



IAPP
CIPP/USSM

Certified Information
Privacy Professional

**STUDY
GUIDE**

UNITED STATES EXAM

Includes interactive online learning environment and study tools:

2 custom practice exams

More than 100 electronic flashcards

Searchable key term glossary

MIKE CHAPPLE, PHD, CIPP/US
JOE SHELLEY, CIPP/US

 **SYBEX[®]**
A Wiley Brand

IAPP

CIPP/USSM

Certified Information Privacy Professional Study Guide

United States Exam



IAPP

CIPP/USSM

Certified Information Privacy Professional

Study Guide

United States Exam



Mike Chapple
Joe Shelley



Copyright © 2021 by John Wiley & Sons, Inc. All rights reserved.

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.

Published simultaneously in Canada and the United Kingdom.

ISBN: 978-1-119-75546-3

ISBN: 978-1-119-75761-0 (ebk.)

ISBN: 978-1-119-75551-7 (ebk.)

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning, or otherwise, except as permitted under Section 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, Inc., 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 750-4470, or on the web at www.copyright.com. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, or online at <http://www.wiley.com/go/permission>.

Limit of Liability/Disclaimer of Warranty: While the publisher and author have used their best efforts in preparing this book, they make no representations or warranties with respect to the accuracy or completeness of the contents of this book and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives or written sales materials. The advice and strategies contained herein may not be suitable for your situation. You should consult with a professional where appropriate. Neither the publisher nor author shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages.

For general information on our other products and services or for technical support, please contact our Customer Care Department within the United States at (800) 762-2974, outside the United States at (317) 572-3993 or fax (317) 572-4002.

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic formats. For more information about Wiley products, visit our web site at www.wiley.com.

Library of Congress Control Number: 2021937722

TRADEMARKS: WILEY and the Wiley logo are trademarks or registered trademarks of John Wiley & Sons, Inc. and/or its affiliates, in the United States and other countries, and may not be used without written permission. IAPP and CIPP/US are registered trademarks or service marks of The International Association of Privacy Professionals, Inc. All other trademarks are the property of their respective owners. John Wiley & Sons, Inc. is not associated with any product or vendor mentioned in this book.

Cover Image: © Getty Images Inc./Jeremy Woodhouse

Cover Design: Wiley

*To Matthew – I am so proud of everything you've become and can't wait to see
the difference you make in the world!*

—Mike

To Jessie—my best friend and the love of my life.

—Joe

Acknowledgments

Even though only the authors' names appear on the front cover, the production of a book is a collaborative effort involving a huge team. Wiley always brings a top-notch collection of professionals to the table, and that makes the work of authors so much easier.

In particular, we'd like to thank Jim Minatel, our acquisitions editor. Jim is a consummate professional, and it is an honor and a privilege to continue to work with him on yet another project. Here's to many more!

We also greatly appreciated the editing and production team for the book, including David Clark, our project editor, who brought years of experience and great talent to the project. Our technical editors, Joanna Grama and Marcos Vierya, provided indispensable insight and expertise. This book would not have been the same without their valuable contributions. Saravanan Dakshinamurthy, our production editor, guided us through layouts, formatting, and final cleanup to produce a great book. We would also like to thank the many behind-the-scenes contributors, including the graphics, production, and technical teams who make the book and companion materials into a finished product.

Our agent, Carole Jelen of Waterside Productions, continues to provide us with wonderful opportunities, advice, and assistance throughout our writing careers.

Finally, we would like to thank our families who supported us through the late evenings, busy weekends, and long hours that a book like this requires to write, edit, and get to press.

About the Authors

Mike Chapple, Ph.D., CIPP/US, is the author of the best-selling *CISSP (ISC)² Certified Information Systems Security Professional Official Study Guide* (Sybex, 9th edition, 2021) and the *CISSP (ISC)² Official Practice Tests* (Sybex 3rd edition, 2021). He is an information security professional with two decades of experience in higher education, the private sector, and government.

