

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.

Copyright © 2022 by Jones & Bartlett Learning, LLC, an Ascend Learning Company

All rights reserved. No part of the material protected by this copyright may be reproduced or utilized in any form, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without written permission from the copyright owner.

The content, statements, views, and opinions herein are the sole expression of the respective authors and not that of Jones & Bartlett Learning, LLC. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not constitute or imply its endorsement or recommendation by Jones & Bartlett Learning, LLC and such reference shall not be used for advertising or product endorsement purposes. All trademarks displayed are the trademarks of the parties noted herein. *Legal and Privacy Issues in Information Security, Third Edition* is an independent publication and has not been authorized, sponsored, or otherwise approved by the owners of the trademarks or service marks referenced in this product.

There may be images in this book that feature models; these models do not necessarily endorse, represent, or participate in the activities represented in the images. Any screenshots in this product are for educational and instructive purposes only. Any individuals and scenarios featured in the case studies throughout this product may be real or fictitious, but are used for instructional purposes only.

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

© Jones & Bartlett Learning, LLC. NOT FOR SALE OR DISTRIBUTION.

Contents

Preface	xix
Acknowledgments	xxi
About the Author	xxiii

PART I **Fundamental Concepts** **1**

CHAPTER 1

Information Security Overview	3
Why Is Information Security an Issue?	4
What Is Information Security?	5
What Is Confidentiality?	6
What Is Integrity?	7
What Is Availability?	8
Basic Information Security Concepts	10
Vulnerabilities	10
Threats	12
Risks	14
Safeguards	15
Choosing Safeguards	18
What Are Common Information Security Concerns?	18
Shoulder Surfing	18
Social Engineering	19
Phishing and Targeted Phishing Scams	19
Malware	20
Spyware and Keystroke Loggers	21
Logic Bombs	21
Backdoors	22
Denial of Service Attacks	22
What Are the Mechanisms That Ensure Information Security?	23
Laws and Legal Duties	23
Contracts	23
Organizational Governance	24
<i>Data Protection Models</i>	<i>24</i>

