national DNC list. That's the only one we're required to follow. At SunriseLynx, we call until they ask us not to."
Bizarrely, Evan requires telemarketers to keep records of recipients who ask them to call "another time." This, to Larry, is a clear indication that they don't want to be called at all. Evan doesn't see it that way.
Larry believes that Evan's arrogance also affects the way he treats employees. The U.S. Constitution protects American workers, and Larry believes that the rights of those at SunriseLynx are violated regularly. At first Evan seemed friendly, even connecting with employees on social media. However, following Evan's political posts, it became clear to Larry that employees with similar affiliations were the only ones offered promotions.
Further, Larry occasionally has packages containing personal-use items mailed to work. Several times, these have come to him already opened, even though this name was clearly marked. Larry thinks the opening of personal mail is common at SunriseLynx, and that Fourth Amendment rights are being trampled under Evan's leadership.
Larry has also been dismayed to overhear discussions about his coworker, Sadie. Telemarketing calls are regularly recorded for quality assurance, and although Sadie is always professional during business, her personal conversations sometimes contain sexual comments. This too is something Larry has heard Evan laughing about. When he mentioned this to a coworker, his concern was met with a shrug. It was the coworker's belief that employees agreed to be monitored when they signed on. Although personal devices are left alone, phone calls, emails and browsing histories are all subject to surveillance. In fact, Larry knows of one case in which an employee was fired after an undercover investigation by an outside firm turned up evidence of misconduct. Although the employee may have stolen from the company, Evan could have simply contacted the authorities when he first suspected something amiss.
Larry wants to take action, but is uncertain how to proceed.
In what area does Larry have a misconception about private-sector employee rights?

A. The applicability of federal law

B. The enforceability of local law

C. The strict nature of state law

D. The definition of tort law

Suggested Answer: *A*

Community vote distribution

A (100%)

Bhimesh Most Recent 1 year, 11 months ago
When it comes to postal mail, organizations are legally allowed to open and read any mail addressed to the organization once delivered, even if a specific employee's name is on the parcel.
upvoted 1 times

Bhimesh 1 year, 11 months ago
Workplace Privacy U.S. Regulatory Bodies that Protect Employee Privacy - Employee privacy is protected by several federal agencies, including the U.S. Department of Labor (DOL), the Equal Employment Opportunity Commission (EEOC), the Federal Trade Commission (FTC), the Consumer Financial Protection Bureau (CFPB), and the National Labor Relations Board (NLRB
upvoted 1 times

Question #73 *Topic 1*

SCENARIO -
Please use the following to answer the next question:
Larry has become increasingly dissatisfied with his telemarketing position at SunriseLynx, and particularly with his supervisor, Evan. Just last week, he overheard Evan mocking the state's Do Not Call list, as well as the people on it. "If they were really serious about not being bothered," Evan said, "They'd be on the national DNC list. That's the only one we're required to follow. At SunriseLynx, we call until they ask us not to."
Bizarrely, Evan requires telemarketers to keep records of recipients who ask them to call "another time." This, to Larry, is a clear indication that they don't want to be called at all. Evan doesn't see it that way.
Larry believes that Evan's arrogance also affects the way he treats employees. The U.S. Constitution protects American workers, and Larry believes that the rights of those at SunriseLynx are violated regularly. At first Evan seemed friendly, even connecting with employees on social media. However, following Evan's political posts, it became clear to Larry that employees with similar affiliations were the only ones offered promotions.
Further, Larry occasionally has packages containing personal-use items mailed to work. Several times, these have come to him already opened, even though this name was clearly marked. Larry thinks the opening of personal mail is common at SunriseLynx, and that Fourth Amendment rights are being trampled under Evan's leadership.
Larry has also been dismayed to overhear discussions about his coworker, Sadie. Telemarketing calls are regularly recorded for quality assurance, and although Sadie is always professional during business, her personal conversations sometimes contain sexual comments. This too is something Larry has heard Evan laughing about. When he mentioned this to a coworker, his concern was met with a shrug. It was the coworker's belief that employees agreed to be monitored when they signed on. Although personal devices are left alone, phone calls, emails and browsing histories are all subject to surveillance. In fact, Larry knows of one case in which an employee was fired after an undercover investigation by an outside firm turned up evidence of misconduct. Although the employee may have stolen from the company, Evan could have simply contacted the authorities when he first suspected something amiss.
Larry wants to take action, but is uncertain how to proceed.
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

Suggested Answer: *B*

Community vote distribution

B (100%)

Bhimesh Most Recent 1 year, 11 months ago

The Equal Employment Opportunity Commission (EEOC) The EEOC works to prevent discrimination in the workplace - Both the FTC and the CFPB regulate unfair and deceptive practices and enforce a variety of laws Using social media to monitor current employees Though employers are generally legally permitted to use social media in informing their decisions, they must not violate existing antidiscrimination and privacy laws Invasive monitoring practices may provide the basis for discrimination lawsuits if the employer accesses and appears to use information that is legally protected. This includes protected classes such as religion, ethnicity, gender or sexual orientation, "political affiliations", and other sensitive information, all of which is commonly available on individuals' social media pages. Although reading publicly available information is clearly lawful, acting in a discriminatory way in the workplace is not.

