

Table of Contents

About the Editors	v
About the Contributors	vii
Table of Chapters	xiii
Table of Contents	xv
Foreword	liii
Preface	lv
Acknowledgments	lvii
Table of Abbreviations	lix

Chapter 1 Overview of U.S. Information Privacy Law

The Basics	1-4
<i>Definitions</i>	1-4
Q 1.1 What is information privacy law?	1-4
Q 1.1.1 What types of information do information privacy laws protect?	1-4
Q 1.2 How does information privacy law define “personally identifiable information”?	1-4
Q 1.3 What is “sensitive information”?	1-5
Q 1.4 What is “non-personal information”?	1-6
Q 1.5 What is a “persistent identifier”?	1-6
<i>General Principles for Privacy Policies and Practices</i>	1-7
Q 1.6 When should a company design its information privacy policies and practices?	1-7
Q 1.7 What are the general principles that a company must keep in mind when designing its information privacy policies and practices?	1-7
<i>Notice</i>	1-9
Q 1.8 How should a company provide notice to users of its information privacy practices?	1-9

PRIVACY LAW ANSWER BOOK 2020

<i>Consumer Choice and Consent</i>	1-10
Q 1.9 What does “consumer choice and consent” mean?.....	1-10
Q 1.9.1 When must a company provide users with a choice concerning the use of their PII?.....	1-10
Q 1.9.2 What is consumer consent to a company’s information practices required?.....	1-11
<i>Access and Review</i>	1-11
Q 1.10 What access to their PII must a company provide to consumers?	1-11
<i>Data Security</i>	1-12
Q 1.11 What should a company do to keep customer data secure?.....	1-12
<i>Enforcement</i>	1-12
Q 1.12 What types of actions constitute violations of information privacy laws?	1-12
Q 1.12.1 Which agencies take enforcement action against privacy violations?.....	1-13
Privacy by Design	1-13
Q 1.13 What is privacy by design?	1-13
Q 1.13.1 What are the basic principles of privacy by design?.....	1-14
Q 1.13.2 How should a company implement privacy by design?	1-14
Legislative and Regulatory Framework	1-15
<i>Federal Regulation</i>	1-15
Q 1.14 What laws does the United States have concerning information privacy?.....	1-15
Q 1.14.1 What are “general applicability” laws?.....	1-15
Q 1.15 What is the FTC?.....	1-16
Q 1.15.1 What authority does the FTC have to regulate privacy or bring privacy enforcement cases?	1-16
Q 1.16 What are “unfair” acts or practices?.....	1-17
Q 1.17 What are “deceptive” acts or practices?.....	1-17
<i>State Regulation</i>	1-18
Q 1.18 What state laws apply to information privacy issues?.....	1-18
Q 1.19 Are changes to state data privacy laws likely in the near future?	1-20

Table of Contents

<i>Industry-Specific Regulation</i>	1-20
Q 1.20 What types of industry-specific laws apply to information privacy issues?	1-20
<i>Technology-Specific Regulation</i>	1-20
Q 1.21 Are there any information privacy laws that apply specifically to audiovisual products?	1-20
Q 1.22 Are there any information privacy laws or guidelines that apply specifically to mobile devices and applications?	1-21
<i>Non-U.S. Regulation</i>	1-22
Q 1.23 Do other countries have laws about information privacy with which U.S.-based companies must comply?	1-22
Guidance and Best Practices	1-23
<i>Privacy Certifications</i>	1-23
Q 1.24 What are privacy certifications, and are they necessary?	1-23
<i>Industry Guidelines and Codes of Conduct</i>	1-24
Q 1.25 In addition to federal and state law, what guidance on information privacy should companies review and consider?	1-24
Q 1.25.1 What best practices are included in the FTC report <i>Protecting Consumer Privacy in an Era of Rapid Change</i> ?.....	1-25
<i>Social Media</i>	1-26
Q 1.26 What privacy concerns are raised for a company that integrates social media into its business plans?	1-26
Future Outlook	1-27
Q 1.27 What does the future hold for information privacy laws?	1-27

Chapter 2 Privacy Policies

Overview: Legislative and Regulatory Framework; Best Practices	2-3
<i>Statutory Requirements</i>	2-3
Q 2.1 Is a privacy policy required by law?	2-3

<i>Posting Requirements</i>	2-4
Q 2.2 Where should a company post its online privacy policy?	2-4
<i>Policy Scope and Content</i>	2-5
Q 2.3 If a company operates several websites, can it use the same privacy policy for all of them?	2-5
Q 2.4 Is there an “off-the-shelf” privacy policy that a company can use as its own privacy policy?.....	2-5
<i>Privacy Policy for Mobile Apps</i>	2-6
Q 2.5 Does a company need a separate privacy policy for its mobile applications?	2-6
<i>Multilayered Policy</i>	2-7
Q 2.6 What is a multilayered policy?	2-7
Privacy Policy Provisions	2-8
<i>Terms and Disclosures</i>	2-8
Q 2.7 What terms should a company include in its privacy policy?	2-8
Q 2.7.1 What other disclosures should a company include in its privacy policy?	2-10
Q 2.7.2 For a company subject to the EU’s GDPR requirements, what additional information should be included in its privacy policy?	2-11
<i>Anticipating Future Information Practices</i>	2-13
Q 2.8 Can a company’s privacy policy cover future uses of personal information even though it currently does not use information in those ways?	2-13
Preparing the Privacy Policy	2-14
<i>Developing an Initial Draft</i>	2-14
Q 2.9 How should a company begin to draft its privacy policy?.....	2-14
Q 2.9.1 Who should participate in the preparation of the privacy policy?	2-14
<i>Format, Style, Language</i>	2-15
Q 2.10 How should a privacy policy be formatted?	2-15

Table of Contents

<i>Revising/Updating the Privacy Policy: Notification and Consent Requirements</i>	2-15
Q 2.11 What are the most important considerations for a company when changing or updating its privacy policy?.....	2-15
Q 2.11.1 How should a company notify users of policy changes and (if necessary) obtain consent?.....	2-15
Q 2.11.2 Are companies subject to any legal requirements regarding updating privacy policies?	2-17
Obtaining Users’ Affirmative Consent	2-18
<i>Generally</i>	2-18
Q 2.12 Can a company assume users have consented to its information practices by disclosing them in its privacy policy?.....	2-18
<i>Sharing User Information with Vendors/Affiliates</i>	2-18
Q 2.13 Does a company need to obtain users’ affirmative consent before sharing their personal information with affiliates or vendors?.....	2-18
<i>Sharing User Information for Advertising/Marketing Purposes</i>	2-19
Q 2.14 Is a user’s affirmative consent required to share personal information with third parties for advertising or marketing purposes?.....	2-19
<i>Sharing User Information for Litigation Purposes</i>	2-20
Q 2.15 Is user consent required to produce personal information in connection with litigation or in response to a request or subpoena from the government?.....	2-20
<i>Material Changes to the Privacy Policy</i>	2-21
Q 2.16 Is affirmative consent from users required each time a company changes or updates its privacy policy?.....	2-21
Q 2.16.1 What is a “material change” to a privacy policy?	2-21
Q 2.17 What should a company do if a customer does not consent to the new privacy policy?	2-22
<i>Sharing User Information in the Event of Merger/Sale</i>	2-22
Q 2.18 Is users’ affirmative consent required to transfer personal information to a third party in the event of a merger, sale, or similar transaction?.....	2-22

Enforcement of a Privacy Policy.....2-23

Unfair and Deceptive Acts and Practices.....2-23

Q 2.19 Is a privacy policy enforceable?2-23

Government Agency Enforcement Actions.....2-24

 Q 2.19.1 What are common types of enforcement actions brought against companies regarding their privacy policies?2-24

Private Actions; Class Actions.....2-26

 Q 2.19.2 What are common types of private actions brought against companies connected to their privacy policies?.....2-26

