

PRIVACY LAW

ANSWER BOOK

2019 Edition



PLI'S COMPLETE LIBRARY OF TREATISE TITLES

ART LAW

Art Law: The Guide for Collectors, Investors, Dealers & Artists

BANKING & COMMERCIAL LAW

Asset-Based Lending: A Practical Guide to Secured Financing
Consumer Financial Services Answer Book
Equipment Leasing—Leveraged Leasing
Financial Institutions Answer Book: Law, Governance, Compliance
Hillman on Commercial Loan Documentation
Hillman on Documenting Secured Transactions: Effective Drafting and Litigation
Maritime Law Answer Book

BANKRUPTCY LAW

Bankruptcy Deskbook
Personal Bankruptcy Answer Book

BUSINESS, CORPORATE & SECURITIES LAW

Accountants' Liability
Anti-Money Laundering: A Practical Guide to Law and Compliance
Antitrust Law Answer Book
Broker-Dealer Regulation
Conducting Due Diligence in a Securities Offering
Corporate Compliance Answer Book
Corporate Legal Departments: Practicing Law in a Corporation
Corporate Political Activities Deskbook
Corporate Whistleblowing in the Sarbanes-Oxley/Dodd-Frank Era
Covered Bonds Handbook
Cybersecurity: A Practical Guide to the Law of Cyber Risk
Derivatives Deskbook: Close-Out Netting, Risk Mitigation, Litigation
Deskbook on Internal Investigations, Corporate Compliance, and White Collar Issues
Directors' and Officers' Liability: Current Law, Recent Developments, Emerging Issues
Doing Business Under the Foreign Corrupt Practices Act
EPA Compliance and Enforcement Answer Book
Exempt and Hybrid Securities Offerings
Fashion Law and Business: Brands & Retailers
Financial Product Fundamentals: Law, Business, Compliance
Financial Services Mediation Answer Book
Financial Services Regulation Deskbook
Financially Distressed Companies Answer Book
Global Business Fraud and the Law: Preventing and Remediating Fraud and Corruption
Hedge Fund Regulation
Initial Public Offerings: A Practical Guide to Going Public
Insider Trading Law and Compliance Answer Book
Insurance and Investment Management M&A Deskbook
International Corporate Practice: A Practitioner's Guide to Global Success
Investment Adviser Regulation: A Step-by-Step Guide to Compliance and the Law
Legal Guide to the Business of Marijuana
Life at the Center: Reflections on Fifty Years of Securities Regulation
Mergers, Acquisitions and Tender Offers: Law and Strategies
Mutual Funds and Exchange Traded Funds Regulation
Outsourcing: A Practical Guide to Law and Business
Privacy Law Answer Book
Private Equity Funds: Formation and Operation
Proskauer on Privacy: A Guide to Privacy and Data Security Law in the Information Age
Public Company Deskbook: Complying with Federal Governance & Disclosure Requirements
SEC Compliance and Enforcement Answer Book
Securities Investigations: Internal, Civil and Criminal

Securities Law and Practice Deskbook
The Securities Law of Public Finance
Securities Litigation: A Practitioner's Guide
Social Media and the Law
Soderquist on Corporate Law and Practice
Sovereign Wealth Funds: A Legal, Tax and Economic Perspective
A Starter Guide to Doing Business in the United States
Technology Transactions: A Practical Guide to Drafting and Negotiating Commercial Agreements
Variable Annuities and Variable Life Insurance Regulation

COMMUNICATIONS LAW

Advertising and Commercial Speech: A First Amendment Guide
Sack on Defamation: Libel, Slander, and Related Problems
Telecommunications Law Answer Book

EMPLOYMENT LAW

Employment Law Yearbook
ERISA Benefits Litigation Answer Book
Labor Management Law Answer Book

ESTATE PLANNING AND ELDER LAW

Blattmachr on Income Taxation of Estates and Trusts
Estate Planning & Chapter 14: Understanding the Special Valuation Rules
International Tax & Estate Planning: A Practical Guide for Multinational Investors
Manning on Estate Planning
New York Elder Law
Stocker on Drawing Wills and Trusts

HEALTH LAW

FDA Deskbook: A Compliance and Enforcement Guide
Health Care Litigation and Risk Management Answer Book
Health Care Mergers and Acquisitions Answer Book
Medical Devices Law and Regulation Answer Book
Pharmaceutical Compliance and Enforcement Answer Book

IMMIGRATION LAW

Fragomen on Immigration Fundamentals: A Guide to Law and Practice

INSURANCE LAW

Business Liability Insurance Answer Book
Insurance Regulation Answer Book
Reinsurance Law

INTELLECTUAL PROPERTY LAW

Copyright Law: A Practitioner's Guide
Faber on Mechanics of Patent Claim Drafting
Federal Circuit Yearbook: Patent Law Developments in the Federal Circuit
How to Write a Patent Application
Intellectual Property Law Answer Book
Kane on Trademark Law: A Practitioner's Guide
Likelihood of Confusion in Trademark Law
Patent Claim Construction and *Markman* Hearings
Patent Law: A Practitioner's Guide
Patent Licensing and Selling: Strategy, Negotiation, Forms
Patent Litigation
Pharmaceutical and Biotech Patent Law
Post-Grant Proceedings Before the Patent Trial and Appeal Board
Substantial Similarity in Copyright Law
Trade Secrets: A Practitioner's Guide

LITIGATION

Arbitrating Commercial Disputes in the United States
Class Actions and Mass Torts Answer Book
Depositions Answer Book
Electronic Discovery Deskbook
Essential Trial Evidence: Brought to Life by Famous Trials, Films, and Fiction
Expert Witness Answer Book
Evidence in Negligence Cases
Federal Bail and Detention Handbook
How to Handle an Appeal
Medical Malpractice: Discovery and Trial
Product Liability Litigation: Current Law, Strategies and Best Practices
Sinclair on Federal Civil Practice
Trial Handbook

REAL ESTATE LAW

Commercial Ground Leases
Friedman on Contracts and Conveyances of Real Property
Friedman on Leases
Holtzschue on Real Estate Contracts and Closings: A Step-by-Step Guide to Buying and Selling Real Estate
Net Leases and Sale-Leasebacks

TAX LAW

The Circular 230 Deskbook: Related Penalties, Reportable Transactions, Working Forms
The Corporate Tax Practice Series: Strategies for Acquisitions, Dispositions, Spin-Offs, Joint Ventures, Financings, Reorganizations & Restructurings
Foreign Account Tax Compliance Act Answer Book
Internal Revenue Service Practice and Procedure Deskbook
International Tax & Estate Planning: A Practical Guide for Multinational Investors
International Tax Controversies: A Practical Guide
International Trade Law Answer Book: U.S. Customs Laws and Regulations
Langer on Practical International Tax Planning
The Partnership Tax Practice Series: Planning for Domestic and Foreign Partnerships, LLCs, Joint Ventures & Other Strategic Alliances
Private Clients Legal & Tax Planning Answer Book
Transfer Pricing Answer Book

GENERAL PRACTICE PAPERBACKS

Anatomy of a Mediation: A Dealmaker's Distinctive Approach to Resolving Dollar Disputes and Other Commercial Conflicts
Attorney-Client Privilege Answer Book
Drafting for Corporate Finance: Concepts, Deals, and Documents
Pro Bono Service by In-House Counsel: Strategies and Perspectives
Smart Negotiating: How to Make Good Deals in the Real World
Thinking Like a Writer: A Lawyer's Guide to Effective Writing & Editing
Working with Contracts: What Law School Doesn't Teach You

**Order now at www.pli.edu
Or call (800) 260-4754 Mon.–Fri., 9 a.m.–6 p.m.**

**Practising Law Institute
1177 Avenue of the Americas
New York, NY 10036**

When ordering, please use Priority Code NWS9-X.