upvoted 1 times

Question #74 *Topic 1*

SCENARIO -
Please use the following to answer the next question:
Larry has become increasingly dissatisfied with his telemarketing position at SunriseLynx, and particularly with his supervisor, Evan. Just last week, he overheard Evan mocking the state's Do Not Call list, as well as the people on it. "If they were really serious about not being bothered," Evan said, "They'd be on the national DNC list. That's the only one we're required to follow. At SunriseLynx, we call until they ask us not to."
Bizarrely, Evan requires telemarketers to keep records of recipients who ask them to call "another time." This, to Larry, is a clear indication that they don't want to be called at all. Evan doesn't see it that way.
Larry believes that Evan's arrogance also affects the way he treats employees. The U.S. Constitution protects American workers, and Larry believes that the rights of those at SunriseLynx are violated regularly. At first Evan seemed friendly, even connecting with employees on social media. However, following Evan's political posts, it became clear to Larry that employees with similar affiliations were the only ones offered promotions.
Further, Larry occasionally has packages containing personal-use items mailed to work. Several times, these have come to him already opened, even though this name was clearly marked. Larry thinks the opening of personal mail is common at SunriseLynx, and that Fourth Amendment rights are being trampled under Evan's leadership.
Larry has also been dismayed to overhear discussions about his coworker, Sadie. Telemarketing calls are regularly recorded for quality assurance, and although Sadie is always professional during business, her personal conversations sometimes contain sexual comments. This too is something Larry has heard Evan laughing about. When he mentioned this to a coworker, his concern was met with a shrug. It was the coworker's belief that employees agreed to be monitored when they signed on. Although personal devices are left alone, phone calls, emails and browsing histories are all subject to surveillance. In fact, Larry knows of one case in which an employee was fired after an undercover investigation by an outside firm turned up evidence of misconduct. Although the employee may have stolen from the company, Evan could have simply contacted the authorities when he first suspected something amiss.
Larry wants to take action, but is uncertain how to proceed.
Which act would authorize Evan's undercover investigation?

A. The Whistleblower Protection Act

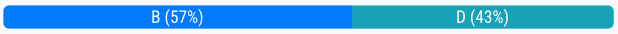
B. The Stored Communications Act (SCA)

C. The National Labor Relations Act (NLRA)

D. The Fair and Accurate Credit Transactions Act (FACTA)

Suggested Answer: *C*

Community vote distribution



impchoi Highly Voted 3 years, 9 months ago
Stored communications. As previously discussed, the SCA creates a general prohibition against the unauthorized acquisition, alteration or blocking of electronic communications while in electronic storage in a facility through which an electronic communications service is provided.119 Violations for interceptions can lead to criminal penalties or a civil lawsuit. The law provides for exceptions. Two exceptions that may apply to the employer are for conduct authorized: "By the person or entity providing a wire or electronic communications service" (often the employer)120 "By a user of that service with respect to a communication of or intended for that user"121
upvoted 6 times

aprivate1 Most Recent 2 years ago
This one got muddy. The correct answer is D - FACTA. Specifically, the Vail Letter prompted FACTA to amend the FCRA where if certain conditions are met, an employer does not need to notify an employee it is obtaining a consumer report. (See pg 398-399 of the 4th ed book)
upvoted 2 times

Bhimesh 2 years, 5 months ago

Selected Answer: B

Email and Telephone Monitoring

As with video and photographic monitoring, companies have similar reasons to monitor employee communications by phone and email. The ECPA's business purpose exception applies here as well, but that exception applies only to work-related communications. This means that employers have to stop surveillance if a conversation seems to be personal. Some employers deal with this through policies banning personal communications using company phones or email.

The “SCA” plays a role here as well.

Emails stored on a server are not considered communications by the ECPA and thus not subject to the Wiretap Act. As long as companies notify employees that they do not have an expectation of privacy for information stored on company servers, the “SCA” permits employers to review information it stores.

The ECPA and the related “Stored Communications Act (SCA)” permit the monitoring as long as certain requirements are met

upvoted 1 times

Bhimesh 2 years, 5 months ago

Email and Telephone Monitoring As with video and photographic monitoring, companies have similar reasons to monitor employee communications by phone and email. The ECPA's business purpose exception applies here as well, but that exception applies only to work-related communications. This means that employers have to stop surveillance if a conversation seems to be personal. Some employers deal with this through policies banning personal communications using company phones or email. The “SCA” plays a role here as well. Emails stored on a server are not considered communications by the ECPA and thus not subject to the Wiretap Act. As long as companies notify employees that they do not have an expectation of privacy for information stored on company servers, the “SCA” permits employers to review information it stores. The ECPA and the related “Stored Communications Act (SCA)” permit the monitoring as long as certain requirements are metBy contrast, the employer listening to an employee’s purely personal call would risk running afoul of the wiretap laws. Courts have split on how broadly to define “ordinary course of business,” which is a reason that many employers rely instead on the “consent exception” for interception of telephone calls. Note that the federal law is not pre-emptive, so if an organization is monitoring or recording calls, it runs the risk of violating the stricter law in the “all-party consent” states mentioned above- it should not rely on any of these exceptions outside the specific state.Under federal law, “interception is permitted” if a person is the party to the call or if one of the parties has given consent. A number of states, however, have the stricter rule that all of the parties to the call must consent. This all-party consent requirement is why customers often hear a message giving notice that a call is being recorded for quality assurance or other purposes A second exception relevant to many companies concerns interception done in the “ordi

upvoted 1 times

Bhimesh 2 years, 5 months ago

By contrast, the employer listening to an employee’s purely personal call would risk running afoul of the wiretap laws. Courts have split on how broadly to define “ordinary course of business,” which is a reason that many employers rely instead on the “consent exception” for interception of telephone calls. Note that the federal law is not pre-emptive, so if an organization is monitoring or recording calls, it runs the risk of violating the stricter law in the “all-party consent” states mentioned above- it should not rely on any of these exceptions outside the specific state.