Chapter 3 Children’s Privacy

Overview: COPPA and the COPPA Rule3-3

Q 3.1 Is there a particular law or regulation that governs children’s privacy in the United States?3-3

Definitions3-3

Q 3.2 What is COPPA?3-3

“Website or Online Service Directed to Children”3-4

Q 3.3 Who is subject to COPPA?3-4

Q 3.4 What is an “online service” under COPPA?3-5

Q 3.5 What factors make a website or online service “directed to children”?3-5

 Q 3.5.1 Can a website or online service that is designed for or is frequented by multiple audiences, including children under thirteen, be considered “directed to children”?3-7

 Q 3.5.2 What is a “general-audience” website or online service?3-7

 Q 3.5.3 Can one part of a website be “directed to children” under COPPA while another part of the same website is not?3-7

 Q 3.5.4 Is the use of students’ personal information, as opposed to children’s information, restricted by COPPA?3-8

Table of Contents

<i>Collection and Disclosure of Personal Information</i>	3-9
Q 3.6 What constitutes “personal information” under COPPA?	3-9
Q 3.7 What constitutes “collection” of personal information under COPPA?	3-10
Q 3.7.1 Does COPPA regulate the collection of personal information <i>about</i> children, or only the collection of personal information <i>from</i> children?	3-11
Q 3.8 What constitutes “disclosure” of personal information under COPPA?	3-12
<i>Obligations for Covered Operators</i>	3-12
Q 3.9 What obligations does COPPA impose on operators of sites that collect personal information from children?	3-12
Operators Not Ordinarily Subject to COPPA	3-13
Q 3.10 When is an operator of a general-audience website or online service subject to COPPA, and what are the operator’s obligations in those circumstances?	3-13
Q 3.10.1 When is a website operator deemed to have “actual knowledge” that it has collected personal information from children younger than thirteen years old?	3-13
Q 3.11 Is the operator of a general-audience website or online service subject to COPPA if it collects personal information from the users of a third party’s child-directed website or online service?	3-15
Q 3.12 Does COPPA apply to websites or online services operated by nonprofit organizations?	3-16
Q 3.13 Does COPPA apply to foreign-based (non-U.S.) websites or online services?	3-16
Special Considerations for Child-Directed Websites and Online Services	3-16
<i>Conduct of Third Parties</i>	3-16
Q 3.14 Can an operator of a website or online service that is directed to children be held liable for third parties’ collection of personal information on the operator’s website or online service?	3-16
Q 3.14.1 Is an operator of a website or online service that is directed to children required to notify third parties that the site or service is directed to children?	3-17

<i>Online Advertising Considerations</i>	3-18
Q 3.15 How can online advertising trigger COPPA obligations?.....	3-18
Q 3.15.1 Are there uses of persistent identifiers that are acceptable under COPPA?.....	3-18
<i>File Uploading/Sharing</i>	3-19
Q 3.16 Does permitting children to upload files to or share personal information on a child-directed website or online service trigger COPPA obligations?.....	3-19
Age-Screening	3-19
Q 3.17 How might an operator of a website or online service age-screen its users?.....	3-19
Q 3.18 Can an operator of a child-directed website or online service age-screen users younger than thirteen years old?.....	3-19
Q 3.18.1 Does COPPA permit an operator of a general-audience website to block all users who are younger than thirteen years old?.....	3-20
Q 3.19 Does an operator of a general-audience website or online service have any obligations under COPPA when children lie about their ages during an age-screening process?.....	3-20
Privacy Policies and Direct Notices	3-21
<i>Generally</i>	3-21
Q 3.20 What information must a website or online service that is directed to children include in its privacy policy?.....	3-21
Q 3.21 Does COPPA require operators to create a separate privacy policy on the collection of information from children?.....	3-21
<i>Privacy Policy Posting Requirements</i>	3-22
Q 3.22 Where and in what manner should a website that is directed to children post links to its privacy policy?.....	3-22
Q 3.23 Where should a child-directed mobile application provide its privacy policy?.....	3-22
<i>Direct Notice Requirements</i>	3-23
Q 3.24 What is “direct notice” under COPPA, and when is it required?.....	3-23
Q 3.24.1 What constitutes a “material change” in information practices?.....	3-23
Q 3.25 What must be included in a direct notice?.....	3-24

Table of Contents

Q 3.26	What methods should be used to deliver direct notice to parents?.....	3-27
Verifiable Parental Consent		3-27
<i>General Requirement</i>		3-27
Q 3.27	When must an operator obtain verifiable parental consent?.....	3-27
<i>Methods for Verifiable Parental Consent</i>		3-28
Q 3.28	What are the methods for obtaining verifiable parental consent?.....	3-28
Q 3.28.1	What is the “email-plus” method for obtaining verifiable parental consent?.....	3-29
Q 3.28.2	Can an operator use consent methods for obtaining verifiable personal consent outside those recommended by the COPPA Rule?	3-29
Q 3.28.3	Can an operator of a child-directed website or online service use a third party to obtain verifiable parental consent on the operator’s behalf?.....	3-30
<i>No Verifiable Parental Consent Obtained</i>		3-31
Q 3.29	What actions must an operator of a child-directed website or online service take if a parent does not respond to a direct notice or give verifiable consent?.....	3-31
Q 3.30	Can an operator of a child-directed website or online service bar access to its website or service if the operator does not receive verifiable parental consent?	3-31
Q 3.31	Can an operator of a child-directed website or online service rely upon a school to provide consent to its collection of personal information from students or use or disclosure of such information?	3-32
Exceptions to Prior Parental Consent		3-32
Q 3.32	Are there circumstances in which prior parental consent is not required?.....	3-32
<i>“One-Time Contact” Exception</i>		3-35
Q 3.33	Under what circumstances might an operator of a child-directed website or online service use the “one-time contact” exception?.....	3-35
Q 3.33.1	How does the “one-time contact” exception work in practice?.....	3-35

<i>“Multiple-Contact” Exception</i>	3-36
Q 3.34 Under what circumstances might an operator of a child-directed website or online service use the “multiple-contact” exception?	3-36
Q 3.34.1 How does the “multiple-contact” exception work in practice?	3-36
<i>“Support for Internal Operations” Exception</i>	3-37
Q 3.35 What constitutes “support for the internal operations of the Web site or online service”?.....	3-37
Q 3.35.1 How does the “support for internal operations” exception to the verifiable parental consent requirement work in practice?	3-37
Q 3.35.2 Can any activities other than those expressly listed in the definition of “support for the internal operations of the Web site or online service” be considered activities performed in support for internal operations under the exception?	3-38
Q 3.35.3 Does the “support for internal operations” exception permit a website operator or a third party to perform site analytics?	3-38
Q 3.35.4 Does the “support for internal operations” exception allow personalized advertisements to be run on child-directed websites?	3-39
Parental Right of Review	3-39
Q 3.36 What rights do parents have to access information collected online from their children?	3-39
Security Obligations	3-40
Q 3.37 What security measures must an operator of a website or online service take to protect children’s personal information?.....	3-40
Safe Harbor Programs	3-41
Q 3.38 What is the COPPA safe harbor program?	3-41
Q 3.39 What is the safe harbor process?.....	3-42
Q 3.39.1 What are the benefits and costs of participation in an FTC-approved COPPA safe harbor program?.....	3-42
Q 3.39.2 Has the FTC approved any COPPA safe harbor programs?.....	3-43

Table of Contents

Enforcement	3-43
<i>Generally</i>	3-43
Q 3.40 Who enforces COPPA?	3-43
Q 3.41 Is there a private right of action under COPPA?.....	3-44
<i>Violations/Penalties</i>	3-44
Q 3.42 What are the penalties for violation of the COPPA Rule?.....	3-44
<i>FTC Enforcement Actions</i>	3-45
Q 3.43 What kinds of enforcement actions does the FTC take under COPPA?	3-45
<i>State Enforcement</i>	3-46
Q 3.44 Do the states enforce COPPA?	3-46
Q 3.45 Do any states have additional requirements related to children’s data privacy?	3-46