PRIVACY LAW ANSWER BOOK

2019 Edition

Debevoise & Plimpton LLP

Edited by
**Jeremy Feigelson
Jim Pastore
Jane Shvets**

Practising Law Institute
New York City

#239465

This work is designed to provide practical and useful information on the subject matter covered. However, it is sold with the understanding that neither the publisher nor the author is engaged in rendering legal, accounting, or other professional services. If legal advice or other expert assistance is required, the services of a competent professional should be sought.

QUESTIONS ABOUT THIS BOOK?

If you have questions about billing or shipments, or would like information on our other products, please contact our **customer service department** at info@pli.edu or at (800) 260-4PLI.

For any other questions or suggestions about this book, contact PLI's **editorial department** at plipress@pli.edu.

For general information about Practising Law Institute, please visit **www.pli.edu**.

Legal Editor: Lori Wood

Copyright © 2016, 2017, 2018 by Practising Law Institute. All rights reserved. Printed in the United States of America. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of Practising Law Institute.

LCCN: 2016941654
ISBN: 978-1-4024-3141-8

About the Editors

JEREMY FEIGELSON, a litigation partner, co-chairs Debevoise & Plimpton's Cybersecurity & Data Privacy Practice and is a member of the firm's Intellectual Property & Media Group. He frequently represents clients in litigations and government investigations that involve the Internet and new technologies. His practice includes litigation and counseling on cybersecurity, data privacy, trademark, false advertising, copyright, and defamation matters. In 2017, *Expert Guide: Best of the Best USA* ranked him as one of the top thirty data privacy and cybersecurity attorneys in the United States. In 2015, *Law360* recognized him as a "Privacy MVP," and *The National Law Journal* named him a cybersecurity "Trailblazer." He is recommended for Technology: Data Protection and Privacy in *The Legal 500 United States* (2015). Mr. Feigelson joined Debevoise in 1992 and became a partner in 2001. He received his A.B. magna cum laude from Princeton University's Woodrow Wilson School of Public and International Affairs in 1984. He received his J.D. cum laude from the University of Chicago Law School in 1991, where he was admitted to the Order of the Coif and served as Articles Editor of the *Law Review*. He served as law clerk to the Hon. Milton I. Shadur, U.S. District Court for the Northern District of Illinois.

JIM PASTORE is a litigation partner and a member of Debevoise & Plimpton's Cybersecurity & Data Privacy Practice and Intellectual Property & Media Group. His practice focuses on privacy and cybersecurity issues. Mr. Pastore is recognized by *Chambers USA 2018* as a leading lawyer for Privacy and Data Security, and by *Law360* as a Rising Star for 2017 among the top cybersecurity and data privacy attorneys under forty. *Cybersecurity Docket* (2016) named Mr. Pastore one of the "Incident Response 30," a collection of thirty of the "best and brightest" incident response attorneys in the country. Mr. Pastore served for five years as an assistant U.S. Attorney in the Southern District of New York. He spent most of his time as a prosecutor with the Complex Frauds Unit and Computer Hacking and Intellectual Property Section, and successfully litigated eight jury trials to verdict. Mr. Pastore also obtained a first-of-its-kind order in the prosecution of the Rove Digital organization to prevent catastrophic Internet outage from the so-called

doomsday virus. Mr. Pastore was an associate at Debevoise from 2004 to 2009, focusing on IP litigation. He worked on a variety of high-profile matters, including the well-publicized Google Books copyright litigation. Mr. Pastore earned his J.D., with distinction, from Stanford Law School in 2004. He served as co-president of the Stanford Law & Technology Association and was a member of the *Stanford Technology Law Review*. He received his B.A., summa cum laude and Phi Beta Kappa, from the University of Notre Dame in 2001.

JANE SHVETS is a partner in Debevoise & Plimpton's Cybersecurity & Data Privacy Practice and White Collar & Regulatory Defense Group, based in the London office. Her practice focuses on white collar defense and internal investigations, in particular regarding compliance assessments; data privacy, data protection, and cybersecurity matters; and compliance with corrupt practices legislation. Ms. Shvets has also represented a variety of U.S. and foreign corporate clients in complex litigation and international arbitration matters, with a particular emphasis on Eastern Europe and Russia. She has represented clients in various industries, including transportation, natural resources, food and beverage, retail, and construction. Ms. Shvets received a J.D. with honors from Harvard Law School in 2007. During law school, Ms. Shvets served as Senior Editor of the *Harvard Law Review* and as an intern at the U.S. State Department's Office of the Legal Adviser, the Parliamentary Assembly of the Council of Europe, and the European Roma Rights Center. Ms. Shvets graduated summa cum laude from New York University in 2004.

About the Contributors

JEFFREY CUNARD, managing partner of Debevoise & Plimpton's Washington, D.C. office, leads the firm's corporate information technology practice. He is an internationally recognized practitioner in the field of the Internet and cyber law and focuses on data privacy, data protection, and cybersecurity matters. He has broad experience in transactions, including mergers and acquisitions, licenses, joint ventures, and outsourcing arrangements. Mr. Cunard's practice also encompasses U.S. and international media and telecommunications law, including privatizations and regulatory advice. He frequently works on litigation matters at the intersection of copyright and technology. Mr. Cunard graduated summa cum laude in English and Political Science from the University of California at Los Angeles in 1977 and received a J.D. in 1980 from the Yale Law School, where he was an editor of the *Yale Law Journal*. He served as law clerk to the Hon. Wm. Matthew Byrne, U.S. District Court for the Central District of California.

LUKE DEMBOSKY is a litigation partner based in Debevoise & Plimpton's Washington, D.C. office, co-chairs the firm's Cybersecurity & Data Privacy Practice, and is a member of the White Collar & Regulatory Defense Group. His practice focuses on cybersecurity incident preparation and emergency response, related civil litigation and regulatory defense, as well as national security issues. Prior to joining the firm, Mr. Dembosky served as Deputy Assistant Attorney General for National Security in the National Security Division of the U.S. Department of Justice and as Deputy Chief for Litigation in the Computer Crime and Intellectual Property Section of the Department of Justice. In the former capacity, Mr. Dembosky was the senior official responsible for managing the Department of Justice's investigation and prosecution of numerous major hacking incidents, including the cyber breaches of Sony Pictures, Target, Home Depot, Anthem, and the Office of Personnel Management, among many others. Mr. Dembosky worked on a range of transnational cybersecurity matters for the Department of Justice and served as an assistant U.S. attorney for the Western District of Pennsylvania, where he prosecuted numerous large-scale, national, and international cybersecurity and intellectual property crime cases. Mr. Dembosky

earned his J.D. cum laude from the University of Pittsburgh School of Law in 1994, where he was elected to Order of the Coif, Order of the Barristers, and was managing editor of the *University of Pittsburgh Law Review*. He received his B.A., with High Distinction, from Pennsylvania State University in 1990. Mr. Dembosky served as a law clerk to the Hon. Richard L. Nygaard of the U.S. Court of Appeals for the Third Circuit.