U.S. National Security Information 25

Voluntary Organizations 26

Do Special Kinds of Data Require Special Kinds of Protection? 26

CHAPTER SUMMARY 27

KEY CONCEPTS AND TERMS 28

CHAPTER 1 ASSESSMENT 28

ENDNOTES 29

CHAPTER 2

Privacy Overview 31

Why Is Privacy an Issue? 32

What Is Privacy? 33

Types of Personal Information 34

How Is Privacy Different from Information Security? 35

What Are the Sources of Privacy Law? 36

Constitutional Law 36

Federal Law 38

Freedom of Information Act (1966) 38

Privacy Act (1974) 39

E-Government Act (2002) 39

Electronic Communications Privacy Act (1986) 39

The Wiretap Act (1968, amended) 39

Census Confidentiality (1952) 39

Mail Privacy Statute (1971) 40

Cable Communications Policy Act (1984) 40

Driver's Privacy Protection Act (1994) 40

State Laws 40

Common Law 41

Intrusion Into Seclusion 41

Portrayal in a False Light 42

Appropriation of Likeness or Identity 42

Public Disclosure of Private Facts 42

Voluntary Agreements 43

What Are Threats to Personal Data Privacy in the Information Age? 44

Technology-Based Privacy Concerns 44

Spyware 44

Cookies, Web Beacons, and Clickstreams 45

Wireless Technologies 47

GPS Technology 48

Security Breaches 48

People-Based Privacy Concerns 49

Social Networking Sites 50

Online Data Gathering 51

What Is Workplace Privacy? 51

Telephone, Voicemail, and Email Monitoring 52

Telephone and Voicemail Monitoring 52

Email Monitoring 53

Computer Use Monitoring 54

Off-Duty Computer Monitoring 55

Video Surveillance Monitoring 55

Special Rules for Public Employees 56

What Are General Principles for Privacy Protection in Information Systems? 57

Privacy Policies 58

International Privacy Laws 59

CHAPTER SUMMARY 59

KEY CONCEPTS AND TERMS 60

CHAPTER 2 ASSESSMENT 60

ENDNOTES 61

CHAPTER 3

The American Legal System 63

The American Legal System 64

Federal Government 64

Legislative Branch 65

Executive Branch 67

Judicial Branch 67

State Government 70

Sources of American Law 73

Common Law 73

Code Law 74

Constitutional Law 74

How Does It All Fit Together? 74

Types of Law 75

Civil 75

Criminal 76

Administrative 77

The Role of Precedent 78

Regulatory Authorities 79

What Is the Difference Between Compliance and Audit? 80

How Do Security, Privacy, and Compliance Fit Together? 81

CHAPTER SUMMARY 82

KEY CONCEPTS AND TERMS 82

CHAPTER 3 ASSESSMENT 83

ENDNOTES 84

PART II Laws Influencing Information Security 85

CHAPTER 4	Security and Privacy of Consumer Financial Information	87
	Business Challenges Facing Financial Institutions	88
	The Different Types of Financial Institutions	89
	Consumer Financial Information	90
	Who Regulates Financial Institutions?	90
	The Federal Reserve System	91
	Federal Deposit Insurance Corporation	92
	National Credit Union Administration	93
	Office of the Comptroller of the Currency	94
	Special Role of the Federal Financial Institutions Examination Council	95
	Special Roles of the Consumer Financial Protection Bureau and the Federal Trade Commission	96
	<i>Consumer Financial Protection Bureau</i>	96
	<i>Federal Trade Commission</i>	96
	The Gramm-Leach-Bliley Act	97
	Purpose, Scope, and Main Requirements	97
	The Privacy Rule	98
	The Safeguards Rule	99
	The Pretexting Rule	102
	Oversight	103
	Federal Trade Commission Red Flags Rule	103
	Purpose	103
	Scope	103
	Main Requirements	104
	Oversight	105
	Payment Card Industry Standards	106
	Purpose	107
	Scope	107
	Main Requirements	108
	Oversight	108
	Case Studies and Examples	109
	FTC Privacy and Safeguards Rule Enforcement	109
	Credit Card Security Example	110
	CHAPTER SUMMARY	111
	KEY CONCEPTS AND TERMS	111
	CHAPTER 4 ASSESSMENT	111
	ENDNOTES	112

CHAPTER 5**Security and Privacy of Information Belonging to Children and in Educational Records 115****Challenges in Protecting Children on the Internet 116**

Identification of Children	117
First Amendment and Censorship	118
Defining Obscenity	118

Children's Online Privacy Protection Act 119

Purpose of COPPA	119
Scope of the Regulation	120
Main Requirements	121
<i>Privacy Policy</i>	121
<i>Privacy Policy Content</i>	121
<i>Gaining Parental Consent</i>	122
Oversight	124

Children's Internet Protection Act 124

Purpose	124
Scope of the Regulation	125
Main Requirements	125
<i>Content Filtering</i>	125
<i>Internet Safety Policy</i>	127
<i>Exceptions</i>	127
Oversight	128

Family Educational Rights and Privacy Act (FERPA) 128

Scope	128
Main Requirements	129
<i>Annual Notification</i>	130
<i>Access to Education Records</i>	130
<i>Amendment of Education Records</i>	131
<i>Disclosure of Education Records</i>	131
Disclosure Exceptions Under FERPA	132
Security of Student Records Under FERPA	133
Oversight	133
State Laws Protecting Student Data	134