upvoted 1 times

Bhimesh 2 years, 5 months ago

Under federal law, “interception is permitted” if a person is the party to the call or if one of the parties has given consent. A number of states, however, have the stricter rule that all of the parties to the call must consent. This all-party consent requirement is why customers often hear a message giving notice that a call is being recorded for quality assurance or other purposes A second exception relevant to many companies concerns interception done in the “ordinary course of business”. This exception can apply where the device used for the interception is “furnished to the subscriber or user by a provider of wire or electronic communication service in the ordinary course of its business.” To qualify for the exception, the interception itself must also be in the normal “course of the user’s business”. Normal course of business here would apply to routine monitoring in a call centre.

upvoted 1 times

Priv24 2 years, 5 months ago

Look at the book 12.2.2.5. The answer is D.

upvoted 1 times

Romeokton 2 years, 7 months ago

The investigation is not described to be related to communication. It is a suspected theft. The official book says: Under FACTA, employers are not required to notify an employee that an outside organization is conducting an investigation. So, for me here is D and impchoi is wrong.

upvoted 1 times

Ambulocetus 3 years, 1 month ago

FACTA doesn't apply. The FCRA does not apply to investigations conducted by the in-house personnel. In addition, FCRA does not apply when a third-party, who is not in the business of providing such reports, does the investigation .

upvoted 1 times

smp175 3 years, 2 months ago

Answer is B for reasons impchoi stated. Not sure if the comments pointing to D without support are trolling or not... Nothing implicates FACTA...

upvoted 1 times

Shaza123 3 years, 6 months ago

The correct answer is D .

upvoted 2 times

Shaza123 3 years, 6 months ago

The correct answer is D - FACTA.

upvoted 2 times

Question #75 *Topic 1*

SCENARIO -
Please use the following to answer the next question:
Larry has become increasingly dissatisfied with his telemarketing position at SunriseLynx, and particularly with his supervisor, Evan. Just last week, he overheard Evan mocking the state's Do Not Call list, as well as the people on it. "If they were really serious about not being bothered," Evan said, "They'd be on the national DNC list. That's the only one we're required to follow. At SunriseLynx, we call until they ask us not to."
Bizarrely, Evan requires telemarketers to keep records of recipients who ask them to call "another time." This, to Larry, is a clear indication that they don't want to be called at all. Evan doesn't see it that way.
Larry believes that Evan's arrogance also affects the way he treats employees. The U.S. Constitution protects American workers, and Larry believes that the rights of those at SunriseLynx are violated regularly. At first Evan seemed friendly, even connecting with employees on social media. However, following Evan's political posts, it became clear to Larry that employees with similar affiliations were the only ones offered promotions.
Further, Larry occasionally has packages containing personal-use items mailed to work. Several times, these have come to him already opened, even though this name was clearly marked. Larry thinks the opening of personal mail is common at SunriseLynx, and that Fourth Amendment rights are being trampled under Evan's leadership.
Larry has also been dismayed to overhear discussions about his coworker, Sadie. Telemarketing calls are regularly recorded for quality assurance, and although Sadie is always professional during business, her personal conversations sometimes contain sexual comments. This too is something Larry has heard Evan laughing about. When he mentioned this to a coworker, his concern was met with a shrug. It was the coworker's belief that employees agreed to be monitored when they signed on. Although personal devices are left alone, phone calls, emails and browsing histories are all subject to surveillance. In fact, Larry knows of one case in which an employee was fired after an undercover investigation by an outside firm turned up evidence of misconduct. Although the employee may have stolen from the company, Evan could have simply contacted the authorities when he first suspected something amiss.
Larry wants to take action, but is uncertain how to proceed.
In regard to telemarketing practices, Evan the supervisor has a misconception regarding?

A. The conditions under which recipients can opt out

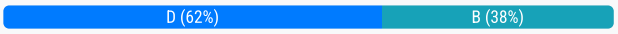
B. The wishes of recipients who request callbacks

C. The right to monitor calls for quality assurance

D. The relationship of state law to federal law

Suggested Answer: *B*

Community vote distribution



Bhimesh Most Recent 1 year, 11 months ago
State Telemarketing Laws As neither the TSR nor the FCC rules "pre-empt state laws", the majority of states have enacted telemarketing laws creating additional legal requirements for telemarketers. For example, more than half the states require that telemarketers obtain a license or register with the state. States can also create their own DNC lists, with differing exceptions, fines or methods of consumer enrolment from their federal counterpart. Some states require that telemarketers identify themselves at the beginning of the call or that the telemarketer terminate the call without rebuttal if the recipient of the call so desires.
upvoted 3 times

ca57687 1 year, 11 months ago
Federal law sets the floor for rights and state law can provide additional rights to citizens. Evan is mislead saying ""If they were really serious about not being bothered, they'd be on the national DNC list. That's the only one we're required to follow."
upvoted 2 times

testaking917 2 years, 6 months ago
D is correct they have to follow state list too
upvoted 1 times

smp175 2 years, 8 months ago

From the scenario: “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.” The national DNC list does not supersede state DNC lists in states that maintain such lists (i.e., the TSR does not preempt state statutes in this regard). Therefore, the answer is D. Evan has a misconception about federal vs state law with respect to DNC lists.

upvoted 3 times

Question #76 *Topic 1*

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

Suggested Answer: *A*

Community vote distribution

A (100%)

Bhimesh Most Recent 1 year, 11 months ago

In the United States, private-sector employees in general have “limited” expectations of privacy at the workplace. The physical facilities belong to the employer, and employers in the private sector thus generally have ‘BROAD LEGAL AUTHORITY’ to do monitoring and searches at work These employer rights are frequently ‘MORE LIMITED’ in Europe and other countries, where ‘employees often have a broader set of protections against monitoring under data protection, collective bargaining, and other employment laws’. Companies with employees both in the United States and abroad thus may need to develop different policies and IT systems that conform to the varying laws

upvoted 1 times

Question #77 *Topic 1*

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)