JYOTIN HAMID, a partner in Debevoise & Plimpton's Litigation Department, handles a diverse array of complex litigation matters, with particular focus on employment litigation and intellectual property disputes. In the employment area, he has successfully handled numerous discrimination, whistleblower, contract, compensation, and corporate raiding litigations involving high-level executives in a broad range of industries. He is also deeply involved in Debevoise's market-leading intellectual property practice. He has litigated trademark and trade dress cases involving some of the most well-known brands in the world. Mr. Hamid joined Debevoise in 1998 and became a partner in 2007. He received his J.D. in 1998 from Yale Law School, where he was a member of the *Journal of International Law*, and his B.A., summa cum laude, in 1995 from Tulane University, where he was a member of Phi Beta Kappa.

SATISH KINI, chair of Debevoise & Plimpton's Banking Group, is also a member of the Financial Institutions Group that advises clients on a wide range of regulatory and transactional issues. He has represented a variety of banks, securities broker-dealers, insurers, asset managers, and leading industry trade associations on regulatory reform issues. Mr. Kini also has led internal fact investigations of clients involving allegations of data breaches/fraud, money laundering and sanctions compliance issues, and advised clients on compliance governance and structuring. He has testified on Dodd-Frank issues before Congress and has represented clients on Dodd-Frank and other matters before the federal banking agencies, the U.S. Securities and Exchange Commission, the Financial Stability Oversight Council, and the U.S. Treasury Department and its Financial Crimes Enforcement Network (FinCEN) and Office of Foreign Assets Control (OFAC). Prior to joining Debevoise, Mr. Kini served in the Legal Division of the Federal Reserve Board and, from 1992 to 1993, clerked for the Hon. Judge Richard J. Cardamone of

the U.S. Court of Appeals for the Second Circuit. He received his B.A. magna cum laude from Colgate University in 1985 and his J.D. from Columbia University School of Law in 1992, where he was a Harlan Fiske Stone Scholar, a John M. Olin Fellow in Law and Economics, and the Managing Editor of the *Columbia Law Review*.

HENRY LEBOWITZ is a corporate partner and member of Debevoise & Plimpton's Corporate Intellectual Property Group. His practice focuses on leading the IP and technology aspects of mergers and acquisitions, financings, capital markets, and other corporate transactions. He also regularly assists clients in evaluating patents, trademarks, and other intellectual property, developing effective IP portfolios, assessing the merits of IP-related litigation and other disputes, and implementing strategies to avoid or favorably resolve such disputes. He joined Debevoise in 2017. From 1995 to 1996, Mr. Lebowitz served as a law clerk to the Hon. Raymond C. Clevenger III of the U.S. Court of Appeals for the Federal Circuit. He received a B.S. from Columbia University in 1989 and earned his J.D. in 1995 from the Columbia University School of Law, where he was a James Kent Scholar, the recipient of the Carroll G. Harper Prize in Intellectual Property, and a member of the *Columbia Law Review*.

MAURA KATHLEEN MONAGHAN is Co-Chair of Debevoise & Plimpton's Commercial Litigation Group. Her practice focuses on a wide range of complex commercial litigation, including privacy class actions, products liability, mass tort litigation, environmental, healthcare, regulatory and criminal investigations, and arbitration. Some of Ms. Monaghan's high-profile matters include representing American Airlines in litigation arising from 9/11, Toyota Motor Sales in criminal and civil litigation alleging recall-related fraud, and a major U.S. hospital network in a wide and diverse range of matters. Prior to joining Debevoise in 1998, Ms. Monaghan served as a law clerk to the Hon. Loretta A. Preska, U.S. District Court for the Southern District of New York from 1996 to 1997 and to the Hon. Dennis G. Jacobs, U.S. Court of Appeals for the Second Circuit from 1997 to 1998. Ms. Monaghan received her J.D. magna cum laude from Fordham University in 1996, where she was Order of the Coif and a Writing and Research Editor for the *Law Review*, and her B.S.F.S. cum laude from Georgetown University in 1990.

DAVID A. O'NEIL is a litigation partner and member of the Debevoise & Plimpton's White Collar & Regulatory Defense Group. His practice focuses on white collar criminal defense, internal investigations, privacy and cybersecurity, congressional investigations, and AML/sanctions enforcement defense. Mr. O'Neil served for eight years in prominent positions within the Department of Justice. In early 2014, the president and attorney general designated Mr. O'Neil to lead the Criminal Division, where he was responsible for supervising more than 600 attorneys investigating and prosecuting the full range of federal crimes, including corporate malfeasance, cybercrime, fraud offenses, and money laundering. Mr. O'Neil also served as Deputy Assistant Attorney General for the Fraud Section. Before moving to the Criminal Division, Mr. O'Neil served for three years as Senior Associate Deputy Attorney General and Chief of Staff to the Deputy Attorney General, the department's second-in-command. He also brokered a landmark agreement with major technology companies over disclosures of government demands for customer information. Mr. O'Neil began his career at DOJ as a federal prosecutor in the U.S. Attorney's Office for the Southern District of New York. He earned his J.D., magna cum laude, in 2000 from Harvard Law School, where he was an editor of the *Harvard Law Review*. He graduated magna cum laude from Princeton University with an A.B. in History in 1995. He clerked for Judge Robert D. Sack of the U.S. Court of Appeals for the Second Circuit and then for U.S. Supreme Court Justice Ruth Bader Ginsburg.

DAVID SARRATT is a partner in Debevoise & Plimpton's Litigation Department. He is an experienced trial lawyer whose practice focuses on technology and cybersecurity matters, white collar criminal defense, internal investigations, and complex civil litigation. Prior to joining the firm, Mr. Sarratt served as an assistant U.S. Attorney in the Eastern District of New York from 2010 to 2014. As a federal prosecutor, Mr. Sarratt supervised and participated in a wide variety of investigations and prosecutions involving, among other crimes, international terrorism, computer intrusions, export violations, fraud, and racketeering. He successfully tried numerous cases to verdict and briefed and argued appeals in the U.S. Court of Appeals for the Second Circuit. Mr. Sarratt received his J.D. from the University of Virginia School of Law in 2004, where he graduated Order of the Coif and was an articles editor of

About the Contributors

the *Virginia Law Review*. He earned a B.A., Phi Beta Kappa, from the University of Virginia in 2000 and served as a law clerk for the Hon. Douglas H. Ginsburg, U.S. Court of Appeals for the D.C. Circuit, and for the Hon. John Gleeson, U.S. District Court, Eastern District of New York.

Table of Chapters

Chapter 1	Overview of U.S. Information Privacy Law
Chapter 2	Privacy Policies
Chapter 3	Children’s Privacy
Chapter 4	Financial Privacy
Chapter 5	Medical Privacy
Chapter 6	Mobile Privacy
Chapter 7	Digital Workplace Privacy
Chapter 8	Advertising, Tracking, and Monetization of Consumer Data
Chapter 9	Privacy Enforcement and Litigation
Chapter 10	Global Privacy Laws

Table of Contents

About the Editors	vii
About the Contributors	ix
Table of Chapters	xv
Table of Contents	xvii
Foreword	lv
Preface	lvii
Acknowledgments	lix
Table of Abbreviations	lxi

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”?	1-5
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>	1-8
Q 1.8 How should a company provide notice to users of its information privacy practices?	1-8

PRIVACY LAW ANSWER BOOK 2019

<i>Consumer Choice and Consent</i>	1-9
Q 1.9 What does “consumer choice and consent” mean?.....	1-9
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 When 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>	1-11
Q 1.11 What should a company do to keep customer data secure?	1-11
<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?.....	1-13
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>	1-17
Q 1.18 What state laws apply to information privacy issues?.....	1-17
<i>Industry-Specific Regulation</i>	1-18
Q 1.19 What types of industry-specific laws apply to information privacy issues?	1-18