Mike currently serves as a teaching professor in the IT, Analytics, and Operations department at the University of Notre Dame's Mendoza College of Business, where he teaches undergraduate and graduate courses on cybersecurity, data management, and business analytics.

Before returning to Notre Dame, Mike served as executive vice president and chief information officer of the Brand Institute, a Miami-based marketing consultancy. Mike also spent four years in the information security research group at the National Security Agency and served as an active duty intelligence officer in the U.S. Air Force.

Mike is technical editor for *Information Security Magazine* and has written more than 25 books. He earned both his B.S. and Ph.D. degrees from Notre Dame in computer science and engineering. Mike also holds an M.S. in computer science from the University of Idaho and an MBA from Auburn University. Mike holds the Certified Information Privacy Professional/US (CIPP/US), Cybersecurity Analyst+ (CySA+), Security+, Certified Information Security Manager (CISM), Certified Cloud Security Professional (CCSP), and Certified Information Systems Security Professional (CISSP) certifications.

Learn more about Mike and his other security certification materials at his website, CertMike.com.

Joe Shelley, M.A., CIPP/US, is a leader in higher education information technologies. He is currently the vice president for Libraries and Information Technology at Hamilton College in New York. In his role, Joe oversees central IT infrastructure, enterprise systems, information security and privacy programs, IT risk management, business intelligence and analytics, institutional research and assessment, data governance, and overall technology strategy. Joe also directs the Library and Institutional Research. In addition to supporting the teaching and research mission of the college, the library provides education in information sciences, digital and information literacy, and information management.

Before joining Hamilton College, Joe served as the chief information officer at the University of Washington Bothell in the Seattle area. During his 12 years at UW Bothell, Joe was responsible for learning technologies, data centers, web development, enterprise applications, help desk services, administrative and academic computing, and multimedia production. He implemented the UW Bothell information security program, cloud computing strategy, and IT governance, and he developed new initiatives for supporting teaching and learning, faculty research, and e-learning.

Joe earned his bachelor's degree in interdisciplinary arts and sciences from the University of Washington and his master's degree in educational technology from Michigan State University. Joe has held certifications and certificates for CIPP/US, ITIL, project management, and Scrum.

About the Technical Editors

Joanna Lyn Grama, JD, CIPT is an associate vice president with Vantage Technology Consulting Group and has more than 20 years of experience with a strong focus in law, higher education, information security, and data privacy. A former member of the U.S. Department of Homeland Security's Data Privacy and Integrity Advisory Committee, Joanna is a frequent author and regular speaker on information security and privacy topics. She is also a board member for the Central Indiana chapter of the Information Systems Audit and Control Association (ISACA), and a member of the International Association for Privacy Professionals (IAPP), the American Bar Association, Section of Science and Technology Law (Information Security Committee), and the Indiana State Bar Association (Written Publications Committee). She has earned the CISSP, CIPT, CDPSE, CRISC, and GSTRT certifications. Joanna graduated from the University of Illinois College of Law with honors.

Marcos Vieyra is the associate vice president and chief information security officer for the University of South Carolina, where he leads the information security, privacy, and digital accessibility programs and is a trusted adviser to the CIO and other university executives.

Prior to returning to the University of South Carolina, Marcos served as the CISO-in-residence for the SANS Technology Institute, and before that served as the chief information security officer for the state of South Carolina.

Marcos began his IT career in 1995, where he served as his squadron's system administrator in the U.S. Air Force, and learned the importance of operational security. Marcos's full-time information security and privacy career started at the University of South Carolina in 2004, where he also eventually earned his Bachelor of Arts degree in philosophy. Marcos has earned and maintains current the following information security and privacy certifications: GSTRT, CISSP, CIPP/IT, CIPP/US, CIPM. He is a member of the IAPP Fellow of Information Privacy (FIP) inaugural class.

When Marcos isn't working, he can be found spending time with his wife Michelle, usually doing something outdoors, with animals, watching movies, or some combination of those activities.