Chapter 4 Financial Privacy

Overview	4-2
Q 4.1 What are the principal laws and regulations governing privacy in the financial industry?.....	4-2
The Gramm-Leach-Bliley Act	4-3
<i>The Basics</i>	4-3
Q 4.2 What role does the GLBA play in protecting consumer financial privacy?	4-3
Q 4.3 What does the GLBA Privacy Rule provide?	4-4
Q 4.4 Have agencies issued any official guidance on compliance with the GLBA Privacy Rule on which companies can rely?	4-4
<i>Individuals and Information Protected by the GLBA</i>	4-4
Q 4.5 Whom does the GLBA protect?	4-4
Q 4.5.1 Who is a “consumer” for GLBA purposes?.....	4-5
Q 4.5.2 Who is a “customer” for GLBA purposes?	4-5
Q 4.5.3 Who is a “former customer” for GLBA purposes?	4-5

PRIVACY LAW ANSWER BOOK 2020

Q 4.6	What constitutes “nonpublic personal information” under the GLBA Privacy Rule?	4-6
Q 4.6.1	What are examples of information that is NPI and information that is not NPI?	4-6
Q 4.6.2	Is all personally identifiable financial information covered?	4-6
<i>Companies Subject to the GLBA</i>		4-7
Q 4.7	Which companies must comply with the GLBA Privacy Rule?	4-7
Q 4.8	What is a “financial institution”?	4-7
Q 4.8.1	What are “financial activities”?	4-7
Q 4.8.2	What are some examples of businesses that are considered “financial institutions”?	4-8
Q 4.8.3	What are some examples of businesses that are <i>not</i> considered “financial institutions”?	4-9
Q 4.8.4	Can web-based companies be financial institutions under the GLBA?	4-9
Q 4.8.5	Are law firms financial institutions?	4-10
Q 4.9	Are any financial institutions exempt from compliance with the GLBA Privacy Rule?	4-10
Q 4.10	If a company is not a financial institution, does it have to be concerned with the GLBA Privacy Rule?	4-10
<i>Privacy Policies and Notices</i>		4-10
Q 4.11	What types of notices are financial institutions required to provide?	4-10
Q 4.11.1	Is there an official model privacy notice?	4-11
Q 4.11.2	What information must financial institutions include in their privacy notices?	4-12
Q 4.11.3	Does a company need to provide annual notice to former customers?	4-12
Q 4.11.4	Does a company need to provide consumers with a privacy notice and an opportunity to opt out if it is sharing NPI only with affiliated companies?	4-12
Q 4.11.5	Can a company and its affiliates jointly provide a single privacy notice?	4-13
Q 4.11.6	Does a company need to provide a different privacy notice for each type of relationship it has with customers?	4-13
Q 4.12	How should a financial institution provide its privacy notice?	4-13
Q 4.12.1	Where on a company’s website should privacy and opt-out notices be posted?	4-14

Table of Contents

Q 4.12.2	Must a privacy notice meet any formatting requirements?	4-14
Q 4.13	If a company's privacy notice is lengthy, does it need to send the entire policy to customers or consumers?	4-14
Q 4.13.1	What is a short-form privacy notice?	4-15
Q 4.13.2	What is a simplified privacy notice?	4-15
Q 4.14	When must a privacy notice be delivered?	4-15
Q 4.14.1	Are there any exceptions to the requirement to mail customers an annual privacy notice?	4-16
<i>Opt-Out Notices</i>		4-16
Q 4.15	What must a company's privacy notice say regarding a customer or consumer's right to opt out of disclosure of NPI?	4-16
Q 4.15.1	What is a reasonable amount of time to give consumers and customers to opt out?	4-17
Q 4.15.2	What opt-out methods should a company provide to its consumers?	4-17
Q 4.16	When can a covered individual opt out?	4-18
Q 4.16.1	For how long is an opt-out valid?	4-18
Q 4.17	Is there any information that a company may never disclose, even if a consumer does not opt out?	4-18
<i>Statutory Exceptions to Notice Requirements</i>		4-18
Q 4.18	Are there exceptions to a financial institution's obligations to provide privacy and opt-out notices?	4-18
Q 4.18.1	What are the obligations of a company if it only discloses NPI pursuant to a section 13, section 14, or section 15 exception?	4-19
Q 4.18.2	What are the obligations of a company if it only discloses NPI pursuant to a section 14 or section 15 exception?	4-19
Q 4.19	What kinds of agents or service providers are covered by the section 13 exception?	4-19
Q 4.19.1	Does a company need to do anything in particular to qualify for a section 13 exception?	4-19
Q 4.20	What does it mean for a company to disclose information in order to "effect, administer, or enforce a transaction" under section 14?	4-20
Q 4.21	What does the section 15 exception cover?	4-20

<i>Reuse and Redisclosure</i>	4-21
Q 4.22 Are there limitations on what nonaffiliated third-party recipients may do with NPI that a financial institution provides?	4-21
Q 4.22.1 What restrictions exist on the redisclosure of NPI received pursuant to a section 14 or section 15 exception?	4-22
Q 4.22.2 Are there any other rules under the GLBA that companies should be aware of?	4-22
<i>Enforcement of the GLBA</i>	4-23
Q 4.23 Which agencies have enforcement responsibilities for the GLBA Privacy Rule?	4-23
Q 4.24 Is there a private right of action to sue for failure to comply with the GLBA?	4-24
The Fair Credit Reporting Act	4-25
<i>The Basics</i>	4-25
Q 4.25 What is the Fair Credit Reporting Act?	4-25
Q 4.25.1 What is a “consumer” under the FCRA?	4-25
Q 4.26 What is a “credit reporting agency”?	4-25
Q 4.27 What is a “consumer report”?	4-26
Q 4.27.1 Is a consumer report limited to nonpublic information?	4-27
Q 4.27.2 What is an “investigative consumer report”?	4-27
Q 4.28 What is considered personally identifiable information for purposes of the FCRA?	4-28
Q 4.29 How does the FCRA limit the use of consumer report information?	4-28
<i>Duties of Users of Consumer Report Information</i>	4-29
Q 4.30 Under the FCRA, does a user of consumer report information owe any duty to the CRA that provides the report?	4-29
Q 4.30.1 Does a company have a responsibility to notify a consumer about how it uses his consumer report?	4-30
Q 4.30.2 Do users of consumer reports have an obligation to protect the consumer’s information?	4-30
Q 4.31 May a user of consumer reports also provide consumer report information to a third party without becoming a CRA?	4-31
Q 4.31.1 May a user of consumer reports share consumer report information with its affiliates?	4-31

Table of Contents

Q 4.31.2	How can “other information” be shared among affiliated companies?	4-31
Q 4.32	Do companies that use consumer reports for employment purposes have additional duties?	4-32
Q 4.32.1	What other state or federal laws should a company looking to use background check information for employment purposes be aware of?	4-33
Q 4.33	Do employers taking adverse action based on non-consumer report information have to notify the employee?	4-34
Q 4.34	Are investigative consumer reports treated differently?	4-35
Q 4.35	Do furnishers of consumer report information to CRAs have additional obligations under the FCRA?	4-35
	<i>Prescreened Offers of Credit or Insurance</i>	4-37
Q 4.36	What is a prescreened offer?	4-37
Q 4.36.1	Does the FCRA permit the use of consumer report information to make a prescreened offer?	4-37
Q 4.36.2	What is a firm offer of credit?	4-38
Q 4.36.3	Can a company combine a firm offer of credit with an offer for products and services?	4-38
Q 4.37	What disclosures are users of prescreening services required to make?.....	4-39
Q 4.37.1	What requirements regarding format and content must prescreen opt-out notices meet?	4-40
Q 4.37.2	Are there special considerations for electronic prescreened notices?	4-41
	<i>The Affiliate Marketing Rule</i>	4-42
Q 4.38	What is the Affiliate Marketing Rule?	4-42
Q 4.38.1	What is “eligibility information”?	4-42
Q 4.38.2	What does it mean to “make a solicitation”?	4-43
Q 4.39	Is Internet marketing considered a solicitation under the Affiliate Marketing Rule?.....	4-44
Q 4.39.1	Can a company market to consumers based on information accessed from a database shared among affiliates?.....	4-44
Q 4.39.2	What is constructive sharing?	4-44
Q 4.40	What form of notice is required by the Affiliate Marketing Rule?	4-45
Q 4.40.1	Can companies consolidate affiliate marketing notices with notices required by other laws or regulations?.....	4-46
Q 4.40.2	Which affiliate must provide notice?	4-47
Q 4.40.3	What content is required in the notice?.....	4-48