Table of Contents

<i>Technology-Specific Regulation</i>	1-19
Q 1.20 Are there any information privacy laws that apply specifically to audiovisual products?	1-19
Q 1.21 Are there any information privacy laws or guidelines that apply specifically to mobile devices and applications?	1-19
<i>Non-U.S. Regulation</i>	1-20
Q 1.22 Do other countries have laws about information privacy with which U.S.-based companies must comply?	1-20
Guidance and Best Practices	1-21
<i>Privacy Certifications</i>	1-21
Q 1.23 What are privacy certifications, and are they necessary?	1-21
<i>Industry Guidelines and Codes of Conduct</i>	1-22
Q 1.24 In addition to federal and state law, what guidance on information privacy should companies review and consider?.....	1-22
Q 1.24.1 What best practices are included in the FTC report <i>Protecting Consumer Privacy in an Era of Rapid Change</i> ?.....	1-23
<i>Social Media</i>	1-25
Q 1.25 What privacy concerns are raised for a company that integrates social media into its business plans?	1-25
Future Outlook	1-25
Q 1.26 What does the future hold for information privacy laws?	1-25

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
<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

Table of Contents

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
<i>Unfair and Deceptive Acts and Practices</i>	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.....2-27

 Q 2.19.2 What are common types of private actions brought against companies connected to their privacy policies?.....2-27

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

Collection and Disclosure of Personal Information3-9

Q 3.6 What constitutes “personal information” under COPPA?3-9

Table of Contents

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?	3-14
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	3-17
	<i>Conduct of Third Parties</i>	3-17
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?	3-17
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?	3-18

<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?.....	3-19
<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?.....	3-20
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?.....	3-21
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?.....	3-22
<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?	3-23
<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?	3-24

Table of Contents

Q 3.25	What must be included in a direct notice?	3-24
Q 3.26	What methods should be used to deliver direct notice to parents?.....	3-27
Verifiable Parental Consent		3-28
<i>General Requirement</i>		3-28
Q 3.27	When must an operator obtain verifiable parental consent?	3-28
<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?	3-30
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?	3-31
<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?	3-32
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		3-33
Q 3.32	Are there circumstances in which prior parental consent is not required?.....	3-33
<i>“One-Time Contact” Exception</i>		3-36
Q 3.33	Under what circumstances might an operator of a child-directed website or online service use the “one-time contact” exception?.....	3-36
Q 3.33.1	How does the “one-time contact” exception work in practice?.....	3-36

<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?.....	3-37
<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?	3-38
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?	3-39
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	3-40
Q 3.36 What rights do parents have to access information collected online from their children?.....	3-40
Security Obligations	3-41
Q 3.37 What security measures must an operator of a website or online service take to protect children's personal information?	3-41
Safe Harbor Programs	3-42
Q 3.38 What is the COPPA safe harbor program?	3-42
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?	3-43
Q 3.39.2 Has the FTC approved any COPPA safe harbor programs?.....	3-44

Table of Contents

Enforcement	3-44
<i>Generally</i>	3-44
Q 3.40 Who enforces COPPA?	3-44
Q 3.41 Is there a private right of action under COPPA?.....	3-44
<i>Violations/Penalties</i>	3-45
Q 3.42 What are the penalties for violation of the COPPA Rule?.....	3-45
<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?	3-47

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 2019

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?	4-11
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

Table of Contents

Q 4.12.1	Where on a company's website should privacy and opt-out notices be posted?	4-14
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>	4-22
Q 4.23 Which agencies have enforcement responsibilities for the GLBA Privacy Rule?	4-22
Q 4.24 Is there a private right of action to sue for failure to comply with the GLBA?	4-23
The Fair Credit Reporting Act	4-23
<i>The Basics</i>	4-23
Q 4.25 What is the Fair Credit Reporting Act?	4-23
Q 4.25.1 What is a “consumer” under the FCRA?	4-24
Q 4.26 What is a “credit reporting agency”?	4-24
Q 4.27 What is a “consumer report”?.....	4-25
Q 4.27.1 Is a consumer report limited to nonpublic information?.....	4-26
Q 4.27.2 What is an “investigative consumer report”?	4-26
Q 4.28 What is considered personally identifiable information for purposes of the FCRA?.....	4-27
Q 4.29 How does the FCRA limit the use of consumer report information?	4-27
<i>Duties of Users of Consumer Report Information</i>	4-28
Q 4.30 Under the FCRA, does a user of consumer report information owe any duty to the CRA that provides the report?	4-28
Q 4.30.1 Does a company have a responsibility to notify a consumer about how it uses his consumer report?	4-28
Q 4.30.2 Do users of consumer reports have an obligation to protect the consumer’s information?	4-29
Q 4.31 May a user of consumer reports also provide consumer report information to a third party without becoming a CRA?.....	4-29
Q 4.31.1 May a user of consumer reports share consumer report information with its affiliates?	4-30

Table of Contents

Q 4.31.2	How can “other information” be shared among affiliated companies?	4-30
Q 4.32	Do companies that use consumer reports for employment purposes have additional duties?	4-30
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?	4-32
Q 4.33	Do employers taking adverse action based on non-consumer report information have to notify the employee?	4-33
Q 4.34	Are investigative consumer reports treated differently?	4-33
Q 4.35	Do furnishers of consumer report information to CRAs have additional obligations under the FCRA?	4-34
	<i>Prescreened Offers of Credit or Insurance</i>	4-35
Q 4.36	What is a prescreened offer?	4-35
Q 4.36.1	Does the FCRA permit the use of consumer report information to make a prescreened offer?	4-35
Q 4.36.2	What is a firm offer of credit?	4-36
Q 4.36.3	Can a company combine a firm offer of credit with an offer for products and services?	4-37
Q 4.37	What disclosures are users of prescreening services required to make?.....	4-38
Q 4.37.1	What requirements regarding format and content must prescreen opt-out notices meet?	4-38
Q 4.37.2	Are there special considerations for electronic prescreened notices?.....	4-39
	<i>The Affiliate Marketing Rule</i>	4-40
Q 4.38	What is the Affiliate Marketing Rule?.....	4-40
Q 4.38.1	What is “eligibility information”?	4-40
Q 4.38.2	What does it mean to “make a solicitation”?	4-41
Q 4.39	Is Internet marketing considered a solicitation under the Affiliate Marketing Rule?.....	4-42
Q 4.39.1	Can a company market to consumers based on information accessed from a database shared among affiliates?.....	4-43
Q 4.39.2	What is constructive sharing?	4-43
Q 4.40	What form of notice is required by the Affiliate Marketing Rule?	4-43
Q 4.40.1	Can companies consolidate affiliate marketing notices with notices required by other laws or regulations?	4-45