Contents at a Glance

<i>Introduction</i>		<i>xxi</i>
<i>Assessment Test</i>		<i>xxx</i>
Chapter 1	Privacy in the Modern Era	1
Chapter 2	Legal Environment	31
Chapter 3	Regulatory Enforcement	53
Chapter 4	Information Management	73
Chapter 5	Private Sector Data Collection	101
Chapter 6	Government and Court Access to Private Sector Information	147
Chapter 7	Workplace Privacy	175
Chapter 8	State Privacy Laws	199
Chapter 9	International Privacy Regulation	223
Appendix	Answers to Review Questions	241
<i>Index</i>		259

Contents

Introduction *xxi*

Assessment Test *xxx*

Chapter 1	Privacy in the Modern Era	1
	Introduction to Privacy	2
	What Is Privacy?	3
	What Is Personal Information?	4
	What Isn't Personal Information?	5
	Why Should We Care About Privacy?	7
	Generally Accepted Privacy Principles	8
	Management	9
	Notice	10
	Choice and Consent	10
	Collection	10
	Use, Retention, and Disposal	11
	Access	11
	Disclosure to Third Parties	12
	Security for Privacy	13
	Quality	14
	Monitoring and Enforcement	14
	Developing a Privacy Program	15
	Crafting Strategy, Goals, and Objectives	15
	Appointing a Privacy Official	17
	Privacy Roles	18
	Building Inventories	18
	Conducting a Privacy Assessment	19
	Implementing Privacy Controls	20
	Ongoing Operation and Monitoring	20
	Online Privacy	21
	Privacy Notices	21
	Privacy and Cybersecurity	22
	Cybersecurity Goals	23
	Relationship Between Privacy and Cybersecurity	24
	Privacy by Design	25
	Summary	26
	Exam Essentials	26
	Review Questions	27

Chapter 2	Legal Environment	31
	Branches of Government	32
	Legislative Branch	32
	Executive Branch	33
	Judicial Branch	34
	Understanding Laws	36
	Sources of Law	36
	Analyzing a Law	41
	Legal Concepts	43
	Legal Liability	44
	Torts and Negligence	45
	Summary	46
	Exam Essentials	46
	Review Questions	48
Chapter 3	Regulatory Enforcement	53
	Federal Regulatory Authorities	54
	Federal Trade Commission	54
	Federal Communications Commission	60
	Department of Commerce	61
	Department of Health and Human Services	61
	Banking Regulators	62
	Department of Education	63
	State Regulatory Authorities	63
	Self-Regulatory Programs	64
	Payment Card Industry	64
	Advertising	65
	Trust Marks	66
	Safe Harbors	67
	Summary	67
	Exam Essentials	68
	Review Questions	69
Chapter 4	Information Management	73
	Data Governance	74
	Building a Data Inventory	74
	Data Classification	75
	Data Flow Mapping	77
	Data Lifecycle Management	78
	Workforce Training	79
	Cybersecurity Threats	80
	Threat Actors	80
	Incident Response	85
	Phases of Incident Response	86
	Preparation	87

	Detection and Analysis	87
	Containment, Eradication, and Recovery	88
	Post-incident Activity	88
	Building an Incident Response Plan	90
	Data Breach Notification	92
	Vendor Management	93
	Summary	94
	Exam Essentials	94
	Review Questions	96
Chapter 5	Private Sector Data Collection	101
	FTC Privacy Protection	103
	General FTC Privacy Protection	103
	The Children's Online Privacy Protection Act (COPPA)	104
	Future of Federal Enforcement	107
	Medical Privacy	110
	The Health Insurance Portability and Accountability Act (HIPAA)	110
	The Health Information Technology for Economic and Clinical Health Act	118
	The 21st Century Cures Act	120
	Confidentiality of Substance Use Disorder Patient Records Rule	120
	Financial Privacy	121
	Privacy in Credit Reporting	121
	Gramm–Leach–Bliley Act (GLBA)	125
	Red Flags Rule	128
	Consumer Financial Protection Bureau	129
	Educational Privacy	130
	Family Educational Rights and Privacy Act (FERPA)	130
	Telecommunications and Marketing Privacy	132
	Telephone Consumer Protection Act (TCPA) and Telemarketing Sales Rule (TSR)	132
	The Junk Fax Prevention Act (JFPA)	135
	Controlling the Assault of Non-solicited Pornography and Marketing (CAN-SPAM) Act	135
	Telecommunications Act and Customer Proprietary Network Information	137
	Cable Communications Policy Act	138
	Video Privacy Protection Act (VPPA) of 1988	139
	Summary	140
	Exam Essentials	141
	Review Questions	143