Q 4.40.4	For which affiliates is a consumer’s opt-out effective?	4-48
Q 4.40.5	Can an opt-out notice be provided in electronic form, and if so, how?	4-49
Q 4.41	Are there exceptions to the Affiliate Marketing Rule?	4-50
Q 4.41.1	When do a company and a consumer have a pre-existing relationship?	4-50
Q 4.41.2	Does a consumer’s response to a free promotional offer create a pre-existing business relationship?	4-51
Q 4.41.3	Can servicing rights create a pre-existing relationship with a consumer?	4-51
<i>The Identity Theft Red Flag Rules</i>		4-52
Q 4.42	What are the Identity Theft Red Flag Rules?	4-52
Q 4.42.1	What companies are covered by the Red Flag Rules?	4-52
Q 4.43	What elements are required in an Identity Theft Prevention Program?	4-53
Q 4.43.1	How should a company’s Identity Theft Prevention Program identify relevant red flags?	4-54
Q 4.43.2	How should a company’s Identity Theft Prevention Program comply with its obligation to detect red flags?	4-54
Q 4.43.3	How should a company’s Identity Theft Prevention Program respond to detected red flags?	4-55
Q 4.43.4	What are a company’s obligations with respect to updating its Identity Theft Prevention Program?	4-55
Q 4.43.5	What are a company’s obligations with respect to oversight and administration of its Identity Theft Prevention Program?	4-55
<i>Enforcement of the FCRA</i>		4-56
Q 4.44	Which agencies enforce the FCRA?	4-56
Q 4.44.1	How do the CFPB and FTC enforce a violation of the FCRA?	4-56
Q 4.44.2	Can the CFPB or FTC assess a penalty or fine against a company for a violation of the FCRA?	4-57
Q 4.44.3	Can state authorities also enforce the FCRA?	4-57
Q 4.45	Is there a private right of action for failure to comply with the FCRA?	4-57
State Financial Privacy Regulation		4-58
Q 4.46	Are there any state laws that protect personal financial information?	4-58

Table of Contents

Q 4.47	Aren't state financial privacy laws preempted by the federal laws?	4-59
Q 4.48	Do any states impose greater privacy duties on financial institutions than those provided for by federal law?	4-61
Q 4.48.1	What is the California Financial Information Privacy Act (FIPA)?.....	4-62
Q 4.48.2	What is New York's regulation entitled "Cybersecurity Requirements for Financial Services Companies"?	4-63
Q 4.49	What are some important considerations regarding state regulation of privacy for companies that do business in multiple states?.....	4-64
Payment Card Transactions		4-65
<i>Overview</i>		4-65
Q 4.50	Are there specific financial privacy issues related to payment card transactions?	4-65
Q 4.51	Who is involved in a payment card transaction?	4-65
Q 4.51.1	Who are card associations?	4-66
Q 4.51.2	Who is an issuer bank?	4-66
Q 4.51.3	Who is an acquirer bank?	4-66
Q 4.51.4	Who is a payment processor?	4-66
<i>Processing Payment Card Transactions: Authorization; Clearing and Settlement</i>		4-66
Q 4.52	How is a payment card transaction processed?.....	4-66
Q 4.52.1	How does the payment card authorization process work?.....	4-67
Q 4.52.2	How does the payment card clearing and settlement process work?.....	4-68
Q 4.52.3	How are the issuer and acquirer paid?.....	4-68
<i>Industry Standards</i>		4-69
Q 4.53	What responsibilities do parties involved in payment card transactions have?	4-69
Q 4.53.1	Are there additional rules that apply to companies that accept payment through e-commerce websites?	4-69
Q 4.54	What is the PCI Security Standards Council?	4-70
Q 4.55	What do the PCI DSS require?	4-71
Q 4.55.1	What are the consequences of noncompliance with PCI DSS?	4-71
Q 4.56	Are there additional standards for mobile transactions?	4-71

<i>Liability</i>	4-72
Q 4.57 Who bears the loss for a fraudulent payment card transaction?	4-72
Q 4.58 Who bears the loss in the event of a data breach?	4-73

Chapter 5 Medical Privacy

Introduction	5-2
Q 5.1 What is medical privacy?	5-2
Q 5.2 What are the principal laws and regulations relating to medical privacy?.....	5-2
<i>HIPAA Overview</i>	5-3
Q 5.3 What is HIPAA?.....	5-3
Q 5.3.1 What aspects of health information are governed by the Privacy Rule?.....	5-4
Q 5.3.2 . . . by the Security Rule?	5-5
Q 5.3.3 . . . by the Breach Notification Rule?.....	5-5
<i>Protected Health Information</i>	5-6
Q 5.4 How does HIPAA define “health information”?.....	5-6
Q 5.4.1 What information does HIPAA protect?.....	5-7
Q 5.4.2 What is PHI?	5-7
Q 5.4.3 What is individually identifiable health information?	5-7
Q 5.4.4 What is de-identified health information?.....	5-7
Q 5.4.5 What types of health information are not protected by HIPAA?	5-7
<i>Entities Subject to HIPAA</i>	5-8
Q 5.5 What types of organizations are regulated by HIPAA?	5-8
Q 5.6 What is a “covered entity” under HIPAA?.....	5-8
Q 5.6.1 What is a “covered transaction”?.....	5-8
Q 5.6.2 What health plans are covered entities?	5-8
Q 5.6.3 What healthcare clearinghouses are covered entities?	5-9
Q 5.6.4 What healthcare providers are covered entities?.....	5-9
Q 5.6.5 How can a company determine whether it is a covered entity?	5-9
Q 5.7 What is a “business associate”?	5-10

Table of Contents

<i>Obligations of and Relating to Business Associates</i>	5-11
Q 5.8 What obligations apply to business associates under HIPAA?	5-11
Q 5.9 Under what conditions can a business associate receive PHI from a covered entity?.....	5-11
Q 5.9.1 What conditions must be included in a business associate agreement?.....	5-11
Q 5.9.2 Are there model business associate agreements that a company can use for guidance?	5-12
Q 5.10 What are the obligations of subcontractors to a business associate?	5-12
Q 5.11 Are covered entities responsible for the HIPAA violations of their business associates and their subcontractors?	5-13
<i>Use and Disclosure of PHI Under the Privacy Rule</i>	5-14
Q 5.12 What restrictions does the Privacy Rule apply to the use or disclosure of PHI?.....	5-14
Q 5.12.1 What is a personal representative?.....	5-14
Q 5.12.2 What is the difference between consent and written authorization?.....	5-14
Q 5.13 When is a covered entity required to disclose PHI?	5-15
Q 5.14 When is a business associate required to disclose PHI?.....	5-15
Q 5.15 When is a covered entity or business associate permitted (but not required) to use or disclose PHI?.....	5-15
Q 5.15.1 Can an individual place restrictions on how PHI is used and disclosed by a company for treatment, payment, and healthcare business operations?.....	5-16
Q 5.15.2 Is an individual's consent required for use or disclosure of PHI for treatment, payment, and healthcare business operations?	5-16
Q 5.15.3 Can PHI ever be used or disclosed after an individual has been given an opportunity to object and does not do so?	5-17
Q 5.15.4 May additional PHI be used and disclosed incident to an otherwise permitted use or disclosure? If so, under what circumstances?	5-17
Q 5.15.5 When is it permissible for PHI to be used and disclosed in the public interest or benefit?	5-18
Q 5.15.6 Can a covered entity resist disclosing PHI in response to a subpoena?.....	5-20
Q 5.15.7 Can a covered entity or business associate use and disclose PHI for research, public health issues, or healthcare business operations?	5-21