Suggested Answer: *A*

Community vote distribution

A (100%)

Bhimesh 1 year, 11 months ago

A contract Law can alter the rules between employer and employee. An individual employee, for instance, might negotiate a contract that says that certain private activities are outside the scope of the employment relationship. Turning to tort law, at least three common-law torts can be relevant to employee privacy. First is the tort of "intrusion upon seclusion," which states: "One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy A second tort claim can be "publicity given to private life," which states: "One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, A third tort claim is for defamation, which focuses on a false or defamatory statement. The common law supplies some possible protections for employees.Constitutional Law The U.S. Constitution has significant workplace privacy provisions that apply to the federal and state governments, but they do not affect private-sector employment. Notably, the Fourth Amendment prohibits unreasonable searches and seizures by state actors. Courts have interpreted this amendment to place limits on the ability of government employers to search employees' private spaces, such as lockers and desks. In general for private-sector actors, however, there is no state action, and "no constitutional law governs employment privacy"

upvoted 1 times

Bhimesh 1 year, 11 months ago

Selected Answer: A

A contract Law can alter the rules between employer and employee. An individual employee, for instance, might negotiate a contract that says that certain private activities are outside the scope of the employment relationship.

Turning to tort law, at least three common-law torts can be relevant to employee privacy.

First is the tort of "intrusion upon seclusion," which states: "One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy

A second tort claim can be "publicity given to private life," which states: "One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy,

A third tort claim is for defamation, which focuses on a false or defamatory statement.

The common law supplies some possible protections for employees.

upvoted 1 times

Bhimesh Most Recent 1 year, 11 months ago

Constitutional Law The U.S. Constitution has significant workplace privacy provisions that apply to the federal and state governments, but they do not affect private-sector employment. Notably, the Fourth Amendment prohibits unreasonable searches and seizures by state actors. Courts have interpreted this amendment to place limits on the ability of government employers to search employees' private spaces, such as lockers and desks. In general for private-sector actors, however, there is no state action, and "no constitutional law governs employment privacy"

upvoted 1 times

Question #78 *Topic 1*

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

Suggested Answer: *B*

Community vote distribution

D (100%)

impchoi Highly Voted 3 years, 3 months ago

The U.S. Constitution has significant workplace privacy provisions that apply to the federal and state governments, but they do not affect private-sector employment. Notably, the Fourth Amendment prohibits unreasonable searches and seizures by state actors. Courts have interpreted this amendment to place limits on the ability of government employers to search employees' private spaces, such as lockers and desks.4 Some states, including California, have extended their constitutional rights to privacy to private-sector employees.5 In general for private-sector actors, however, there is no state action, and no constitutional law governs employment privacy

upvoted 5 times

Bhimesh Most Recent 1 year, 11 months ago

Constitutional Law The U.S. Constitution has significant workplace privacy provisions that apply to the federal and state governments, but they do not affect private-sector employment. Notably, the Fourth Amendment prohibits unreasonable searches and seizures by state actors. Courts have interpreted this amendment to place limits on the ability of government employers to search employees' private spaces, such as lockers and desks. In general for private-sector actors, however, there is no state action, and "no constitutional law governs employment privacy"

upvoted 1 times

jjjrbm 2 years, 4 months ago

answer is D

upvoted 2 times

smp175 2 years, 8 months ago

The constitution is a relatively short document. To the extent there is physical security precedent that predates this technological age, it comes largely from 4th amendment case law. The best answer is D - albeit it could be worded better. It provides protections to *employees* of federal and state governments.

upvoted 3 times

Question #79 *Topic 1*

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

Suggested Answer: *A*

Community vote distribution

A (100%)

Bhimesh Most Recent 1 year, 11 months ago

The ECPA represents the primary legislation regulating the ability of the federal government to eavesdrop on U.S. citizens' communications. Title I of the ECPA, known as the Wiretap Act, prohibits spying on real-time communications without consent. Exceptions to the Wiretap Act: Law enforcement may also intercept communications with appropriate court orders, such as a warrant. • Legal eavesdropping by the government is permitted as authorized by appropriate laws, such as the Foreign Intelligence Surveillance Act (FISA), discussed later in this chapter. • Law enforcement may also intercept communications with appropriate court orders, such as a warrant. • Communications may be intercepted or recorded with the consent of only one party in the communication.

upvoted 1 times

Romeokton 2 years, 1 month ago

I support the indicated answer (crosschecked with the book).

upvoted 1 times

Question #80 *Topic 1*

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

A. Questions about age

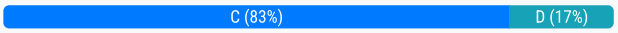
B. Questions about a disability

C. Questions about national origin

D. Questions about intended pregnancy

Suggested Answer: *C*

Community vote distribution



447bcdc Most Recent 1 year, 9 months ago

D. Questions about intended pregnancy. Title VII of the Civil Rights Act of 1964 prohibits employment discrimination based on race, color, religion, sex, or national origin. While questions about age, disability, and national origin can be sensitive and potentially discriminatory, they are not explicitly prohibited by Title VII.

upvoted 1 times

Bhimesh 2 years, 5 months ago

Title VII of the Civil Rights Act protects job seekers from discrimination based on… Race, Color, Religion, National origin, Religion, or Sex. And Look at this (options, should be changed) The act, as subsequently amended, further prohibits discrimination based on pregnancy or childbirth status. The Civil Rights Act was also later aligned with the Age Discrimination in Employment Act (ADEA), which protects anyone over 40 from discrimination based on age.