Q 4.40.2	Which affiliate must provide notice?	4-45
Q 4.40.3	What content is required in the notice?	4-46
Q 4.40.4	For which affiliates is a consumer’s opt-out effective?	4-47
Q 4.40.5	Can an opt-out notice be provided in electronic form, and if so, how?	4-48
Q 4.41	Are there exceptions to the Affiliate Marketing Rule?	4-48
Q 4.41.1	When do a company and a consumer have a pre-existing relationship?	4-49
Q 4.41.2	Does a consumer’s response to a free promotional offer create a pre-existing business relationship?	4-49
Q 4.41.3	Can servicing rights create a pre-existing relationship with a consumer?	4-50
<i>The Identity Theft Red Flag Rules</i>		4-50
Q 4.42	What are the Identity Theft Red Flag Rules?	4-50
Q 4.42.1	What companies are covered by the Red Flag Rules?	4-50
Q 4.43	What elements are required in an Identity Theft Prevention Program?	4-52
Q 4.43.1	How should a company’s Identity Theft Prevention Program identify relevant red flags?	4-52
Q 4.43.2	How should a company’s Identity Theft Prevention Program comply with its obligation to detect red flags?	4-53
Q 4.43.3	How should a company’s Identity Theft Prevention Program respond to detected red flags?	4-53
Q 4.43.4	What are a company’s obligations with respect to updating its Identity Theft Prevention Program?	4-54
Q 4.43.5	What are a company’s obligations with respect to oversight and administration of its Identity Theft Prevention Program?	4-54
<i>Enforcement of the FCRA</i>		4-54
Q 4.44	Which agencies enforce the FCRA?	4-54
Q 4.44.1	How do the CFPB and FTC enforce a violation of the FCRA?	4-55
Q 4.44.2	Can the CFPB or FTC assess a penalty or fine against a company for a violation of the FCRA?	4-55
Q 4.44.3	Can state authorities also enforce the FCRA?	4-56
Q 4.45	Is there a private right of action for failure to comply with the FCRA?	4-56

Table of Contents

State Financial Privacy Regulation	4-57
Q 4.46 Are there any state laws that protect personal financial information?	4-57
Q 4.47 Aren't state financial privacy laws preempted by the federal laws?	4-57
Q 4.48 Do any states impose greater privacy duties on financial institutions than those provided for by federal law?	4-60
Q 4.48.1 What is the California Financial Privacy Act (SB1)?	4-60
Q 4.48.2 What is New York's regulation entitled "Cybersecurity Requirements for Financial Services Companies"?	4-62
Q 4.49 What are some important considerations regarding state regulation of privacy for companies that do business in multiple states?	4-63
Payment Card Transactions	4-63
<i>Overview</i>	4-63
Q 4.50 Are there specific financial privacy issues related to payment card transactions?	4-63
Q 4.51 Who is involved in a payment card transaction?	4-64
Q 4.51.1 Who are card associations?	4-64
Q 4.51.2 Who is an issuer bank?	4-64
Q 4.51.3 Who is an acquirer bank?	4-64
Q 4.51.4 Who is a payment processor?	4-65
<i>Processing Payment Card Transactions: Authorization; Clearing and Settlement</i>	4-65
Q 4.52 How is a payment card transaction processed?	4-65
Q 4.52.1 How does the payment card authorization process work?	4-65
Q 4.52.2 How does the payment card clearing and settlement process work?	4-66
Q 4.52.3 How are the issuer and acquirer paid?	4-66
<i>Industry Standards</i>	4-66
Q 4.53 What responsibilities do parties involved in payment card transactions have?	4-66
Q 4.53.1 Are there additional rules that apply to companies that accept payment through e-commerce websites?	4-67
Q 4.54 What is the PCI Security Standards Council?	4-68

Q 4.55	What do the PCI DSS require?	4-68
Q 4.55.1	What are the consequences of noncompliance with PCI DSS?	4-69
Q 4.56	Are there additional standards for mobile transactions?	4-69
<i>Liability</i>		4-70
Q 4.57	Who bears the loss for a fraudulent payment card transaction?	4-70
Q 4.58	Who bears the loss in the event of a data breach?	4-70

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?	5-6
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

Table of Contents

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
	<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?	5-16
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
Q 5.15.8	When must a company obtain written authorization to use or disclose PHI?	5-21
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>		5-24
Q 5.16	Can a company use or disclose an individual's PHI in its entirety, or are there limitations on its use?	5-24
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?	5-25
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?	5-27
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?	5-28

Table of Contents

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
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?	5-31
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
State Laws	5-34
Q 5.28	Does the Privacy Rule preempt state law governing health information privacy?	5-34
Q 5.29	What state medical privacy laws apply?	5-35
HIPAA Enforcement and Private Remedies	5-36
Q 5.30	Who has enforcement authority for violations of the HIPAA Privacy Rule?	5-36
Q 5.31	What are the civil penalties for violating the Privacy Rule?	5-36
Q 5.31.1	What is reasonable cause?	5-37
Q 5.31.2	What is reasonable diligence?	5-37
Q 5.31.3	What is willful neglect?	5-38
Q 5.32	What criminal penalties may be imposed in connection with HIPAA violations?	5-38
Q 5.33	Is there a private right of action for violations of HIPAA or the Privacy Rule?	5-38

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

Requirements6-23

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 Communications7-3

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?	7-14
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>	7-18
Q 7.16 Should a company have a social media policy? If so, what information should the policy include?.....	7-18
<i>Social Media in Employment/Hiring Decisions</i>	7-19
Q 7.17 Can a company use social media to screen potential hires?	7-19
Q 7.18 Can a company require candidates to divulge passwords to private social media networks as a condition of employment?.....	7-21
<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?	7-23
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?.....	7-28
Q 7.23 Does a company need a separate BYOD policy if it already has a privacy policy relating to workplace electronic devices?.....	7-29

Table of Contents

Q 7.23.1	What information should a company's BYOD policy include?.....	7-29
Q 7.23.2	Should a company have employees sign the BYOD policy?	7-32
Tracking Employees' Location		7-33
Q 7.24	What is location-based tracking?	7-33
Q 7.24.1	Can a company use location-based tracking to monitor the location of its employees?	7-33
Collection of Genetic Information; Genetic Testing		7-34
Q 7.25	Can a company obtain DNA samples from its employees for purposes of workplace investigations?	7-34
Background Checks		7-35
Q 7.26	What steps, if any, must a company take if it would like to obtain a background check?	7-35
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?	7-36

Chapter 8 Advertising, Tracking, and Monetization of Consumer Data

Overview		8-3
Q 8.1	What is online tracking, and how does it work?.....	8-3
Q 8.2	What are the differences between OBA and content-based advertising?	8-3
Online Behavioral Advertising		8-4
Q 8.3	What is online behavioral advertising?	8-4
Q 8.3.1	How does tracking work in OBA?.....	8-4
Q 8.3.2	What information must an operator collect for advertising to be considered OBA?	8-5
Q 8.3.3	Would an operator be liable after a data breach if it had anonymized all of its data by, for example, using UUIDs?	8-6

Regulation, Enforcement, and Compliance	8-6
<i>Generally</i>	8-6
Q 8.4 Which government agencies are active on OBA?	8-6
Q 8.4.1 What statutes govern OBA?	8-7
Q 8.4.2 How does the FTC enforce its restrictions on OBA?	8-7
<i>Best Practices and Industry Guidelines</i>	8-9
Q 8.5 What are the best practices for using OBA?	8-9
Q 8.6 Are there any industry guidelines for OBA best practices?	8-10
Q 8.6.1 What should companies do to comply with the NAI guidelines?	8-10
Q 8.6.2 What should companies do to comply with the DAA principles?	8-11
Q 8.6.3 What should a website operator’s privacy policy say about OBA?	8-12
<i>California Online Privacy Protection Act</i>	8-12
Q 8.7 How does California’s “do not track” law apply to OBA?	8-12
Q 8.7.1 How does an operator know whether California’s laws apply to it?	8-13
<i>Electronic Communications Privacy Act</i>	8-13
Q 8.8 Can consumers bring private suits against companies who use OBA?	8-13
Q 8.8.1 How does the ECPA arguably apply to OBA?	8-13
Q 8.8.2 How can OBA create a liability under ECPA?	8-14
Q 8.8.3 How can an operator reduce the likelihood of an ECPA violation?	8-15
<i>Computer Fraud and Abuse Act</i>	8-15
Q 8.9 How does the Computer Fraud and Abuse Act apply to OBA?	8-15
<i>Children’s Online Privacy Protection Act</i>	8-16
Q 8.10 What OBA concerns are raised for an operator of a website directed to children?	8-16
Q 8.10.1 What must a website operator do to ensure compliance under COPPA with respect to OBA?	8-16
<i>Video Privacy Protection Act</i>	8-17
Q 8.11 Do any specific laws apply to tracking of online user behavior regarding video content?	8-17