Chapter 6	Government and Court Access to Private Sector Information	147
	Law Enforcement and Privacy	148
	Access to Financial Data	149
	Access to Communications	153
	National Security and Privacy	157
	Foreign Intelligence Surveillance Act (FISA) of 1978	157
	USA-PATRIOT Act	159
	The USA Freedom Act of 2015	162
	The Cybersecurity Information Sharing Act of 2015	163
	Civil Litigation and Privacy	164
	Compelled Disclosure of Media Information	164
	Electronic Discovery	166
	Summary	168
	Exam Essentials	168
	Review Questions	170
Chapter 7	Workplace Privacy	175
	Introduction to Workplace Privacy	176
	Workplace Privacy Concepts	176
	U.S. Agencies Regulating Workplace Privacy Issues	177
	U.S. Antidiscrimination Laws	178
	Privacy Before, During, and After Employment	181
	Employee Background Screening	182
	Employee Monitoring	185
	Investigation of Employee Misconduct	189
	Termination of the Employment Relationship	191
	Summary	193
	Exam Essentials	193
	Review Questions	195
Chapter 8	State Privacy Laws	199
	Federal vs. State Authority	200
	Financial Data	200
	Credit History	201
	California Financial Information Privacy Act	201
	Data Security	202
	Recent Developments	204
	Data Breach Notification Laws	212
	Elements of State Data Breach Notification Laws	212
	Key Differences Among States Today	214
	Recent Developments	215
	Marketing Laws	216
	Summary	217

	Exam Essentials	218
	Review Questions	219
Chapter 9	International Privacy Regulation	223
	International Data Transfers	224
	European Union General Data Protection Regulation	225
	Adequacy Decisions	228
	U.S.-EU Safe Harbor and Privacy Shield	228
	Binding Corporate Rules	230
	Standard Contractual Clauses	230
	Other Approved Transfer Mechanisms	231
	APEC Privacy Framework	231
	Cross-Border Enforcement Issues	233
	Global Privacy Enforcement Network	233
	Resolving Multinational Compliance Conflicts	234
	Summary	234
	Exam Essentials	235
	Review Questions	236
Appendix	Answers to Review Questions	241
	Chapter 1: Privacy in the Modern Era	242
	Chapter 2: Legal Environment	243
	Chapter 3: Regulatory Enforcement	245
	Chapter 4: Information Management	247
	Chapter 5: Private Sector Data Collection	249
	Chapter 6: Government and Court Access to Private Sector Information	251
	Chapter 7: Workplace Privacy	252
	Chapter 8: State Privacy Laws	254
	Chapter 9: International Privacy Regulation	256
	<i>Index</i>	259

Introduction

If you're preparing to take the Certified Information Privacy Professional/US (CIPP/US) exam, you'll undoubtedly want to find as much information as you can about privacy. The more information you have at your disposal and the more hands-on experience you gain, the better off you'll be when attempting the exam. We wrote this study guide with that in mind. The goal was to provide enough information to prepare you for the test—but not so much that you'll be overloaded with information that's outside the scope of the exam.

We've included review questions at the end of each chapter to give you a taste of what it's like to take the exam. If you're already working in the privacy field, we recommend that you check out these questions first to gauge your level of expertise. You can then use the book mainly to fill in the gaps in your current knowledge. This study guide will help you round out your knowledge base before tackling the exam.

If you can answer 90 percent or more of the review questions correctly for a given chapter, you can feel safe moving on to the next chapter. If you're unable to answer that many correctly, reread the chapter and try the questions again. Your score should improve.



Don't just study the questions and answers! The questions on the actual exam will be different from the practice questions included in this book. The exam is designed to test your knowledge of a concept or objective, so use this book to learn the objectives behind the questions.