PRIVACY LAW ANSWER BOOK 2020

Q 5.15.8	When must a company obtain written authorization to use or disclose PHI?	5-22
Q 5.15.9	What are the requirements for a valid authorization?	5-22
Q 5.15.10	How are psychotherapy notes treated under HIPAA?	5-23
Q 5.15.11	Can a company use or disclose PHI for marketing purposes? What are the requirements to do that?	5-24
Q 5.15.12	Can a company sell PHI? What are the requirements to do that?	5-24
<i>The "Minimum Necessary Standard"</i>		5-25
Q 5.16	Can a company use or disclose an individual's PHI in its entirety, or are there limitations on its use?	5-25
Q 5.16.1	Are there any circumstances in which the "minimum necessary standard" is not applicable?	5-25
Q 5.17	Are there limitations with respect to which individuals within an organization can access and use PHI?	5-25
Q 5.18	What policies are required under the minimum necessary standard?	5-26
Q 5.19	Does a company always need to evaluate whether requests for disclosures comply with the minimum necessary standard?	5-26
<i>Privacy Notices and Individual Rights</i>		5-27
Q 5.20	Must a covered entity provide notice to individuals with respect to the use and disclosure of PHI?	5-27
Q 5.21	Must a business associate provide notice to individuals with respect to the use and disclosure of PHI?	5-28
Q 5.22	How must notice be provided?	5-28
Q 5.22.1	If a company operates in an electronic environment, can it provide HIPAA privacy notices electronically?	5-28
Q 5.22.2	Does a company have to provide notice on its website?	5-28
Q 5.22.3	Are there model HIPAA privacy notices that a company can use for guidance?	5-29
Q 5.23	Does a company need to obtain acknowledgments from individuals that they have received HIPAA privacy notices?	5-29
Q 5.24	What rights do individuals have with respect to their PHI?	5-29
Q 5.24.1	What rights do individuals have to access their PHI?	5-29
Q 5.24.2	What rights do individuals have to amend inaccurate or incomplete PHI?	5-30

Table of Contents

Q 5.24.3	What rights do individuals have to request an accounting of PHI disclosures?.....	5-30
Q 5.24.4	What rights do individuals have to restrict the use or disclosure of their PHI?	5-31
Q 5.24.5	What rights do individuals have to request specific modes of communications regarding PHI?	5-32
Privacy Practices		5-32
Q 5.25	If a covered entity is a small company and/or has limited resources, is it granted any flexibility in implementing HIPAA privacy practices?	5-32
Q 5.26	What are the minimum administrative requirements a company must satisfy?	5-32
Q 5.27	Is assistance available to a company in complying with the Privacy Rule?.....	5-34
Q 5.28	What is a Coordinated Vulnerability Disclosure Policy?.....	5-34
Q 5.29	How should MDMs implement CVD policies?.....	5-35
State Laws		5-37
Q 5.30	Does the Privacy Rule preempt state law governing health information privacy?.....	5-37
Q 5.31	What state medical privacy laws apply?	5-38
Q 5.32	Does the California Consumer Privacy Act apply to healthcare entities?	5-39
HIPAA Enforcement and Private Remedies		5-39
Q 5.33	Who has enforcement authority for violations of the HIPAA Privacy Rule?.....	5-39
Q 5.34	What are the civil penalties for violating the Privacy Rule?	5-39
Q 5.34.1	What is reasonable cause?.....	5-41
Q 5.34.2	What is reasonable diligence?	5-41
Q 5.34.3	What is willful neglect?.....	5-41
Q 5.35	What criminal penalties may be imposed in connection with HIPAA violations?.....	5-41
Q 5.36	Is there a private right of action for violations of HIPAA or the Privacy Rule?	5-42

Chapter 6 Mobile Privacy

The Basics	6-3
<i>Definitions</i>	6-3
Q 6.1 What is mobile privacy?.....	6-3
Q 6.2 What are mobile applications?.....	6-3
Q 6.3 Who are the relevant players in the mobile ecosystem?.....	6-4
<i>Specific Privacy Concerns</i>	6-5
Q 6.4 What privacy concerns does the use of mobile apps raise?.....	6-5
<i>Personal Information and Other Data</i>	6-5
Q 6.5 Does any PII have a special definition in the mobile ecosystem?.....	6-5
Q 6.6 What types of persistent identifiers are significant in the mobile ecosystem?.....	6-6
Regulatory Framework	6-7
<i>Statutory Requirements and Best Practices</i>	6-7
Q 6.7 What is the U.S. legal framework governing mobile information privacy?.....	6-7
<i>Agency and Industry Guidance</i>	6-9
Q 6.7.1 What formal guidance exists for app developers?.....	6-9
Q 6.8 Are there additional privacy obligations on a company if its mobile app collects payment information?.....	6-12
Q 6.9 What restrictions exist on the ability to market mobile apps, or a company's products and services more generally, via a mobile device?.....	6-13
<i>Compliance: Privacy by Design</i>	6-13
Q 6.10 What steps should a company take, as a mobile app developer, to ensure that its apps are compliant with privacy law and best practices?.....	6-13
Q 6.10.1 How should a company implement the FTC's recommendation of privacy by design in mobile app development?.....	6-14

Table of Contents

Mobile App Privacy Policies	6-15
<i>Generally</i>	6-15
Q 6.11 If a company already has an online privacy policy, is it necessary to have a separate privacy policy for its mobile apps?	6-15
<i>Policy Terms, Disclosures</i>	6-15
Q 6.12 What terms should a company include in its mobile app privacy policy?.....	6-15
<i>Posting Requirements</i>	6-16
Q 6.13 Where should a company post its mobile app privacy policy?.....	6-16
<i>Short Form Notices</i>	6-17
Q 6.14 Is a company also required to provide a “Short Form Notice” of its information practices?	6-17
Q 6.14.1 What format should a Short Form Notice take?.....	6-17
Q 6.14.2 What terms should be included in a Short Form Notice?.....	6-18
Just-In-Time Disclosures and User Consent	6-18
<i>Requirements</i>	6-18
Q 6.15 When should a mobile application use just-in-time disclosures?	6-18
Q 6.15.1 What is an “unexpected use” of PII?	6-19
Q 6.16 What terms should be included in a mobile application’s just-in-time disclosure?.....	6-20
<i>Implementation and Compliance</i>	6-21
Q 6.17 What are the consequences of failing to provide users with adequate notice before collecting sensitive information or PII for unexpected purposes?	6-21
Q 6.18 How can an app developer make adequate disclosures about the collection of sensitive information such as a user’s geolocation?.....	6-22
Q 6.19 Can an app developer rely on just-in-time disclosures provided by the app platform?.....	6-23

Sharing PII with Third Parties.....6-23

Generally.....6-23

Q 6.20 May app developers share with third parties the PII that they collect via their mobile apps?.....6-23

Requirements.....6-23

Q 6.21 If an app developer shares with third parties PII acquired through its mobile app, what are its obligations to the app users?.....6-23

“Frictionless” Sharing.....6-26

Q 6.22 What kind of disclosure must be made to users if a developer’s mobile app is integrated with social media platforms to automatically share information on users’ actions?.....6-26

Retention of PII.....6-26

Q 6.23 Are there limitations on an app developer’s right to store the sensitive information it collects?.....6-26

Chapter 7 Digital Workplace Privacy

Monitoring of Employees’ Electronic Communications.....7-3

Federal Statutes.....7-3

Q 7.1 What major federal laws govern whether a company can monitor or access employees’ electronic communications?.....7-3

Q 7.2 What are the Electronic Communications Privacy Act and the Stored Communications Act?.....7-3