upvoted 4 times

Romeokton 2 years, 7 months ago

The Civil Rights Act of 1964 (Title VII) bars discrimination in employment due to race, color, religion, sex and national origin

upvoted 1 times

Question #81 *Topic 1*

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

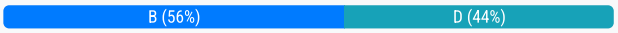
B. It increased the obligation of organizations to dispose of consumer data in ways that prevent unauthorized access

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

Suggested Answer: *B*

Community vote distribution



mab487 Most Recent 1 year, 8 months ago

The Fair and Accurate Credit Transactions Act (FACTA) of 2003 amended the Fair Credit Reporting Act (FCRA) to enhance consumer protections and reduce identity theft risks. One of its key provisions was the Disposal Rule, which mandates organizations to dispose of consumer data securely to prevent unauthorized access or misuse. Other FACTA provisions include free annual credit reports and protections against identity theft.

upvoted 1 times

fightingpotato 1 year, 11 months ago

The Fair and Accurate Credit Transactions Act (FACTA), which was passed in 2003, is an amendment to the Fair Credit Reporting Act (FCRA). One of its key provisions is the requirement for businesses and organizations to take appropriate measures to safely dispose of consumer information derived from consumer reports, such as credit reports, to prevent unauthorized access to the data. This provision is part of the efforts to reduce the risk of identity theft and other types of fraud involving personal information.

upvoted 1 times

joats245 2 years ago

B. Facta disposal rule D is way to narrow "internal investigations", and if right, is less right

upvoted 3 times

Bhimesh 2 years, 5 months ago

Consumer reports may always be shared with written permission from a consumer. Without consumer consent, reports may only be shared for limited other “permissible purposes,” In 2003, the Fair and Accurate Credit Transactions Act (FACTA) amended. FCRA the amendments pre-empted a wide range of state laws on credit reporting, identity theft and other areas within the FCRA FACTA, however, specifically left some existing state laws in effect, notably the California Investigative Consumer Reporting Agencies Act (ICRAA). Under the ICRAA, employers must notify applicants and employees of their intention to obtain and use a consumer report. Once disclosure is made, the employer must obtain the applicant or employee’s written authorization prior to requesting the report.

upvoted 2 times

BM9904 2 years, 6 months ago

“n 2003, the Fair and Accurate Credit Transactions Act (FACTA) amended FCRA. The amendments preempted a wide range of state laws on credit reporting, identity theft and other areas within the FCRA.61 FACTA, however, specifically left some existing state laws in effect, notably the California Investigative Consumer Reporting Agencies Act (ICRAA).62 Under the ICRAA, employers must notify applicants and employees of their intention to obtain and use a consumer report. Once disclosure is made, the employer must obtain the applicant or employee’s written authorization prior to requesting the report” Excerpt From: “IAPP_US_Private_Sector_Privacy_3E.” Apple Books.

upvoted 2 times

Question #82 *Topic 1*

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

A. The CAN-SPAM Act

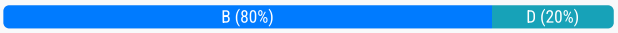
B. The Children's Online Privacy Protection Act (COPPA)

C. The Fair and Accurate Credit Transactions Act (FACTA)

D. The Telemarketing Consumer Protection and Fraud Prevention Act

Suggested Answer: *D*

Community vote distribution



BrianVelasquez Most Recent 3 months, 1 week ago

B. The Children's Online Privacy Protection Act (COPPA): Under 15 U.S.C. § 6502(d), COPPA's preemption clause only applies to state laws that are inconsistent with its regulations. The Federal Trade Commission (FTC) and federal courts have affirmed that COPPA does not preempt or block states from enacting or enforcing stricter laws protecting children's online privacy

upvoted 1 times

mab487 1 year, 8 months ago

COPPA does not preempt stricter state laws, meaning states can implement more stringent regulations regarding children's online privacy. By contrast, the CAN-SPAM Act, FACTA, and the Telemarketing Consumer Protection and Fraud Prevention Act include provisions that preempt stricter state laws in specific areas to ensure uniform national standards.

upvoted 1 times

d654514 1 year, 9 months ago

COPPA has preemption only for inconsistent state laws

upvoted 2 times

Bhimesh 1 year, 11 months ago

As neither the TSR nor the FCC rules pre-empt state laws, the majority of states have enacted telemarketing laws -creating additional legal requirements for telemarketers. For example, more than half the states require that telemarketers obtain a license or register with the state. States can also create their own DNC lists, with differing exceptions, fines or methods of consumer enrolment from their Federal counterpart. Some states require that telemarketers identify themselves at the beginning of the call or that the telemarketer terminate the call without rebuttal if the recipient of the call so desires. Finally, states may require that a written contract be created for certain transactions

upvoted 1 times

Question #83 *Topic 1*

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

Suggested Answer: *A*

Community vote distribution

A (100%)

Bhimesh Most Recent 1 year, 11 months ago

Connecticut describes the covered entities subject to its notification law as “any person who conducts business in this state, and who, in the ordinary course of such person’s business, owns, licenses or maintains computerized data that includes personal information.” Some states limit the definition of “covered entities” to those that “conduct business in that state.” Note, however, that some state laws are narrower, such as the Georgia law applying only to “information brokers.”

upvoted 1 times

Question #84 *Topic 1*

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

Suggested Answer: *B*

Community vote distribution

C (100%)

Shaza123 Highly Voted 3 years ago

C is more accurate than B

upvoted 6 times

Bhimesh Most Recent 1 year, 11 months ago

State Breach Notification Laws In the absence of a federal law, states have taken the lead in setting requirements related to data breaches

upvoted 1 times

Romeokton 2 years, 1 month ago

As AdeyB quotes, but it is not 7.2 - it is 7.6

upvoted 2 times

jjjrbm 2 years, 4 months ago

I agree with AdeyB and Shaza123. C should be the correct answer

upvoted 2 times

AdeyB 2 years, 5 months ago

I'd agree with Shaza123. Refer to the learning material Section 7.2 - "In the absence of a Federal Law, states have taken the lead in setting requirements related to data breaches"

upvoted 4 times

Question #85 *Topic 1*

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

Suggested Answer: *A*

Community vote distribution

B (100%)