Table of Contents

Q 8.11.1	How does a company know whether the VPPA applies to its website?	8-17
Q 8.11.2	Is anyone who watches a video online a “consumer” protected under the VPPA?	8-19
Q 8.11.3	When does an operator have “knowledge” it is transmitting information under the VPPA?	8-19
Q 8.11.4	How can a website operator reduce the likelihood of a VPPA violation?	8-20
Tracking and Collection of User Data		8-22
<i>Cookies</i>		8-22
Q 8.12	Can website users avoid having their information tracked for OBA?.....	8-22
Q 8.12.1	May a website operator circumvent software that allows users to block cookies?	8-22
<i>Data Brokers</i>		8-23
Q 8.13	What considerations are raised where an operator enables its OBA by obtaining information from a third party?.....	8-23
<i>Collection of Information from Multiple Sources</i>		8-23
Q 8.14	What considerations are raised where an operator uses OBA by collecting information from multiple websites or devices?	8-23
Social Media Advertising		8-24
Q 8.15	What OBA opportunities does social media afford?.....	8-24
<i>Social Context Advertising</i>		8-25
Q 8.16	What is social context advertising?	8-25
Q 8.16.1	What are the relevant privacy considerations when determining whether to use social context advertising on a social media platform?	8-25
Q 8.17	What steps should a company take when advertising on social media to ensure its advertising complies with the right-of-publicity laws?	8-26
Q 8.17.1	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?.....	8-26
Q 8.17.2	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?.....	8-27

California Consumer Privacy Act	8-27
Q 8.18 What organizations does the California Consumer Privacy Act apply to?	8-28
Q 8.19 What kind of data is covered by the California Consumer Privacy Act?	8-28
Q 8.20 What must covered businesses do under the California Consumer Privacy Act?	8-29
Q 8.21 Can a business charge a fee for customers who opt out of having their data sold?	8-30
Q 8.22 How does the California Consumer Privacy Act compare to the GDPR?	8-30
Q 8.23 What should businesses do to prepare for the CCPA?	8-31

Chapter 9 Privacy Enforcement and Litigation

Federal Trade Commission Enforcement	9-2
<i>The FTC Act, Section 5 Authority</i>	9-2
Q 9.1 What authority does the FTC have to take enforcement action against privacy violations?.....	9-2
Q 9.2 Can the FTC enforce section 5 against companies in all industries?	9-3
Q 9.2.1 What are the priority areas of enforcement currently for the FTC?.....	9-4
<i>FTC Investigations</i>	9-5
Q 9.3 If the FTC suspects a company is engaged in deceptive or unfair privacy practices, what does it do?.....	9-5
Q 9.3.1 How does the FTC decide to launch an investigation?.....	9-6
Q 9.3.2 Will the FTC provide notice of the alleged violation?.....	9-6
Q 9.3.3 What should a company do in response to an FTC investigation?.....	9-6
Q 9.3.4 How long does an FTC investigation take?	9-8
Q 9.3.5 Are investigations by the FTC publicly disclosed?	9-8
Q 9.3.6 What happens if the FTC completes its investigation and determines that no violation has occurred?	9-9
Q 9.3.7 What happens if the FTC completes its investigation and determines that a violation has likely occurred?	9-9

Table of Contents

<i>FTC Consent Orders</i>	9-10
Q 9.4 What is a consent order?.....	9-10
Q 9.4.1 In privacy enforcement actions, what terms does a consent order typically include?.....	9-10
Q 9.4.2 What amount of civil penalty is typically included in consent orders?.....	9-11
Q 9.4.3 How long do the requirements in a consent order generally last?.....	9-11
Q 9.4.4 What are possible consequences of not complying with a consent order or court order?.....	9-11
<i>FTC Administrative Proceedings</i>	9-13
Q 9.5 What does an administrative proceeding involve?.....	9-13
Q 9.5.1 What are the possible outcomes of an FTC administrative hearing?.....	9-14
Q 9.5.2 Are there limits on what the FTC can include in a cease-and-desist order?.....	9-14
Q 9.5.3 Can an ALJ's initial decision be appealed?.....	9-14
<i>FTC Remedies</i>	9-15
Q 9.6 Can the FTC issue a penalty for a violation of section 5?.....	9-15
Q 9.6.1 How are civil penalties assessed and imposed?.....	9-15
Q 9.6.2 Can the FTC obtain civil penalties from third parties?.....	9-15
Q 9.7 Can the FTC seek consumer redress?.....	9-16
Q 9.8 Can the FTC bring a criminal action for a violation of section 5?.....	9-16
Q 9.9 Can the FTC bring an action in court without first conducting an administrative hearing?.....	9-16
Federal Enforcement Other Than by the FTC	9-17
Q 9.10 What federal agencies other than the FTC bring privacy and data security enforcement cases against companies?.....	9-17
Enforcement by State Attorneys General	9-18
<i>State UDAP Statutes</i>	9-18
Q 9.11 What authority do state AGs have to take enforcement action with regard to privacy rights?.....	9-18

<i>Investigation of Suspected Violations</i>	9-19
Q 9.12 If a state AG suspects a violation of a UDAP law, what will the state AG do first?	9-19
Q 9.12.1 What should a company do if it receives CIDs or other legal demand from a state AG?.....	9-19
Q 9.13 Can a settlement be reached with state AGs before an action is filed in court?	9-19
<i>Enforcement Priorities and Trends</i>	9-20
Q 9.14 Are information privacy and security priorities for state attorneys general?.....	9-20
Q 9.14.1 How have state AGs been enforcing information privacy and security issues in recent years?.....	9-20
Government Requests for Data	9-21
Q 9.15 What should a company do if it receives a request from a governmental entity for electronic information it possesses?	9-21
<i>International Considerations</i>	9-22
Q 9.15.1 What should a company do if the information requested is stored outside the United States?.....	9-22
Q 9.16 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?	9-23
Private Litigation/Class Actions	9-23
Q 9.17 What is a privacy class action?	9-23
Q 9.18 What kind of conduct can give rise to data privacy class actions?	9-23
Q 9.19 What kind of conduct can give rise to data security class actions?	9-24
<i>Statutory Authority</i>	9-25
Q 9.20 Upon which statutory authorities do privacy class action plaintiffs most often rely?.....	9-25
<i>Litigation Trends</i>	9-25
Q 9.21 What trends are current in the world of privacy class actions?	9-25