 Q 7.2.1 What types of information does the ECPA protect?.....7-3

 Q 7.2.2 Do the ECPA and SCA prohibit a company from accessing employees’ electronic communications?.....7-4

Q 7.3 What is the Computer Fraud and Abuse Act?.....7-4

State Laws and Other Protections.....7-5

Q 7.4 Are there any state laws concerning the monitoring or access of employees’ electronic communications and online activities?.....7-5

Table of Contents

<i>Employer Practices and Policies</i>	7-6
Q 7.5 What steps should a company take in order to monitor employees' electronic communications and online activity?	7-6
Q 7.5.1 What types of electronic resources should a company's policy address?	7-7
Q 7.5.2 Should a company's policy apply only to company-provided electronic resources?	7-7
Q 7.6 In what circumstances can a company review an employee's email mailbox?	7-8
Q 7.6.1 What should a company's policy state with respect to emails sent and received via a company email address?	7-8
Q 7.6.2 Can a company also access emails sent from a personal device through the company's email network?	7-8
Q 7.6.3 Can a company access emails sent or received through its employee's personal, web-based, password-protected email account on work devices?	7-9
Q 7.7 Can a company access employee text messages stored on work-issued mobile devices?	7-9
Q 7.8 Can a company access employee text messages stored on personal mobile devices?	7-11
Q 7.9 What rights does a company have to review and disclose an employee's communications in the context of litigation or a government investigation?	7-11
Q 7.9.1 Does a company have broader rights to review employee electronic communications if it is investigating potential misconduct on the part of the employee?	7-12
Social Media	7-12
<i>Employer Practices</i>	7-12
Q 7.10 Can a company monitor its employees on social media sites?	7-12
Q 7.11 Can a company ask an employee to provide passwords for personal social media accounts?	7-15
Q 7.12 Can a company provide guidelines for what its employees can or cannot post on social media sites when employees are acting in their professional capacity?	7-15
Q 7.13 Can a company provide guidelines for employees' personal use of social media?	7-15

Q 7.14	Can a company discipline or take action against an employee based on information the employee posts on a social media site?	7-16
	<i>Social Media Posts As Protected Concerted Activity</i>	7-16
Q 7.15	Are an employee’s social media posts about his job considered protected activity under the NLRA?	7-16
	<i>Employer Policies</i>	7-19
Q 7.16	Should a company have a social media policy? If so, what information should the policy include?.....	7-19
	<i>Social Media in Employment/Hiring Decisions</i>	7-20
Q 7.17	Can a company use social media to screen potential hires?	7-20
Q 7.18	Can a company require candidates to divulge passwords to private social media networks as a condition of employment?.....	7-22
	<i>Social Media in Discovery and Litigation</i>	7-22
Q 7.19	What steps should a company take with respect to social media if litigation with an employee has commenced or appears likely?	7-22
	Bring-Your-Own-Device (BYOD) Programs and Policies	7-23
Q 7.20	What is “BYOD”?.....	7-23
Q 7.20.1	What are the benefits of adopting a BYOD program?.....	7-23
Q 7.21	What are the parameters of a typical BYOD program?	7-24
Q 7.21.1	Can an employer that adopts a BYOD program access and review an employee’s personal content stored on any device used for work purposes?.....	7-24
Q 7.21.2	Is an employer obligated to reimburse employees for costs related to using their own electronic devices for work purposes?	7-25
Q 7.21.3	Is an employer obligated to pay overtime to eligible employees who use personal devices for work-related purposes?	7-26
Q 7.22	What risks are associated with a BYOD program?.....	7-27
Q 7.22.1	How can a company mitigate the legal risks associated with instituting a BYOD program?.....	7-27
Q 7.22.2	How can a company mitigate the security risks associated with instituting a BYOD program?.....	7-29

Table of Contents

Q 7.23	Does a company need a separate BYOD policy if it already has a privacy policy relating to workplace electronic devices?.....	7-30
Q 7.23.1	What information should a company’s BYOD policy include?	7-30
Q 7.23.2	Should a company have employees sign the BYOD policy?.....	7-33
Q 7.23.3	Are there additional concerns for companies that use a “bring your own account” (BYOA) or “bring your own cloud” (BYOC) model?	7-34
Tracking Employees’ Location		7-35
Q 7.24	What is location-based tracking?	7-35
Q 7.24.1	Can a company use location-based tracking to monitor the location of its employees?	7-35
Collection of Genetic Information; Genetic Testing		7-36
Q 7.25	Can a company obtain DNA samples from its employees for purposes of workplace investigations?	7-36
Background Checks		7-38
Q 7.26	What steps, if any, must a company take if it would like to obtain a background check?	7-38
Q 7.27	What steps, if any, must a company take if it would like to take an adverse employment action based on information in a background check?	7-38
 Chapter 8 Advertising, Tracking, and Privacy		
Overview		8-3
Q 8.1	What is online tracking, and how does it work?.....	8-3
Q 8.2	How is user activity online being captured?.....	8-3
Q 8.3	Can users still be identified and tracked if they “block” cookies and browser-based storage of their data?	8-4
Q 8.4	Can activity on different devices be connected?	8-4
Q 8.5	What are the differences between online behavioral advertising and content-based advertising?.....	8-5

Online Behavioral Advertising	8-5
Q 8.6 What is online behavioral advertising?.....	8-5
Q 8.6.1 How does tracking work in online behavioral advertising?.....	8-6
Q 8.6.2 What information must an operator collect for advertising to be considered online behavioral advertising?.....	8-7
Q 8.6.3 Would an operator be liable after a data breach if it had anonymized all of its data by, for example, using UUIDs?.....	8-7
Regulation, Enforcement, and Compliance	8-8
<i>Generally</i>	8-8
Q 8.7 Which government agencies are active in enforcing regulations related to online behavioral advertising?.....	8-8
Q 8.7.1 What statutes govern online behavioral advertising?.....	8-8
Q 8.7.2 How does the FTC enforce its restrictions on online behavioral advertising?.....	8-9
<i>Best Practices and Industry Guidelines</i>	8-10
Q 8.8 What are the best practices for using online behavioral advertising?.....	8-10
Q 8.9 Are there any industry guidelines for OBA best practices?.....	8-11
Q 8.9.1 What should companies do to comply with the NAI guidelines?.....	8-12
Q 8.9.2 What should companies do to comply with the DAA principles?.....	8-14
Q 8.9.3 What should a website operator’s privacy policy say about online behavioral advertising?.....	8-15
<i>California Online Privacy Protection Act</i>	8-15
Q 8.10 How does California’s “do not track” law apply to online behavioral advertising?.....	8-15
Q 8.10.1 How does an operator know whether California’s laws apply to it?.....	8-16
<i>Electronic Communications Privacy Act</i>	8-16
Q 8.11 Can consumers bring private suits against companies who use online behavioral advertising?.....	8-16
Q 8.11.1 How does the ECPA arguably apply to online behavioral advertising?.....	8-16

Table of Contents

Q 8.11.2	How can online behavioral advertising create a liability under ECPA?.....	8-17
Q 8.11.3	How can an operator reduce the likelihood of an ECPA violation?.....	8-18
<i>Computer Fraud and Abuse Act</i>		8-18
Q 8.12	How does the Computer Fraud and Abuse Act apply to online behavioral advertising?	8-18
<i>Children’s Online Privacy Protection Act</i>		8-19
Q 8.13	What OBA concerns are raised for an operator of a website directed to children?	8-19
Q 8.13.1	What must a website operator do to ensure compliance under COPPA with respect to online behavioral advertising?	8-19
<i>Video Privacy Protection Act</i>		8-20
Q 8.14	Do any specific laws apply to tracking of online user behavior regarding video content?	8-20
Q 8.14.1	How does a company know whether the VPPA applies to its website?.....	8-20
Q 8.14.2	Is anyone who watches a video online a “consumer” protected under the VPPA?.....	8-22
Q 8.14.3	When does an operator have “knowledge” it is transmitting information under the VPPA?.....	8-22
Q 8.14.4	How can a website operator reduce the likelihood of a VPPA violation?.....	8-23
Tracking and Collection of User Data		8-24
<i>Cookies</i>		8-24
Q 8.15	Can website users avoid having their information tracked for OBA?.....	8-24
Q 8.15.1	May a website operator circumvent software that allows users to block cookies?.....	8-25
<i>Data Brokers</i>		8-25
Q 8.16	What considerations are raised where an operator enables its OBA by obtaining information from a third party?.....	8-25
<i>Collection of Information from Multiple Sources</i>		8-26
Q 8.17	What considerations are raised where an operator uses OBA by collecting information from multiple websites or devices?.....	8-26