Abae Highly Voted 3 years, 7 months ago

I think the answer is B.

upvoted 6 times

KCCM Most Recent 2 years, 1 month ago

Correct answer B

upvoted 1 times

Bhimesh 2 years, 5 months ago

The CAN-SPAM Act provides a good example of federal preemption because it does not allow states to enforce any stricter statutes. For example, the CAN-SPAM Act prevents states from passing laws requiring recipients to opt in to receive commercial messages.

upvoted 1 times

Romeokton 2 years, 7 months ago

CAN-SPAM preempts state law and states are not allowed to pass stricter laws

upvoted 1 times

AdeyB 2 years, 11 months ago

Word of warning that the latest version of the learning material (Page 283) states "CAN-SPAM preempts most state laws....." i.e. Not all state laws

upvoted 1 times

Egofskam 3 years, 4 months ago

B - HIPAA does not preempt more stringent state laws, whereas CAN-SPAM preempts state law with the narrow exception for those that prohibit falsity or deception

upvoted 3 times

Privaceeeeee9876 3 years, 4 months ago

States can enact stricter PHI privacy laws but cannot lessen the federal HIPAA requirements

upvoted 1 times

Shaza123 3 years, 6 months ago

B is the correct answer.

upvoted 3 times

Question #86 *Topic 1*

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

Suggested Answer: *D*

Community vote distribution

C (100%)

Abae Highly Voted 3 years, 7 months ago

The answer is C." For example, more than half the states require that telemarketers obtain a license or register with the state.39" Excerpt From: "IAPP_US_TB_US-Private-Sector-Privacy-3E_1.0." Apple Books. "states may require that a written contract be created for certain transaction". Excerpt From: "IAPP_US_TB_US-Private-Sector-Privacy-3E_1.0." Apple Books.

upvoted 7 times

7cae8a8 Most Recent 2 years, 2 months ago

I agree with C.

upvoted 1 times

Bhimesh 2 years, 5 months ago

State Telemarketing Laws As neither the TSR nor the FCC rules pre-empt state laws, the majority of states have enacted telemarketing laws -creating additional legal requirements for telemarketers. For example, "more than half the states require that telemarketers obtain a license or register with the state."

upvoted 1 times

Romeokton 2 years, 7 months ago

Abae nailed it - this is exactly what answers.

upvoted 1 times

AdeyB 2 years, 11 months ago

Answer is C. Learning Material Section 11.1.3.

upvoted 1 times

Shaza123 3 years, 6 months ago

the correct answer is C.

upvoted 3 times

Question #87 *Topic 1*

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.

Suggested Answer: *D*

Community vote distribution

D (100%)

7cae8a8 Most Recent 2 years, 2 months ago

D is correct.

upvoted 1 times

Bhimesh 2 years, 5 months ago

In 2010, Massachusetts adopted a more prescriptive encryption rule. The Massachusetts Personal Information Protection Regulation states that all parties that "own or license" personal information pertaining to Massachusetts residents must "encrypt all personal information stored on laptops or other portable devices," as well as wireless transmissions and transmissions sent over public networks.

upvoted 1 times

Romeokton 2 years, 7 months ago

I also go with D, but this is a tricky one as nothing too specific is mentioned in the training materials.

upvoted 1 times

AdeyB 2 years, 11 months ago

D is correct. Page 176 of the learning material

upvoted 1 times

Question #88 *Topic 1*

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

Suggested Answer: *A*

Community vote distribution

A (100%)

Bhimesh Most Recent 1 year, 11 months ago

What is required or prohibited? This law requires all persons to disclose any breach of system security to any "Resident of California" whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person Why does this law exist? SB 1386 was enacted because security breaches of computerized databases are feared to cause identity theft and individuals should be notified about these breaches so they can take steps to protect themselves. Anyone with a security breach that puts people at real risk of identity the should consider notifying them even if they are not subject to this law.

upvoted 1 times

Romeokton 2 years, 1 month ago

SB 1386 went into affect on July 1, 2003. Under the law, covered parties must disclose any breach of the security of personal data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

upvoted 1 times

Question #89 *Topic 1*

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

Suggested Answer: *B*

Community vote distribution

B (100%)

Bhimesh Most Recent 1 year, 11 months ago

All states with data breach notification laws use similar language to describe the required timing of notifications to affected parties. The most common phrase used in conjunction with timing is "the most expedient time possible and without unreasonable delay." Numerous states specify a limit to the time allowed when this common phrase is utilized, with 45 days after the discovery of the breach being the most common timeframe permitted by these states. For companies operating nationally, it is important to note that the industry best practice is to report within 30 days after the discovery of the breach, meaning that a delay of 45 days could be considered unreasonable (without a valid explanation) in certain states. For example - Colorado and Florida provide for a 30-day time frame. New Mexico, Ohio, Oregon, Rhode Island, Tennessee, Vermont, Washington and Wisconsin mandate a 45-day time frame. Louisiana stipulates a 60-day requirement. "States that Require Notification within a Specific Time Frame,"

upvoted 1 times

Romeokton 2 years, 1 month ago

Florida as erwingr says.