The CIPP/US Exam

The CIPP/US certification is designed to be the gold standard credential for privacy professionals working in the United States and those seeking to enter the field. It is offered by the International Association of Privacy Professionals (IAPP) and fits into their suite of geographic-based privacy certifications.

The exam covers five major domains of privacy knowledge:

1. Introduction to the U.S. Privacy Environment
2. Limits on Private- Sector Collection and Use of Data
3. Government and Court Access to Private- Sector Information
4. Workplace Privacy
5. State Privacy Laws

These five areas include a range of topics, from building a privacy program to understanding U.S. privacy laws and regulations. You'll find that the exam focuses heavily on scenario-based learning. For this reason, you may find the exam easier if you have some real-world privacy experience, although many individuals pass the exam before moving into their first privacy role.

The CIPP/US exam consists of 90 multiple-choice questions administered during a 150-minute exam period. Each of the exam questions has four possible answer options. Exams are scored on a scale ranging from 100 to 500, with a minimum passing score of 300. Every exam item is weighted equally, but the passing score is determined using a secret formula, so you won't know exactly what percentage of questions you need to answer correctly to pass.

Exam Tip

There is no penalty for answering questions incorrectly. A blank answer and an incorrect answer have equal weight. Therefore, you should fill in an answer for every question, even if it is a complete guess!

IAPP charges \$550 for your first attempt at the CIPP/US exam and then \$375 for retake attempts if you do not pass on the first try. More details about the CIPP/US exam and how to take it can be found in the IAPP Candidate Certification Handbook at iapp.org/certify/candidate-handbook.

You should also know that certification exams are notorious for including vague questions. You might see a question for which two of the possible four answers are correct—but you can choose only one. Use your knowledge, logic, and intuition to choose the best answer and then move on. Sometimes, the questions are worded in ways that would make English majors cringe—a typo here, an incorrect verb there. Don't let this frustrate you; answer the question and move on to the next one.



Certification providers often use a process called *item seeding*, which is the practice of including unscored questions on exams. They do this as part of the process of developing new versions of the exam. So, if you come across a question that does not appear to map to any of the exam objectives—or for that matter, does not appear to belong in the exam—it is likely a seeded question. You never really know whether or not a question is seeded, however, so always make your best effort to answer every question.

Taking the Exam

Once you are fully prepared to take the exam, you can visit the IAPP website to purchase your exam voucher:

iapp.org/store/certifications

IAPP partners with Pearson VUE's testing centers, so your next step will be to locate a testing center near you. In the United States, you can do this based on your address or your ZIP code, while non-U.S. test takers may find it easier to enter their city and country. You can search for a test center near you at the Pearson Vue website, where you will need to navigate to "Find a test center."

www.pearsonvue.com/iapp

In addition to the live testing centers, you may also choose to take the exam at your home or office through Pearson VUE's OnVUE service. More information about this program is available here:

home.pearsonvue.com/Test-takers/OnVUE-online-proctoring.aspx

Now that you know where you'd like to take the exam, simply set up a Pearson VUE testing account and schedule an exam. One important note: Once you purchase your exam on the IAPP website, you have one year to register for and take the exam before your registration will expire. Be sure not to miss that deadline!

On the day of the test, take two forms of identification, and make sure to show up with plenty of time before the exam starts. Remember that you will not be able to take your notes, electronic devices (including smartphones and watches), or other materials into the exam with you.



Exam policies can change from time to time. We highly recommend that you check both the IAPP and Pearson VUE sites for the most up-to-date information when you begin your preparing, when you register, and again a few days before your scheduled exam date.

After the CIPP/US Exam

Once you have taken the exam, you will be notified of your score immediately, so you'll know if you passed the test right away. You should keep track of your score report with your exam registration records and the email address you used to register for the exam.

Maintaining Your Certification

IAPP certifications must be renewed periodically. To renew your certification, you either must maintain a paid IAPP membership or pay a \$250 non-member renewal fee. You must also demonstrate that you have successfully completed 20 hours of continuing professional education (CPE).