Social Media Advertising	8-27
Q 8.18 What OBA opportunities does social media afford?.....	8-27
<i>Social Context Advertising</i>	8-27
Q 8.19 What is social context advertising?.....	8-27
Q 8.19.1 What are the relevant privacy considerations when determining whether to use social context advertising on a social media platform?.....	8-28
Q 8.20 What steps should a company take when advertising on social media to ensure its advertising complies with the right-of-publicity laws?.....	8-28
Q 8.20.1 What options does an advertiser have if a social media platform’s terms of use do not provide clear disclosure and obtain consent from users?.....	8-29
Q 8.20.2 If a platform’s terms of use clearly obtain consent for the commercial use of a user’s name or likeness, are potential right-of-publicity concerns eliminated?.....	8-30

Chapter 9 California Consumer Privacy Act

Q 9.1 To which organizations does the CCPA apply?.....	9-2
Q 9.2 What kind of data is covered by the CCPA?.....	9-2
Q 9.3 What must covered businesses do under the CCPA?.....	9-3
Q 9.4 Can a business charge a fee for customers who opt out of having their data sold?.....	9-4
Q 9.4.1 Are there limits on the fee a business can charge to customers who opt out of having their data sold?.....	9-4
Q 9.4.2 What does the requirement that any fee be reasonably related to the value of the data mean in practice?.....	9-5
Q 9.4.3 Are there any other ways of compensating for the lost revenue of opt-out consumers without the uncertainty surrounding the “reasonably related” rule?.....	9-5
Q 9.5 Is it a violation of the CCPA to deny service to consumers who opt out of allowing the sale of their data?.....	9-6
Q 9.6 Who enforces the CCPA?.....	9-6
Q 9.7 Does the CCPA provide a private right of action for consumers?.....	9-6
Q 9.8 Are any types of data exempt from the CCPA?.....	9-7
Q 9.8.1 Do the data exemptions apply to CCPA’s private right of action?.....	9-9

Table of Contents

Q 9.9	How broad is the GLBA exemption under the CCPA?.....	9-9
Q 9.9.1	What information would likely fall under the GLBA exemption?.....	9-10
Q 9.9.2	What personal data that a financial institution handles would not fall under the GLBA exemption?	9-10
Q 9.9.3	What about information governed by FIPA?	9-11
Q 9.10	How does the CCPA compare to the GDPR?	9-11
Q 9.10.1	What are the similarities and differences in entities regulated by the CCPA and GDPR?	9-12
Q 9.10.2	What are the similarities and differences in the definition of “personal information” under the CCPA and GDPR?	9-12
Q 9.10.3	What do the CCPA and GDPR require of third parties?	9-12
Q 9.10.4	What are the similarities and differences in the rights afforded to consumers under the CCPA and GDPR?.....	9-13
Q 9.10.5	How do the CCPA and GDPR treat minors?.....	9-13
Q 9.10.6	What are the similarities and differences for de-identified or anonymized data under the CCPA and GDPR?	9-14
Q 9.10.7	What civil penalties may a company face for noncompliance with the CCPA and GDPR?	9-15
Q 9.11	Is the CCPA likely to be further changed before it goes into effect in 2020?	9-15
	<i>Similar Legislation in Other States</i>	9-15
Q 9.12	Do any other U.S. states have similar legislation?	9-15
Q 9.13	When does Nevada’s legislation go into effect?	9-16
Q 9.14	What are the key differences between Nevada’s SB 220 and the CCPA?	9-16
Q 9.15	What companies does Nevada’s SB 220 apply to?	9-16
Q 9.16	What obligations are imposed under Nevada’s SB 220?.....	9-16
Q 9.17	If a company is compliant with the CCPA requirements, is the company also compliant with Nevada’s SB 220?.....	9-17

Chapter 10 Privacy Enforcement and Litigation

Federal Trade Commission Enforcement	10-2
<i>The FTC Act, Section 5 Authority</i>	10-2
Q 10.1 What authority does the FTC have to take enforcement action against privacy violations?	10-2
Q 10.2 Can the FTC enforce section 5 against companies in all industries?.....	10-3
Q 10.2.1 What are the priority areas of enforcement currently for the FTC?.....	10-4
<i>FTC Investigations</i>	10-5
Q 10.3 If the FTC suspects a company is engaged in deceptive or unfair privacy practices, what does it do?.....	10-5
Q 10.3.1 How does the FTC decide to launch an investigation?	10-6
Q 10.3.2 Will the FTC provide notice of the alleged violation?.....	10-6
Q 10.3.3 What should a company do in response to an FTC investigation?.....	10-7
Q 10.3.4 How long does an FTC investigation take?	10-8
Q 10.3.5 Are investigations by the FTC publicly disclosed?	10-9
Q 10.3.6 What happens if the FTC completes its investigation and determines that no violation has occurred?	10-9
Q 10.3.7 What happens if the FTC completes its investigation and determines that a violation has likely occurred?	10-10
<i>FTC Consent Orders</i>	10-10
Q 10.4 What is a consent order?.....	10-10
Q 10.4.1 In privacy enforcement actions, what terms does a consent order typically include?.....	10-10
Q 10.4.2 What amount of civil penalty is typically included in consent orders?.....	10-11
Q 10.4.3 How long do the requirements in a consent order generally last?.....	10-11
Q 10.4.4 What are possible consequences of not complying with a consent order or court order?	10-11
<i>FTC Administrative Proceedings</i>	10-13
Q 10.5 What does an administrative proceeding involve?.....	10-13
Q 10.5.1 What are the possible outcomes of an FTC administrative hearing?	10-14
Q 10.5.2 Are there limits on what the FTC can include in a cease-and-desist order?.....	10-14
Q 10.5.3 Can an ALJ's initial decision be appealed?	10-14

Table of Contents

<i>FTC Remedies</i>	10-15
Q 10.6 Can the FTC issue a penalty for a violation of section 5?.....	10-15
Q 10.6.1 How are civil penalties assessed and imposed?	10-15
Q 10.6.2 Can the FTC obtain civil penalties from third parties?.....	10-15
Q 10.7 Can the FTC seek consumer redress?.....	10-16
Q 10.8 Can the FTC bring a criminal action for a violation of section 5?.....	10-16
Q 10.9 Can the FTC bring an action in court without first conducting an administrative hearing?.....	10-16
Federal Enforcement Other Than by the FTC	10-17
Q 10.10 What federal agencies other than the FTC bring privacy and data security enforcement cases against companies?	10-17
Enforcement by State Attorneys General	10-18
<i>State UDAP Statutes</i>	10-18
Q 10.11 What authority do state AGs have to take enforcement action with regard to privacy rights?.....	10-18
<i>Investigation of Suspected Violations</i>	10-19
Q 10.12 If a state AG suspects a violation of a UDAP law, what will the state AG do first?	10-19
Q 10.12.1 What should a company do if it receives CIDs or other legal demand from a state AG?.....	10-19
Q 10.13 Can a settlement be reached with state AGs before an action is filed in court?	10-19
<i>Enforcement Priorities and Trends</i>	10-20
Q 10.14 Are information privacy and security priorities for state attorneys general?.....	10-20
Q 10.14.1 How have state AGs been enforcing information privacy and security issues in recent years?.....	10-20
Government Requests for Data	10-21
Q 10.15 What should a company do if it receives a request from a governmental entity for electronic information it possesses?.....	10-21
<i>International Considerations</i>	10-22
Q 10.15.1 What should a company do if the information requested is stored outside the United States?.....	10-22