upvoted 1 times

erwingr 2 years, 3 months ago

State specifics • Laws recognize the need for the affected entity to conduct a "reasonable investigation in order to determine the scope of the breach and to restore the reasonable integrity of the data system" • Laws specify an expeditious time limit of 45 days (FL, NM, OH, RI, TN, VT, WA, WI)

upvoted 2 times

jjjrbm 2 years, 4 months ago

answer is D

upvoted 1 times

Question #90 *Topic 1*

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

A. State identification number

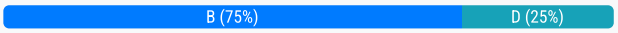
B. First and last name

C. Social Security number

D. Medical information

Suggested Answer: *D*

Community vote distribution



gghadid 1 year, 1 month ago

Selected Answer: B

only the name itself would not be PI; and only few states like California,Delaware stipulate that medical information is PI with names

upvoted 2 times

BrianVelasquez **Most Recent** 3 months ago

Under standard U.S. state data breach notification laws, a first and last name (or first initial and last name) on its own is NOT classified as personal information or "trigger information" that requires notification if breached. Instead, state statutes define "personal information" as an individual's name in combination with one or more highly sensitive data elements

upvoted 1 times

gghadid 1 year, 1 month ago

only the name itself would not be PI; and only few states like California,Delaware stipulate that medical information is PI with namessorry for the wrong answer and explanation, it should be D

upvoted 2 times

Bhimesh 1 year, 11 months ago

Selected Answer: D

Definition of Personal Information

An example of the typical definition of personal information is Connecticut's, which defines it as "an individual's First name or first initial and last name in combination with anyone, or more, of the following data:

(1) Social Security number; (2) driver's license number; (3) state identification card number; or (4) account number or 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

upvoted 1 times

gghadid 1 year, 1 month ago

sorry for the wrong answer and explanation, it should be D

upvoted 1 times

Bhimesh 1 year, 11 months ago

Definition of Personal Information An example of the typical definition of personal information is Connecticut's, which defines it as "an individual's First name or first initial and last name in combination with anyone, or more, of the following data: (1) Social Security number; (2) driver's license number; (3) state identification card number; or (4) account number or 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 accountThis data is part of the definition of personal information in all state data breach elements. For example, Alabama, Arkansas, California, Colorado, Delaware, Florida, Illinois, Maryland, Missouri, Montana, Nevada, North Dakota, Oregon, Rhode Island, South Dakota, Texas, Virginia, and Wyoming "INCLUDE MEDICAL AND HEALTHCARE INFORMATION." The laws in Alaska, Georgia, Maine, North Carolina, and Vermont apply to "passwords, personal identification numbers, account numbers, or other similar information related to financial accounts. " Alabama, Colorado, Delaware, Maryland, Montana, New Mexico, New York, North Carolina, Oregon, South Carolina, South Dakota, and Wyoming "include any federal or state identification number, which serves as a catchall for passport numbers, military identification, and other tax identification numbers.Several states, including Colorado, Delaware, Illinois, Iowa, Maryland, Nebraska, New Mexico, North Carolina, Oregon, Wisconsin, and Wyoming apply to "unique biometric data ("i.e., such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data") or biometric data (consisting of digital measurements of an individual's fingerprints, voice print, retina or iris image, facial characteristics, or hand geometry)." Delaware and Wisconsin specifically "list a DNA profile. " Puerto Rico includes "tax information and work-related evaluations." North Carolina and No

upvoted 1 times

Bhimesh 1 year, 11 months ago

This data is part of the definition of personal information in all state data breach elements.

For example, Alabama, Arkansas, California, Colorado, Delaware, Florida, Illinois, Maryland, Missouri, Montana, Nevada, North Dakota, Oregon, Rhode Island, South Dakota, Texas, Virginia, and Wyoming "INCLUDE MEDICAL AND HEALTHCARE INFORMATION."

The laws in Alaska, Georgia, Maine, North Carolina, and Vermont apply to "passwords, personal identification numbers, account numbers, or other similar information related to financial accounts. "

Alabama, Colorado, Delaware, Maryland, Montana, New Mexico, New York, North Carolina, Oregon, South Carolina, South Dakota, and Wyoming "include any federal or state identification number, which serves as a catchall for passport numbers, military identification, and other tax identification numbers.

upvoted 1 times

Bhimesh 1 year, 11 months ago

This data is part of the definition of personal information in all state data breach elements. For example, Alabama, Arkansas, California, Colorado, Delaware, Florida, Illinois, Maryland, Missouri, Montana, Nevada, North Dakota, Oregon, Rhode Island, South Dakota, Texas, Virginia, and Wyoming "INCLUDE MEDICAL AND HEALTHCARE INFORMATION." The laws in Alaska, Georgia, Maine, North Carolina, and Vermont apply to "passwords, personal identification numbers, account numbers, or other similar information related to financial accounts. " Alabama, Colorado, Delaware, Maryland, Montana, New Mexico, New York, North Carolina, Oregon, South Carolina, South Dakota, and Wyoming "include any federal or state identification number, which serves as a catchall for passport numbers, military identification, and other tax identification numbers.Several states, including Colorado, Delaware, Illinois, Iowa, Maryland, Nebraska, New Mexico, North Carolina, Oregon, Wisconsin, and Wyoming apply to "unique biometric data ("i.e., such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data") or biometric data (consisting of digital measurements of an individual's fingerprints, voice print, retina or iris image, facial characteristics, or hand geometry)." Delaware and Wisconsin specifically "list a DNA profile. " Puerto Rico includes "tax information and work-related evaluations." North Carolina and North Dakota add "mother's maiden name (often used as a security question)."

upvoted 1 times

Bhimesh 1 year, 11 months ago

Several states, including Colorado, Delaware, Illinois, Iowa, Maryland, Nebraska, New Mexico, North Carolina, Oregon, Wisconsin, and Wyoming apply to "unique biometric data ("i.e., such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data") or biometric data (consisting of digital measurements of an individual's fingerprints, voice print, retina or iris image, facial characteristics, or hand geometry)." Delaware and Wisconsin specifically "list a DNA profile. " Puerto Rico includes "tax information and work-related evaluations." North Carolina and North Dakota add "mother's maiden name (often used as a security question)."

upvoted 1 times

Question #91 *Topic 1*

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.

