INFORMATION SYSTEMS SECURITY & ASSURANCE SERIES

ISSA

Legal and Privacy Issues in Information Security

THIRD EDITION

Joanna Lyn Grama

JONES & BARTLETT
LEARNING

World Headquarters
Jones & Bartlett Learning
5 Wall Street
Burlington, MA 01803
978-443-5000
info@jblearning.com
www.jblearning.com

Jones & Bartlett Learning books and products are available through most bookstores and online booksellers. To contact Jones & Bartlett Learning directly, call 800-832-0034, fax 978-443-8000, or visit our website, www.jblearning.com.

Substantial discounts on bulk quantities of Jones & Bartlett Learning publications are available to corporations, professional associations, and other qualified organizations. For details and specific discount information, contact the special sales department at Jones & Bartlett Learning via the above contact information or send an email to specialsales@jblearning.com.

Production Credits

Director of Product Management: Laura Pagluica
Product Manager: Edward Hinman
Content Strategist: Melissa Duffy
Content Coordinator: Paula-Yuan Gregory
Manager, Project Management: Jessica deMartin
Project Specialist: Roberta Sherman
Digital Project Specialist: Rachel DiMaggio
Marketing Manager: Michael Sullivan
Product Fulfillment Manager: Wendy Kilborn
Composition: S4Carlisle Publishing Services
Project Management: S4Carlisle Publishing Services
Cover Design: Kristin E. Parker
Media Development Editor: Faith Brosnan
Rights Specialist: James Fortney
Cover Image: © mirjanajovic/DigitalVision Vectors/Getty Images
Printing and Binding: LSC Communications

Library of Congress Cataloging-in-Publication Data

Names: Grama, Joanna Lyn, author.
Title: Legal and privacy issues in information security / Joanna Lyn Grama.
Other titles: Legal issues in information security
Description: Third edition. | Burlington, Massachusetts : Jones & Bartlett Learning, [2022] | Includes bibliographical references and index.
Identifiers: LCCN 2020028528 | ISBN 9781284207804 (paperback)
Subjects: LCSH: Information storage and retrieval systems--Law and legislation--United States. | Data protection--Law and legislation--United States. | Information storage and retrieval systems--Security measures--Law and legislation--United States.
Classification: LCC KF1263.C65 G73 2022 | DDC 342.7308/58--dc23
LC record available at https://lccn.loc.gov/2020028528

6048

Printed in the United States of America

24 23 22 21 20 10 9 8 7 6 5 4 3 2 1

Contents

To my son, A.J., and my husband, Ananth

Preface

Purpose of This Book

This book is part of the Information Systems Security & Assurance Series from Jones & Bartlett Learning (www.jblearning.com). Designed for courses and curriculums in Information Technology (IT) Security, Cybersecurity, Information Assurance, and Information Systems Security, this series features a comprehensive, consistent treatment of the most current thinking and trends in this critical subject area. These titles deliver fundamental information-security principles packed with real-world applications and examples. Authored by Certified Information Systems Security Professionals (CISSPs), they deliver comprehensive information on all aspects of information security. Reviewed word for word by leading technical experts in the field, these books are not just current, but forward-thinking—putting you in the position to solve the cybersecurity challenges not just of today, but of tomorrow as well.

This book discusses information security, privacy, and the law. Information security is the practice of protecting information to ensure the goals of confidentiality, integrity, and availability. Information security makes sure that accurate information is available to authorized individuals when it is needed. Governments, private organizations, and individuals all use information security to protect information. Sometimes these organizations do a very good job of protecting information. Sometimes they do not.

When governments, private organizations, and individuals do a poor job of protecting the information entrusted to them, legislatures respond with new laws that require a more structured approach to information security. The U.S. federal government has enacted several laws that focus on protecting different types of information. This third edition takes into account the changing legal and regulatory landscape, and growth in privacy concerns, since this book was first published. Finding out which law applies to a particular situation, or type of data, or how best to think about privacy issues related to specific situations or data, is often confusing.

This book tries to help eliminate that confusion. Part One of the book discusses common concepts in information security, privacy, and the law. These concepts are used throughout the book. Part Two discusses the federal and state laws and legal concepts that affect how governments and organizations think about information security. This part uses laws and case studies to help explain these concepts. A quick-reference list of the federal laws and cases that are discussed in the book is included at the end of the book. Finally, Part Three focuses on how to create an information security program that addresses the laws and compliance requirements discussed throughout the book.

Learning Features

The writing style of this book is practical and conversational. Step-by-step examples of information security concepts and procedures are presented throughout the text. Each chapter begins with a statement of learning objectives. Illustrations are used both to clarify the material and to vary the presentation. The text is sprinkled with Notes, Tips, FYIs, Warnings, and Sidebars to alert the reader to additional and helpful information related to the subject under discussion. Chapter Assessments appear at the end of each chapter, with solutions provided in the back of the book.

Chapter summaries are included in the text to provide a rapid review or preview of the material and to help students understand the relative importance of the concepts presented.

Audience

The material is suitable for undergraduate or graduate computer science majors or information science majors, students at a 2-year technical college or community college who have a basic technical background, or readers who have a basic understanding of IT security and want to expand their knowledge.

New to This Edition

The text has been updated to address major legal developments since 2015 impacting the practice of information security and privacy, including revised case examples and references to illustrate concepts explained in the text. It has also updated endnotes and references for students who wish to learn more about concepts explained in the book.

Theory Labs

This text is accompanied by Cybersecurity Theory Labs. These hands-on labs provide guided exercises and case studies where students can learn and practice foundational cybersecurity skills as an extension of the lessons in this textbook. For more information or to purchase the labs, visit go.jblearning.com/grama3e.

Acknowledgments

The third time is the charm, as they say! Many talented people worked long hours to make the third edition of this book a reality, and they all have my sincere appreciation. I wish to thank Jones & Bartlett Learning for inviting me back to work on this edition. The competence of the Jones & Bartlett team makes revision work so much easier. Carole Jelen, my literary agent, continues to earn my gratitude for answering my endless questions with grace and good humor.

I am fortunate to have the support of friends and family members in all that I do. I would especially like to thank my friends and colleagues at Vantage Technology Consulting Group for encouraging me when the "writing times" were tough. In addition, the cheer, advice, subject matter review, and emergency cookie packages from friends Cathy Bates, Faith Graham, Pam Hermes, Amy Keene, Kim Lindros, Kim Milford, Matt Morton, Tim O'Brien, Patricia Rosen, David Seidl, Valerie Vogel, and Jon Young were invaluable. You all are the best and I am grateful for your friendship.

Finally, my husband, Ananth, and son, A.J., deserve special thanks for their tireless support. I am a very lucky person. My love, always, to you both.

About the Author

Joanna Lyn Grama (JD, CISSP, CIPT, CRISC) is an associate vice president at Vantage Technology Consulting Group. She has more than 20 years of experience in higher education with a strong focus on law, IT security policy, compliance, governance, and data privacy issues.

Grama is a former member of the U.S. Department of Homeland Security's Data Privacy and Integrity Advisory Committee (appointed to the Committee by Secretary Janet Napolitano) and served as the chairperson of its technology subcommittee. Grama is also vice president of the board of directors for the central Indiana Information Systems Audit and Control Association (ISACA) chapter; 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. She is a frequent speaker on a variety of IT security topics, including identity theft, personal information security, and university security and privacy compliance issues.