Q 10.16	What should a company do if it receives a legal request from a law enforcement or regulatory agency in a foreign jurisdiction for information stored in the United States?	10-23
Private Litigation/Class Actions		10-23
Q 10.17	What is a privacy class action?	10-23
Q 10.18	What kind of conduct can give rise to data privacy class actions?	10-23
Q 10.19	What kind of conduct can give rise to data security class actions?	10-24
<i>Statutory Authority</i>		10-25
Q 10.20	Upon which statutory authorities do privacy class action plaintiffs most often rely?	10-25
<i>Litigation Trends</i>		10-25
Q 10.21	What trends are current in the world of privacy class actions?	10-25
Defenses		10-27
Q 10.22	What are the most common defenses to privacy class actions concerning data privacy or data security?	10-27
Q 10.22.1	Is unjust enrichment a viable theory of recovery?	10-27
<i>Establishing Standing</i>		10-28
Q 10.23	How is a plaintiff's potential lack of standing used to challenge privacy class actions?	10-28
Q 10.23.1	Have any theories proved successful in establishing standing for privacy class action plaintiffs?	10-30
Q 10.23.2	What can a company do to defend itself if the alleged harm is intangible?	10-31
<i>Compensable Injury Under Negligence Standard</i>		10-32
Q 10.24	How are the requirements for negligence used to challenge privacy class actions?	10-32
<i>Class Certification</i>		10-33
Q 10.25	Are putative privacy class actions often certified?	10-33
Settlements		10-34
Q 10.26	What are typical terms in data privacy class action settlements?	10-34
Q 10.27	What are typical terms in data security class action settlements?	10-36

Table of Contents

Q 10.28	What is the largest settlement in FTC history?	10-36
Preventative Measures	10-37
<i>Generally</i>	10-37
Q 10.29	Are there any steps that a company can take to minimize the likelihood that it will be the defendant in a privacy class action lawsuit?	10-37
<i>Mandatory Arbitration</i>	10-38
Q 10.29.1	Can a company avoid class actions through mandatory arbitration?	10-38
<i>Cyberinsurance</i>	10-39
Q 10.30	What is cyberinsurance?	10-39
Q 10.30.1	What is first-party cyberinsurance coverage?.....	10-40
Q 10.30.2	What is third-party cyberinsurance coverage?	10-40
Q 10.30.3	Are there steps a company can take to determine whether purchasing cyberinsurance would be appropriate?.....	10-40

Chapter 11 Global Privacy Laws

The Global Landscape	11-3
<i>International Privacy Standards and Principles</i>	11-3
Q 11.1	Are there any global or international standards or principles of data privacy?.....	11-3
Q 11.1.1	Have any international bodies sought to create global or international standards of data privacy?	11-4
Q 11.2	What laws govern data privacy and transfers of data from one country to another?.....	11-6
<i>Enforcement</i>	11-7
Q 11.3	How does enforcement of privacy laws vary around the globe?	11-7
Table 11-1	Global Data Transfer Issues by Region	11-7
<i>Penalties</i>	11-10
Q 11.4	What are the consequences of a breach of data privacy laws?	11-10

Concepts of Global Privacy Laws 11-11

Covered Activities..... 11-11

Q 11.5 What activities are covered by data privacy and protection laws? 11-11

Covered Entities 11-13

Q 11.6 Are all business treated the same under global privacy laws? 11-13

Other Definitions..... 11-14

Q 11.7 What is “personal data”? 11-14

Q 11.8 What is meant by a data subject’s “consent”?..... 11-15

Q 11.9 What is meant by data access and data rectification? 11-16

Regulation of Businesses..... 11-17

Registration Requirements..... 11-17

Q 11.10 Does a business need to register to handle personal data? 11-17

Data Protection Officer Requirement 11-17

Q 11.11 Does a business need to appoint a data protection officer (DPO)? 11-17

Breach Notification..... 11-18

Q 11.12 Which countries require breach notification?..... 11-18

Employee Monitoring..... 11-20

Q 11.13 What rules apply to employee monitoring?..... 11-20

Online Sales and Marketing..... 11-21

Q 11.14 What issues arise for businesses conducting online sales and marketing? 11-21

European Union Privacy Law 11-22

GDPR 11-22

Q 11.15 What is the EU framework for data protection and privacy?..... 11-22

 Q 11.15.1 What are the principles of EU data protection laws? 11-22

 Q 11.15.2 In what countries does EU data privacy law apply? 11-23

 Q 11.15.3 What authorities enforce the EU data protection laws? 11-24

Table of Contents

<i>General Data Protection Regulation</i>	11-24
Q 11.15.4 What changes have been brought about by the GDPR?	11-24
<i>International Data Transfers</i>	11-26
Q 11.16 How can a business transfer personal data from the EU to other countries?	11-26
Q 11.16.1 What derogations permit transfers of personal data outside the EU?	11-26
Q 11.16.2 How and when are transfers of personal data outside the EU permitted by data transfer agreements or binding corporate rules?	11-27
Q 11.17 What are the current standards for data transfers between the EU and the United States?	11-27
<i>EU-U.S. Privacy Shield Framework</i>	11-28
Q 11.17.1 Under the Privacy Shield framework, what are an EU individual’s rights and legal remedies?	11-28
Q 11.17.2 How do EU and U.S. authorities cooperate to oversee and enforce the Privacy Shield framework?	11-29
Q 11.17.3 What requirements does the Privacy Shield framework impose on Participants?	11-29
Q 11.17.4 Does the Privacy Shield framework address EU concerns about possibilities under U.S. law for public authorities to access personal data being transferred?	11-31
<i>“Brexit” Consequences</i>	11-31
Q 11.18 How will the United Kingdom’s exit from the EU affect data protection law within the United Kingdom?	11-31
<i>The Right to Be Forgotten</i>	11-32
Q 11.19 What is the “right to erasure,” a/k/a the “right to be forgotten”?	11-32
Canadian Privacy Law	11-32
Q 11.20 Are there specific provisions of Canadian privacy law that U.S. businesses should be aware of?	11-32
<i>PIPEDA</i>	11-33
Q 11.21 Generally, what does Canada’s PIPEDA require?.....	11-33
Q 11.21.1 What is the jurisdictional coverage of PIPEDA, and are there sanctions for failure to comply?	11-33

PRIVACY LAW ANSWER BOOK 2020

Q 11.21.2 Under what circumstances would U.S. persons be exempt from PIPEDA? 11-34

Q 11.21.3 What are U.S. businesses' responsibilities with respect to safeguarding and retaining personal information? 11-34

Privacy Act..... 11-35

Q 11.22 Generally, what does Canada's federal Privacy Act require? 11-35

Provincial Privacy Legislation..... 11-35

Q 11.23 What are some of Canada's provincial laws that a company might be subject to?..... 11-35

Asia-Pacific Privacy Law 11-35

Q 11.24 What are the main challenges for businesses operating in Asia-Pacific? 11-35

Q 11.25 Are there regional data privacy rules in Asia-Pacific, as in Europe?..... 11-36

Q 11.26 What are the main features of national data privacy and protection laws in Asia-Pacific? 11-36

Q 11.27 What enforcement provisions are important for companies doing business in Asia to consider?..... 11-38

The Brazilian Data Protection Law..... 11-39

Q 11.28 Are there data privacy laws in Brazil, similar to Europe? 11-39

Q 11.29 What data is covered by the LGPD?..... 11-39

Q 11.30 What are some of the key provisions of the LGPD? 11-40

Q 11.31 Does the LGPD limit the transfer of personal data outside Brazil? 11-40

Q 11.32 What are the consequences for a breach of the LGPD? 11-41

Appendix 11A Global Data Protection Regulations..... App. 11A-1

Index..... I-1