IAPP provides information on the CPE process via their website:

iapp.org/certify/cpe

Study Guide Elements

This study guide uses a number of common elements to help you prepare. These include the following:

Summaries The summary section of each chapter briefly explains the chapter, allowing you to easily understand what it covers.

Exam Essentials The exam essentials focus on major exam topics and critical knowledge that you should take into the test. The exam essentials focus on the exam objectives provided by IAPP.

Chapter Review Questions A set of questions at the end of each chapter will help you assess your knowledge and if you are ready to take the exam based on your knowledge of that chapter's topics.

Additional Study Tools

This book comes with a number of additional study tools to help you prepare for the exam. They include the following.



Go to www.wiley.com/go/sybextestprep, register your book to receive your unique PIN, and then once you have the PIN, return to www.wiley.com/go/sybextestprep and register a new account or add this book to an existing account.

Sybex Online Learning Environment

Sybex's online learning environment lets you prepare with electronic test versions of the review questions from each chapter and the practice exams that are included in this book. You can build and take tests on specific domains, by chapter, or cover the entire set of CIPP/US exam objectives using randomized tests.

Electronic Flashcards

Our electronic flashcards are designed to help you prepare for the exam. Over 100 flashcards will ensure that you know critical terms and concepts.

Glossary of Terms

Sybex provides a full glossary of terms in PDF format, allowing quick searches and easy reference to materials in this book.

Practice Exams

In addition to the practice questions for each chapter, this book includes access to two full 90-question online practice exams. We recommend that you use them both to test your preparedness for the certification exam.



Several months after publication of this book, slight changes were made to the exam objectives. You can download an update to this Study Guide, covering those changes, at <https://www.wiley.com/go/iappcippstudyguide>

CIPP/US Exam Objectives

IAPP goes to great lengths to ensure that its certification programs accurately reflect the privacy profession's best practices. They also publish ranges for the number of questions on the exam that will come from each domain. The following table lists the five CIPP/US domains and the extent to which they are represented on the exam.

Domain	Questions
1. Introduction to the U.S. Privacy Environment	28–34
2. Limits on Private- Sector Data Collection	20–24
3. Government and Court Access to Private- Sector Information	6–8
4. Workplace Privacy	8–12
5. State Privacy Laws	5–7

CIPP/US Certification Exam Objective Map

OBJECTIVE	CHAPTER
I. Introduction to the U.S Privacy Environment	
I.A Structure of U.S. Law	Chapters 2 and 3
I.A.a Branches of government	Chapters 2
I.A.b Sources of law	Chapter 2
I.A.c Legal definitions	Chapter 2
I.A.d Regulatory authorities	Chapter 3
I.A.e Understanding laws	Chapter 2
I.B Enforcement of U.S. Privacy and Security Laws	Chapters 2, 3, and 9
I.B.a Criminal versus civil liability	Chapters 2
I.B.b General theories of legal liability	Chapter 2
I.B.c Negligence	Chapter 2
I.B.d Unfair and deceptive trade practices (UDTP)	Chapter 3
I.B.e Federal enforcement actions	Chapter 3

OBJECTIVE	CHAPTER
I.B.f State enforcement (Attorneys General (AGs), etc.)	Chapter 3
I.B.g Cross-border enforcement issues (Global Privacy Enforcement Network (GPEN))	Chapter 9
I.B.h Self-regulatory enforcement (PCI, Trust Marks)	Chapter 3
I.C Information Management from a U.S. Perspective	Chapter 1, 4, and 9
I.C.a Data sharing and transfers	Chapter 1
I.C.b Privacy program development	Chapter 1
I.C.c Managing user preferences	Chapter 1
I.C.d Incident response programs	Chapter 4
I.C.e Workforce training	Chapter 4
I.C.f Accountability	Chapter 1
I.C.g Data retention and disposal (FACTA)	Chapter 4
I.C.h Online privacy	Chapter 1
I.C.i Privacy notices	Chapter 1
I.C.j Vendor management	Chapter 4
I.C.k International data transfers	Chapter 9
I.C.l Other key considerations for U.S.-based global multinational companies	Chapter 9
I.C.m Resolving multinational compliance conflicts	Chapter 9
II. Limits on Private- Sector Collection and Use of Data	
II.A Cross- Sector FTC Privacy Protection	Chapter 5
II.A.a The Federal Trade Commission Act	Chapter 5
II.A.b FTC Privacy Enforcement Actions	Chapter 5
II.A.c FTC Security Enforcement Actions	Chapter 5
II.A.d The Children's Online Privacy Protection Act	Chapter 5
II.A.e Future of federal enforcement (Data brokers, Big Data, IoT, AI, unregulated data)	Chapter 5