Case Studies and Examples 134

Children's Privacy	135
Release of Disciplinary Records	135

CHAPTER SUMMARY 136**KEY CONCEPTS AND TERMS 136****CHAPTER 5 ASSESSMENT 137****ENDNOTES 138**

CHAPTER 6

Security and Privacy of Health Information 139

Business Challenges Facing the Healthcare Industry 140

Why Is Healthcare Information So Sensitive? 141

The Health Insurance Portability and Accountability Act 143

Purpose 143

Scope 145

Main Requirements of the Privacy Rule 147

Required Disclosures 148

Permitted Uses and Disclosures 149

Uses and Disclosures That Require Authorization 154

Minimum Necessary Rule 155

Other Individual Rights Under the Privacy Rule 155

Privacy Notices 157

Administrative Requirements 159

Breach Notification Provisions 160

Main Requirements of the Security Rule 161

Safeguards and Implementation Specifications 162

Oversight 168

The Role of State Laws Protecting Medical Records 169

Case Studies and Examples 169

OCR Enforcement Information 169

HIPAA and Federal Trade Communications Act 169

CHAPTER SUMMARY 171

KEY CONCEPTS AND TERMS 171

CHAPTER 6 ASSESSMENT 171

ENDNOTES 172

CHAPTER 7

Corporate Information Security and Privacy Regulation 175

The Enron Scandal and Securities-Law Reform 176

Corporate Fraud at Enron 176

Why Is Accurate Financial Reporting Important? 179

The Sarbanes-Oxley Act of 2002 181

Purpose and Scope 182

Main Requirements 183

Public Company Accounting Oversight Board 183

Document Retention 185

Certification 187

Oversight 191

Compliance and Security Controls 192

COBIT 192

GAIT 192

ISO/IEC Standards 193

NIST Computer Security Guidance 194

SOX Influence in Other Types of Companies 194

Corporate Privacy Issues 195

Case Studies and Examples 196

CHAPTER SUMMARY 197

KEY CONCEPTS AND TERMS 197

CHAPTER 7 ASSESSMENT 197

ENDNOTES 198

CHAPTER 8

Federal Government Information Security and Privacy Regulations 201

Information Security Challenges Facing the Federal Government 202

The Federal Information Security Modernization Act 204

Purpose and Scope 204

Main Requirements 204

Agency Information Security Programs 204

The Role of NIST 207

Central Incident Response Center 211

National Security Systems 212

Oversight 213

Protecting Privacy in Federal Information Systems 214

The Privacy Act of 1974 214

The E-Government Act of 2002 215

OMB Breach Notification Policy 217

Import and Export Control Laws 218

Case Studies and Examples 219

CHAPTER SUMMARY 220

KEY CONCEPTS AND TERMS 221

CHAPTER 8 ASSESSMENT 221

ENDNOTES 222

CHAPTER 9

State Laws Protecting Citizen Information and Breach Notification Laws 225

History of State Actions to Protect Personal Information 226

ChoicePoint Data Breach 226

Breach Notification Regulations 227

California Breach Notification Act 228

Other Breach Notification Laws 230

Activities That Constitute a Breach 230

Time for Notification 230

Contents of Notification 231
Encryption Requirements 232
Penalties for Failure to Notify 232
Private Cause of Action 233

Data-Specific Security and Privacy Regulations 234

Minnesota and Nevada: Requiring Businesses to Comply With Payment Card Industry Standards 234
Indiana: Limiting SSN Use and Disclosure 236
California: Protecting Consumer Privacy 238

Encryption Regulations 239

Massachusetts: Protecting Personal Information 239
Nevada Law: Standards-Based Encryption 241

Data Disposal Regulations 242

Washington: Everyone Has an Obligation 242
New York: Any Physical Record 243

Case Studies and Examples 244

CHAPTER SUMMARY 245

KEY CONCEPTS AND TERMS 245

CHAPTER 9 ASSESSMENT 246

ENDNOTES 247

CHAPTER 10

Intellectual Property Law 249

The Digital Wild West and the Importance of Intellectual Property Law 250

Legal Ownership and the Importance of Protecting Intellectual Property 250

Patents 252

Patent Basics 253
Patent Requirements 253
The Patent Application Process 256
Infringement and Remedies 257
What Is the Difference Between Patents and Trade Secrets? 258

Trademarks 259

Trademark Basics 261
Use in Commerce 262
Distinctive 262
Trademark Registration 263
Infringement and Remedies 265
Relationship of Trademarks on Domain Names 266

Copyright 268

Copyright Basics 268
Copyright Registration 270
Infringement and Remedies 271
Fair Use 272

Protecting Copyrights Online—The Digital Millennium Copyright Act (DMCA) 274

DMCA Basics	274
<i>Technology Protection Measures</i>	274
<i>Online Copyright Infringement</i>	276
<i>Computer Maintenance</i>	277
DMCA Unintended Consequences	277
<i>Title I Concerns</i>	278
<i>Title II Concerns</i>	278

Case Studies and Examples 278

Trade Secrets	278
Service Provider Liability for Copyright Infringement	279
Digital Collections	280

CHAPTER SUMMARY 280

KEY CONCEPTS AND TERMS 281

CHAPTER 10 ASSESSMENT 281

ENDNOTES 282

CHAPTER 11

The Role of Contracts 285

General Contracting Principles 286

Contract Form	286
Capacity to Contract	287
Contract Legality	288
Form of Offer	288
Form of Acceptance	289
Meeting of the Minds	291
Consideration	291
Performance and Breach of Contract	292
Contract Repudiation	294

Contracting Online 295

Legal Capacity Online	297
Form of Offer and Acceptance	297
<i>Email Communications</i>	298
<i>Text and Instant Messages</i>	298
<i>Twitter and Other Social Networking Sites</i>	299
Existence and Enforcement	300
Authenticity and Nonrepudiation	300

Special Types of Contracts in Cyberspace 301

Shrinkwrap Contracts	303
Clickwrap Contracts	303
Browsewrap Contracts	305

How Do These Contracts Regulate Behavior? 306

Emerging Contract Law Issues 307

Cloud Computing	308
Information Security Terms in Contracts	309
<i>Data Definition and Use</i>	310
<i>General Data Protection Terms</i>	310
<i>Compliance With Legal and Regulatory Requirements</i>	311
Case Studies and Examples	312
Contract Formation via Email	312
CHAPTER SUMMARY	313
KEY CONCEPTS AND TERMS	313
CHAPTER 11 ASSESSMENT	314
ENDNOTES	315