Table of Contents

Defenses	9-27
Q 9.22 What are the most common defenses to privacy class actions concerning data privacy or data security?	9-27
Q 9.22.1 Is unjust enrichment a viable theory of recovery?	9-27
<i>Establishing Standing</i>	9-28
Q 9.23 How is a plaintiff's potential lack of standing used to challenge privacy class actions?	9-28
Q 9.23.1 Have any theories proved successful in establishing standing for privacy class action plaintiffs?	9-30
Q 9.23.2 What can a company do to defend itself if the alleged harm is intangible?	9-31
<i>Compensable Injury Under Negligence Standard</i>	9-32
Q 9.24 How are the requirements for negligence used to challenge privacy class actions?	9-32
<i>Class Certification</i>	9-33
Q 9.25 Are putative privacy class actions often certified?	9-33
Settlements	9-34
Q 9.26 What are typical terms in data privacy class action settlements?	9-34
Q 9.27 What are typical terms in data security class action settlements?	9-35
Preventative Measures	9-36
<i>Generally</i>	9-36
Q 9.28 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?	9-36
<i>Mandatory Arbitration</i>	9-36
Q 9.28.1 Can a company avoid class actions through mandatory arbitration?	9-36
<i>Cyberinsurance</i>	9-38
Q 9.29 What is cyberinsurance?	9-38
Q 9.29.1 What is first-party cyberinsurance coverage?	9-38
Q 9.29.2 What is third-party cyberinsurance coverage?	9-39

Q 9.29.3 Are there steps a company can take to determine whether purchasing cyberinsurance would be appropriate?.....9-39

Chapter 10 Global Privacy Laws

The Global Landscape10-3

International Privacy Standards and Principles.....10-3

Q 10.1 Are there any global or international standards or principles of data privacy?10-3

 Q 10.1.1 Have any international bodies sought to create global or international standards of data privacy?.....10-4

Q 10.2 What laws govern data privacy and transfers of data from one country to another?.....10-6

Enforcement.....10-7

Q 10.3 How does enforcement of privacy laws vary around the globe?10-7

Figure 10-1 Global Data Transfer Issues by Region.....10-8

Penalties.....10-9

Q 10.4 What are the consequences of a breach of data privacy laws? 10-9

Concepts of Global Privacy Laws10-10

Covered Activities.....10-10

Q 10.5 What activities are covered by data privacy and protection laws?10-10

Covered Entities.....10-12

Q 10.6 Are all business treated the same under global privacy laws?10-12

Other Definitions.....10-13

Q 10.7 What is “personal data”?10-13

Q 10.8 What is meant by a data subject’s “consent”?.....10-14

Q 10.9 What is meant by data access and data rectification?10-15

Table of Contents

Regulation of Businesses	10-16
<i>Registration Requirements</i>	10-16
Q 10.10 Does a business need to register to handle personal data?	10-16
<i>Data Protection Officer Requirement</i>	10-16
Q 10.11 Does a business need to appoint a data protection officer (DPO)?	10-16
<i>Breach Notification</i>	10-17
Q 10.12 Which countries require breach notification?.....	10-17
<i>Employee Monitoring</i>	10-19
Q 10.13 What rules apply to employee monitoring?.....	10-19
<i>Online Sales and Marketing</i>	10-20
Q 10.14 What issues arise for businesses conducting online sales and marketing?	10-20
European Union Privacy Law	10-21
<i>GDPR</i>	10-21
Q 10.15 What is the EU framework for data protection and privacy?.....	10-21
Q 10.15.1 What are the principles of EU data protection laws?.....	10-21
Q 10.15.2 In what countries does EU data privacy law apply?	10-22
Q 10.15.3 What authorities enforce the EU data protection laws?	10-23
<i>General Data Protection Regulation</i>	10-23
Q 10.15.4 What changes have been brought about by the GDPR?.....	10-23
<i>International Data Transfers</i>	10-24
Q 10.16 How can a business transfer personal data from the EU to other countries?.....	10-24
Q 10.16.1 What derogations permit transfers of personal data outside the EU?.....	10-25
Q 10.16.2 How and when are transfers of personal data outside the EU permitted by data transfer agreements or binding corporate rules?	10-26
Q 10.17 What are the current standards for data transfers between the EU and the United States?	10-26

<i>EU-U.S. Privacy Shield Framework</i>	10-27
Q 10.17.1 Under the Privacy Shield framework, what are an EU individual's rights and legal remedies?	10-27
Q 10.17.2 How do EU and U.S. authorities cooperate to oversee and enforce the Privacy Shield framework?	10-28
Q 10.17.3 What requirements does the Privacy Shield framework impose on Participants?	10-28
Q 10.17.4 Does the Privacy Shield framework address EU concerns about possibilities under U.S. law for public authorities to access personal data being transferred?	10-29
<i>"Brexit" Consequences</i>	10-30
Q 10.18 How will the United Kingdom's exit from the EU affect data protection law within the United Kingdom?	10-30
<i>The Right to Be Forgotten</i>	10-30
Q 10.19 What is the "right to erasure," a/k/a the "right to be forgotten"?	10-30
Canadian Privacy Law	10-31
Q 10.20 Are there specific provisions of Canadian privacy law that U.S. businesses should be aware of?	10-31
<i>PIPEDA</i>	10-31
Q 10.21 Generally, what does Canada's PIPEDA require?.....	10-31
Q 10.21.1 What is the jurisdictional coverage of PIPEDA, and are there sanctions for failure to comply?	10-32
Q 10.21.2 Under what circumstances would U.S. persons be exempt from PIPEDA?	10-33
Q 10.21.3 What are U.S. businesses' responsibilities with respect to safeguarding and retaining personal information?	10-33
<i>Privacy Act</i>	10-33
Q 10.22 Generally, what does Canada's federal Privacy Act require?	10-33
<i>Provincial Privacy Legislation</i>	10-34
Q 10.23 What are some of Canada's provincial laws that a company might be subject to?	10-34

Table of Contents

Asia-Pacific Privacy Law	10-34
Q 10.24 What are the main challenges for businesses operating in Asia-Pacific?	10-34
Q 10.25 Are there regional data privacy rules in Asia-Pacific, as in Europe?.....	10-35
Q 10.26 What are the main features of national data privacy and protection laws in Asia-Pacific?	10-35
Q 10.27 What enforcement provisions are important for companies doing business in Asia to consider?.....	10-37
The Brazilian Data Protection Law	10-37
Q 10.28 Are there data privacy laws in Brazil, similar to Europe?	10-37
Q 10.29 What data is covered by the LGPD?.....	10-38
Q 10.30 What are some of the key provisions of the LGPD?	10-38
Q 10.31 Does the LGPD limit the transfer of personal data outside Brazil?	10-39
Q 10.32 What are the consequences for a breach of the LGPD?	10-39
Appendix 10A Global Data Protection Regulations.....	App. 10A-1
Index	I-1

Foreword

This edition of *Privacy Law Answer Book* confirms what the first two showed readers: Digital technology and the law of privacy are locked in a never-ending game of leapfrog. Since the last edition of this book, consumer adoption of mobile devices and online tools has shown no signs of slowing. More than three quarters of Americans now own a smartphone, compared to just a third in 2011. Meanwhile, the U.S. Congress has begun what may be its most serious look ever at the regulation of social media; American businesses (and their counterparts around the world) began to wrestle in earnest with the European Union's General Data Protection Regulation (GDPR) as it finally came into effect; and, at press time, it was widely expected that the U.S. Supreme Court would soon take another crack at the law of standing in privacy class actions.

This dizzying pace of change is a constant. When I started my legal career in 2001, a dial-up connection was still the primary method for accessing the Internet, and flip phones with a low-quality camera were on the cutting edge. Today, of course, a website has morphed from a trendy luxury to a must-have for any consumer-facing company, social media has gone from non-existent to mission critical, and countless businesses now offer mobile applications. Now Big Data and artificial intelligence are accelerating businesses' ability to know more about their consumers and their prospects than ever before. And as computing ability improves, the ability to turn the ever-expanding pool of collectible data into business value improves as well.