OBJECTIVE	CHAPTER
II.B Medical	Chapter 5
II.B.a The Health Insurance Portability and Accountability Act of 1996 (HIPAA)	Chapter 5
II.B.b Health Information Technology for Economic and Clinical Health (HITECH) Act of 2000	Chapter 5
II.B.c The 21st Century Cures Act of 2016	Chapter 5
II.B.d Confidentiality of Substance Use Disorder Patient Records Rule	Chapter 5
II.C Financial	Chapter 5
II.C.a The Fair Credit Reporting Act (FCRA) of 1970	Chapter 5
II.C.b The Fair and Accurate Credit Transactions Act (FACTA) of 2003	Chapter 5
II.C.c The Financial Services Modernization Act of 1999 (“Gramm-Leach-Bliley” or GLBA)	Chapter 5
II.C.d Red Flags Rule	Chapter 5
II.C.e Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010	Chapter 5
II.C.f Consumer Financial Protection Bureau	Chapter 5
II.C.g Online banking	Chapter 5
II.D Education	Chapter 5
II.D.a Family Educational Rights and Privacy Act (FERPA) of 1974	Chapter 5
II.D.b Education technology	Chapter 5
II.E Telecommunications and Marketing	Chapter 5
II.E.a Telemarketing sales rule (TSR) and the Telephone Consumer Protection Act of 1991 (TCPA)	Chapter 5
II.E.b Combating the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN SPAM)	Chapter 5
II.E.c The Junk Fax Prevention Act (JPFA) of 2005	Chapter 5
II.E.d The Wireless Domain Registry	Chapter 5
II.E.e Telecommunications Act of 1996 and Customer Proprietary Network Information	Chapter 5
II.E.f Cable Communications Privacy Act of 1984	Chapter 5

OBJECTIVE	CHAPTER
II.E.g Video Privacy Protection Act (VPPA) of 1988	Chapter 5
II.E.h Digital advertising	Chapter 5
III. Government and Court Access to Private-Sector Information	
III.A Law Enforcement and Privacy	Chapter 6
III.A.a Access to financial data	Chapter 6
III.A.b Access to communications	Chapter 6
III.A.c The Communications Assistance to Law Enforcement Act (CALEA)	Chapter 6
III.B National Security and Privacy	Chapter 6
III.B.a Foreign Intelligence Surveillance Act (FISA) of 1978	Chapter 6
III.B.b Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA-Patriot Act) of 2001	Chapter 6
III.B.c The USA Freedom Act of 2015	Chapter 6
III.B.d The Cybersecurity Information Sharing Act (CISA) of 2015	Chapter 6
III.C Civil Litigation and Privacy	Chapter 6
III.C.a Compelled disclosure of media information	Chapter 6
III.C.b Electronic discovery	Chapter 6
IV. Workplace Privacy	
IV.A Introduction to Workplace Privacy	Chapter 7
IV.A.a Workplace privacy concepts	Chapter 7
IV.A.b U.S. agencies regulating workplace privacy issues	Chapter 7
IV.A.c U.S. Anti-discrimination laws	Chapter 7
IV.B Privacy before, during, and after employment	Chapter 7
IV.B.a Employee background screening	Chapter 7
IV.B.b Employee monitoring	Chapter 7
IV.B.c Investigation of employee misconduct	Chapter 7
IV.B.d Termination of the employment relationship	Chapter 7