Suggested Answer: *D*

Community vote distribution

D (100%)

Bhimesh Most Recent 1 year, 11 months ago

Option D. The right of individuals harmed by a violation of a law to file a lawsuit against the violation. A private right of action means that individuals and corporations may bring cases to court for violations of a specific law. If a law does not contain a private right of action, it is up to state and federal authorities to prosecute violations of a law. For example, FERPA does not contain a private right of action, so students who suffer data breaches may not sue institutions under FERPA. The U.S. Department of Education(DOL) can bring enforcement actions in such a case. HIPAA and the Gramm–Leach–Bliley Act (GLBA) contain privacy provisions but do not include a “private right of action.” The California Consumer Privacy Act (CCPA), which protects the private information of California residents, DOES CONTAIN a “private right of action.” Under CCPA, an individual can sue an organization they believe has violated their right to privacy

upvoted 1 times

Question #92 *Topic 1*

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.

Suggested Answer: *D*

Community vote distribution

D (100%)

7cae8a8 Most Recent 2 years, 2 months ago

D is correct. The nine principles in the APEC Privacy Framework are preventing harm, notice, collection limitations, uses of personal information, choice, integrity of personal information, security safeguards, access and correction, accountability.

upvoted 1 times

Bhimesh 2 years, 5 months ago

D. Privacy by Design. APEC information privacy principles 1. Preventing Harm 2. Notice 3. Collection Limitations 4. Uses of Personal Information 5. Choice 6. Integrity of Personal Information 7. Security Safeguards 8. Access and Correction 9. Accountability

upvoted 1 times

Question #93 *Topic 1*

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.

Suggested Answer: *B*

Community vote distribution

B (100%)

Bhimesh Most Recent 1 year, 11 months ago

If a privacy policy is revised, the organization should announce the change first to employees, then to both current and former customers through its privacy notice. Both in a 2012 report and in a 2015 update, the FTC stated that companies should obtain “express affirmative consent (opt-in) before making “material” retroactive changes to privacy representations.” The FTC stated that a material change “at a minimum includes sharing consumer information with third parties after committing at the time of collection not to share the data If the policy is not strict enough, then consumers, regulators, and the press may criticize the company for its failure to protect privacy. If a policy is too strict, then open-ended statements or overly ambitious security promises can result in legal penalties or reputational problems if the organization cannot satisfy its promises.

upvoted 1 times

Romeokton 2 years, 1 month ago

The FTC wants businesses to obtain affirmative consent from their customers when they make material adverse retroactive changes to their privacy policies.

upvoted 2 times

Question #94 *Topic 1*

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 offline (e.g., in person), which also satisfies any requirements for online consent.

Suggested Answer: *B*

Community vote distribution

B (100%)

Bhimesh 1 year, 11 months ago

Selected Answer: B

In 1998, the United States enacted the Children's Online Privacy Protection Act (COPPA) to provide special privacy protections for children under the age of 13.

Under COPPA, businesses operating websites used by children have additional requirements to control data collection on children.

This include requirements for privacy notices, "affirmative parental consent," and more.

These protections not only enhance privacy—and therefore safety—for children, but also allow parents to distinguish legitimate child-oriented online services from bad actors.

It also requires "consent by parents" prior to collection of personal information for children "under the age of 13"

The Delaware law defines a minor as a state resident under the age of 18. In 2020, CCPA became effective. This California law prohibits the selling of personal information of California consumers under the age of 16 without "affirmative consent from these individuals."

upvoted 1 times

Bhimesh 1 year, 11 months ago

In 1998, the United States enacted the Children's Online Privacy Protection Act (COPPA) to provide special privacy protections for children under the age of 13. Under COPPA, businesses operating websites used by children have additional requirements to control data collection on children. This include requirements for privacy notices, "affirmative parental consent," and more. These protections not only enhance privacy—and therefore safety—for children, but also allow parents to distinguish legitimate child-oriented online services from bad actors. It also requires "consent by parents" prior to collection of personal information for children "under the age of 13" The Delaware law defines a minor as a state resident under the age of 18. In 2020, CCPA became effective. This California law prohibits the selling of personal information of California consumers under the age of 16 without "affirmative consent from these individuals."COPPA Scope COPPA is intended to regulate operators of online services that collect data about children under the age of 13. Online services include websites, mobile apps, smart devices, and so on. We refer to these collectively as "online services" COPPA applies to online operators that specifically design online services for children under 13 years old and those who know that children under 13 use their services online. For the purposes of this section, a child is a person under the age of 13. Specifically, COPPA applies to the following: Online services intended for children that gather, use, and share children's data General online services where the operator knows they are gathering, using, and sharing children's data Online services that knowingly collect children's personal information from another online service or website targeted at children

upvoted 1 times

Bhimesh Most Recent 1 year, 11 months ago

COPPA Scope COPPA is intended to regulate operators of online services that collect data about children under the age of 13. Online services include websites, mobile apps, smart devices, and so on. We refer to these collectively as “online services” COPPA applies to online operators that specifically design online services for children under 13 years old and those who know that children under 13 use their services online. For the purposes of this section, a child is a person under the age of 13. Specifically, COPPA applies to the following: Online services intended for children that gather, use, and share children's data General online services where the operator knows they are gathering, using, and sharing children's data Online services that knowingly collect children's personal information from another online service or website targeted at children

upvoted 1 times