The law of privacy takes on ever-increasing importance in the face of these changes. The transparency and nature of the collection and use of personal information are under more and more scrutiny and legal regulation. As Director of Privacy at Penguin Random House in the midst of this changing landscape, I have found myself asking questions that companies never encountered in the pre-digital dark ages (i.e., a few years ago): What kind of information do we collect about our consumers? How much of that information does the law call "personal"?

How do we notify consumers of what we collect? How are we permitted to use that information? Where (geographically) can we keep and transfer data? How might the GDPR and other global privacy laws like Brazil's Data Protection Law touch U.S. companies? How have U.S. courts and legislatures reacted to the digital revolution thus far? Where might they take privacy law next?

The 2019 edition of the *Privacy Law Answer Book* provides a reference guide for practitioners asking the same kinds of questions I do. Unlike Europe, the United States has no single, omnibus law on privacy. It is no small task to quickly synthesize the patchwork of privacy laws and regulations that the U.S. federal government and the states impose on business. With this book, attorneys can react quickly as issues arise regarding their clients' evolving collection, use, and storage of personal information.

Providing effective advice on privacy requires attorneys to ask questions as early in the technological development cycle as possible. From the development of internal databases to external marketing applications, key decisions about the collection and use of personal information are made early and often on the business side. *Privacy Law Answer Book* is a tremendous resource for lawyers and other privacy practitioners, allowing them not just to keep pace with the latest developments in privacy, but also to ensure that their clients do not get legally left behind as they work to stay one step ahead of the data privacy challenges of tomorrow.

MIN J. LEE, ESQ.
New York, New York
August 2018

Preface

In a nineteenth-century article still frequently cited as the root of legal privacy rights in the United States, future Supreme Court Justice Louis Brandeis and his co-author Samuel Warren famously argued for a “right to be left alone.”¹ More than 100 years later, commenting on privacy in the digital age, a Silicon Valley CEO famously said: “You have zero privacy anyway. Get over it.”²

Legislatures, regulators, enforcement agencies, and courts in the United States continue to wrestle with the tension reflected in these statements. There continues to be a widely held intuition that the law should place some limits on what one can do with another’s private information. Yet technology races ahead, offering more and more benefits in our daily lives—benefits that are widely welcomed and that often depend on the liberal use of personal data by commercial actors.

Government authorities try to balance these competing concerns through information privacy law. This answer book focuses on the laws that govern how private-sector entities handle personal information in commercial settings. Although personal information is collected and stored in multiple ways, including old-fashioned paper records, this book focuses on electronic data. In particular, this book addresses online privacy policies, the Children’s Online Privacy and Protection Act (COPPA), mobile device privacy, financial privacy, medical privacy, workplace privacy, online behavioral advertising and tracking, and privacy enforcement and litigation. The book concludes with a brief survey of global privacy issues for U.S. lawyers. These are currently among the most discussed and developed topics in privacy law.

In addressing these topics, this answer book aims to address the practical daily needs of both expert privacy attorneys and those

1. Brandeis & Warren, *The Right to Privacy*, 4 HARVARD L. REV. 193 (1899).
2. Polly Springer, *Sun on Privacy*, “*Get Over It*,” WIRED (Jan. 26, 1999) (quoting Sun-Microsystems CEO Scott McNealy).

attorneys who encounter privacy topics in their practice but who may not specialize in these areas of the law. The book is also intended to serve as a useful reference for non-lawyers who may encounter privacy-related issues in their everyday business affairs. Our team hopes that we have met those goals. We welcome feedback from readers to let us know if we have.

JEREMY FEIGELSON & JIM PASTORE
Debevoise & Plimpton LLP
New York, New York

JANE SHVETS
Debevoise & Plimpton LLP
London, England
September 2018

Acknowledgments

This book reflects the teamwork and dedication of many Debevoise & Plimpton attorneys. Special thanks to associates Will Bucher, Jeremy Beutler, and Joshua Shirley who acted as Managing Editors for the 2019 edition, for coordinating the team's efforts to drive this edition to completion.

The firm and the editors thank their colleagues, partners Jeffrey Cunard, Luke Dembosky, Jyotin Hamid, Satish Kini, Henry Lebowitz, Maura Monaghan, David O'Neil, and David Sarratt; and associates Christopher Ford, Chris Garrett, Jared Kagan, Robert Maddox, Friedrich Popp, Naeha Prakash, Olena Ripnick-O'Farrell, Ayushi Sharma, Max Shaul, and Zheng Wang.

Table of Abbreviations

Acronyms, initialisms, and abbreviations used in this book:

AG	attorney general
ALJ	administrative law judge
ATDS	automatic telephone dialing system
BCRs	binding corporate rules
CalOPPA	California Online Privacy Protection Act
CDT	Center for Democracy and Technology
CFAA	Computer Fraud and Abuse Act
CFPB	Consumer Financial Protection Bureau
CFTC	Commodity Futures Trading Commission
CGL	commercial general liability
CID	civil investigative demand
CJEU	Court of Justice of the European Union
CMS	Centers for Medicare and Medicaid Services
CNP	card-not-present (transaction)
COPPA	Children's Online Privacy Protection Act
CPBRA	Consumer Privacy Bill of Rights Act of 2015
CPNI	customer proprietary network information
CRA	credit reporting agency
CTIA	Cellular Telecommunications Industry Association
CVV2	card verification value 2
DAA	Digital Advertising Alliance
DPA	data protection authority
DPO	data protection officer
DTA	data transfer agreement
ECPA	Electronic Communications Privacy Act of 1986

Acronyms, initialisms, and abbreviations used in this book:

EEA	European Economic Area
FAQ	frequently asked question
FCC	Federal Communications Commission
FCRA	Fair Credit Reporting Act of 1970
FCTA	Fair and Accurate Credit Transactions Act of 2003
FDIC	Federal Deposit Insurance Corporation
FERPA	Family Educational Rights and Privacy Act
FFIEC	Federal Financial Institutions Examination Council
FMVPI	face match to verified photo identification
FTC	Federal Trade Commission
GDPR	(European Union) General Data Protection Regulation
GLBA	Gramm-Leach-Bliley Act
HHS	U.S. Department of Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act
IBIPA	Illinois Biometric Information Privacy Act
IFA	Apple Identifier for Advertisers
IFV	Apple Identifier for Vendors
IP	Internet Protocol
ISP	Internet service provider
IMEI	international mobile equipment identity
MAC	media access control
NAI	Network Advertising Initiative
NCUA	National Credit Union Association
NDNCR	national do-not-call registry
NPI	nonpublic personal information
NTIA	National Telecommunications and Information Administration (U.S. Department of Commerce)
OBA	online behavioral advertising

Table of Abbreviations

Acronyms, initialisms, and abbreviations used in this book:

OCC	Office of Comptroller of the Currency
OTRI	Office of Technology Research and Investigation
OTS	Office of Thrift Supervision
PA-DSS	Payment Application Data Security Standard
PCI	payment card industry
PCI DSS	Payment Card Industry Data Security Standards
PII	personally identifiable information
SB1	California Financial Information Privacy Act
SCA	Stored Communications Act
TCPA	Telephone Consumer Protection Act of 1991
UDAP	unfair and deceptive acts and practices
UDID	unique device identifier
UNHRC	United Nations Human Rights Council
UUID	unique user identifier
VPAA	Video Privacy Protection Act