CHAPTER 12

Criminal Law and Tort Law Issues in Cyberspace 317

General Criminal Law Concepts	318
Main Principles of Criminal Law	319
<i>Type of Wrongful Conduct</i>	319
<i>Elements of a Crime</i>	319
<i>Jurisdiction</i>	321
Criminal Procedure	323
Common Criminal Laws Used in Cyberspace	326
The Computer Fraud and Abuse Act (1984)	326
Computer Trespass or Intrusion	329
Theft of Information	329
Interception of Communications Laws	330
Spam and Phishing Laws	330
Cybersquatting	332
Malicious Acts	332
Well-Known Cybercrimes	333
General Tort Law Concepts	334
Strict Liability Torts	334
Negligence Torts	335
Intentional Torts	337
Civil Procedure	338
Common Tort Law Actions in Cyberspace	341
Defamation	341
Intentional Infliction of Emotional Distress	343
Trespass Torts	344
Privacy Violations	345
Case Studies and Examples	346
CAN-SPAM Act	346
Defamation on College Campuses	346
CHAPTER SUMMARY	347
KEY CONCEPTS AND TERMS	347

CHAPTER 12 ASSESSMENT 348

ENDNOTES 349

PART III Security and Privacy in Organizations 351

CHAPTER 13

Information Security Governance 353

What Is Information Security Governance? 354

Information Security Governance Planning 355

Common Information Security Governance Roles 356

Information Security Governance and Management 357

Information Security Governance in the Federal Government 358

Information Security Governance Documents 359

Policies 360

Standards 361

Procedures 361

Guidelines 362

Creating Information Security Policies 363

Policy Development Process 363

Recommended Information Security Policies 367

Acceptable Use Policies 368

AUP Terms 370

Enforcement 371

Anti-Harassment Policies 372

Workplace Privacy and Monitoring Policies 373

Data Retention and Destruction Policies 374

Data Retention Policies 375

Data Destruction Policies 376

Intellectual Property Policies 377

Authentication and Password Policies 377

Security Awareness and Training 379

Case Studies and Examples 380

Acceptable Use Case Study 380

CHAPTER SUMMARY 382

KEY CONCEPTS AND TERMS 382

CHAPTER 13 ASSESSMENT 383

ENDNOTES 384

CHAPTER 14

Risk Analysis, Incident Response, and Contingency Planning 387

Contingency Planning 388

Risk Management 389

Risk Assessment Process 390

- Risk Assessment Team* 391
- Identifying Assets, Vulnerabilities, and Threats* 392
- Likelihood and Potential Loss* 394
- Document Needed Controls* 398
- Risk Response 400
- Training Employees 401
- Continuous Monitoring 401
- Three Types of Contingency Planning 401**
- Incident Response Planning 402
 - Incident Response Team* 403
 - IR Plan Process* 404
- Disaster Recovery and Business Continuity Planning 407
 - DR/BC Team* 408
 - DR/BC Plan Development* 409
- Testing the Plan 412
- Special Considerations 414**
- Addressing Compliance Requirements 414
- When to Call the Police 415
- Public Relations 415
- CHAPTER SUMMARY 416**
- KEY CONCEPTS AND TERMS 416**
- CHAPTER 14 ASSESSMENT 417**
- ENDNOTES 418**

CHAPTER 15

- Computer Forensics and Investigations 419**
- What Is Computer Forensics? 420**
- What Is the Role of a Computer Forensic Examiner? 423**
- Collecting, Handling, and Using Digital Evidence 425**
- The Investigative Process 426
 - Identification* 426
 - Preservation* 426
 - Collection* 427
 - Examination* 429
 - Presentation* 430
- Ethical Principles for Forensic Examination 431
- Legal Issues Involving Digital Evidence 432**
- Authority to Collect Evidence 432
 - The Fourth Amendment and Search Warrants* 432
 - Federal Laws Regarding Electronic Data Collection* 435
- Admissibility of Evidence 439
 - The Hearsay Rule* 441
 - The Best Evidence Rule* 442

	CHAPTER SUMMARY	442
	KEY CONCEPTS AND TERMS	442
	CHAPTER 15 ASSESSMENT	443
	ENDNOTES	444
APPENDIX A	Answer Key	447
APPENDIX B	Standard Acronyms	451
APPENDIX C	Law and Case Citations	455
APPENDIX D	The Constitution of the United States of America	465
	Glossary of Key Terms	483
	References	495
	Index	513

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.

