

# Information Privacy Fundamentals for Librarians and Information Professionals



Cherie L. Givens

# Information Privacy Fundamentals for Librarians and Information Professionals

Cherie L. Givens

ROWMAN & LITTLEFIELD  
Lanham • Boulder • New York • London

Information Privacy Fundamentals for  
Librarians and Information  
Professionals

Published by Rowman & Littlefield  
A wholly owned subsidiary of The Rowman & Littlefield Publishing Group, Inc.  
4501 Forbes Boulevard, Suite 200, Lanham, Maryland 20706  
www.rowman.com

Unit A, Whitacre Mews, 26-34 Stannery Street, London SE11 4AB, United Kingdom


Copyright © 2015 by Cherie L. Givens

*All rights reserved.* No part of this book may be reproduced in any form or by any electronic or mechanical means, including information storage and retrieval systems, without written permission from the publisher, except by a reviewer who may quote passages in a review.

British Library Cataloguing in Publication Information Available

**Library of Congress Cataloging-in-Publication Data**

Givens, Cherie L., 1969-  
Information privacy fundamentals for librarians and information professionals / Cherie L. Givens.  
p. cm.  
Includes bibliographical references and index.  
ISBN 978-1-4422-4211-1 (cloth : alk. paper) — ISBN 978-1-4422-2881-8 (pbk. : alk. paper) —  
ISBN 978-1-4422-2882-5 (ebook)  
1. Records—Access control—United States. 2. Data protection—Law and legislation—United  
States. 3. Computer security—Law and legislation—United States. 4. Privacy. Right of—United  
States. 5. Library legislation—United States. 6. Information services—Law and legislation—United  
States. I. Title.  
KF1263.C65G58 2015  
025.5—dc23  
2014023397

™ The paper used in this publication meets the minimum requirements of American  
National Standard for Information Sciences Permanence of Paper for Printed Library  
Materials, ANSI/NISO Z39.48-1992.

Printed in the United States of America

This book is intended for informational purposes only. It should not be used as legal advice. Readers should consult an attorney for advice regarding specific legal questions and the laws that apply to their unique work environments. Privacy professionals should be consulted by those seeking assistance creating privacy policies, programs, and training as well as performing assessments and audits.

# Acknowledgments

This book would not have been possible without the encouragement, friendship, and assistance of many people. Special thanks are owed to Hank for his enduring support of this endeavor. I thank Eric Moskowitz and Bertha Ochoa for their assistance in editing and preparing this manuscript.

I owe special thanks to the International Association of Privacy Professionals and many of the members of this wonderful group for inspiring me to develop my expertise in the field of information privacy. I appreciate the supportive environment and many learning opportunities that have been made available to me through Privacy Summits, KnowledgeNets, and thoughtful conversations.

I am grateful to Mary Alice Baish, Superintendent of Documents, U.S. Government Printing Office, for providing me with the opportunity to develop privacy policies and procedures, serve as privacy point of contact, and address privacy matters for the Office of the Superintendent of Documents and the Library Services and Content Management business unit. My work at the U.S. Government Printing Office inspired this book.

Special thanks are owed to my editor, Charles Harmon, for suggesting that I write a book about information privacy, giving me the opportunity to do so, and shepherding me along the way. I thank everyone at Rowman & Littlefield who helped to bring this book to press.

# Preface

I wrote this book to help educate librarians and information science professionals about the fundamentals of information privacy. When I worked in library services and content management for the federal government, I had the opportunity to see firsthand that information privacy issues occur in the workplace and that those working in library and information positions can find themselves on the front lines, needing to be able to identify and address these issues. *Information Privacy Fundamentals for Librarians and Information Professionals* is designed to provide an introduction to information privacy laws and practices while incorporating practical privacy information for those who will need to identify and address privacy issues in the workplace.

As information science programs diversify, they provide a broader range of career paths and training for students who will work in increasingly diverse work environments. Many students will find employment outside of the traditional library and school environments. They may work in positions in government, businesses, and health care environments. It is crucial that those in the information professions understand what laws and regulations govern the handling of personally identifiable information (PII) in their work environments and be able to identify information privacy issues and address them.

It is my firm belief that if those of us working in the information professions do not fully embrace information privacy, others will decide our privacy policies and practices. We manage information. Personal data, also known as PII, is a form of information. Becoming proficient in applying the laws, regulations, and best practices for managing personal data is a necessary part of the educational process.

Information privacy is a growing and changing field. No one book can teach you everything you need to know. This book is designed to provide

readers with a foundation that reflects current law and practice on which to build their privacy knowledge. Laws change, practices change, and professionals must continue to educate themselves to keep abreast of those changes. Everyone needs to know how to protect personal data in their professional and personal lives.

It is presumed that this book will be read cover to cover or referred to by chapter for quick reviews. Read it completely for an understanding of the fundamentals of information privacy from a library and information science perspective. Use this book as a reference and consult relevant chapters for specific areas of interest. I have included references where needed to aid those who seek to use this book as a reference only. Some redundancy was necessary to allow for the use of this book as a chapter- and topic-specific reference.



# Table of Contents

Acknowledgments	xiii
Preface	xv
<b>1</b> Introduction to Information Privacy	1
Origins of Privacy Rights	2
U.S. Privacy Rights	2
Privacy and the U.S. Bill of Rights	2
The “Right to Privacy” Is Recognized	3
State Recognition of Privacy	3
Information Privacy Defined	4
Personal Information	4
Personal Data	5
Data Protection	5
Personally Identifiable Information	5
Sensitive Personal Data	5
Privacy Policy	5
Privacy Notice	6
The Development of Privacy Rights Globally	6
Technology Spurs the Creation of Fair Information Practice Principles	7
Protecting Information Privacy	8
U.S. Federal and State Privacy Laws	9
Federal Privacy Laws	9
State Privacy Laws	10
Privacy Education and Application	10
Privacy Literacy	10
Information Privacy in Libraries	10

Applying Information Privacy Knowledge	11
Notes	11
Bibliography	14
<b>2 Protecting Information Privacy: A Professional Imperative</b>	17
Protecting Privacy in Information Environments	17
Privacy and the Right to Receive Information	18
The Right to Receive Information in Libraries	20
Intellectual Privacy	20
Reader Privacy	22
Professional Importance of Protecting Information Privacy	23
Library Associations	24
Archivists Associations	25
Medical Informatics and Health Information Management Associations	25
Conclusion	26
Notes	27
Bibliography	29
<b>3 Major U.S. Privacy Protections: Laws, Regulators, and Approaches to Enforcement</b>	31
Introduction	31
Federal Agency Regulators	32
Trade and Marketing: The Federal Trade Commission	33
Commerce, Trade, and Business Development: The U.S. Department of Commerce	34
Finance: The Consumer Financial Protection Bureau, Federal Reserve Board, and Comptroller of Currency	35
Educational Records: The U.S. Department of Education	35
Privacy in the Workplace: Equal Employment Opportunity Commission	36
Approaches to the Enforcement of Privacy Rights	36
State Attorneys General and State Privacy Laws	36
Self-Regulation	37
Privacy Laws by Sector	37
Marketing and Telecommunications: TCPA, Do Not Call, CAN-SPAM	37
Protecting Children and Teens Online—COPPA	39
Education Records: Family Educational Rights and Privacy Act (FERPA) and the Protection of Pupil Rights Amendment (PPRA)	40
Financial Records: Gramm-Leach-Bliley Act, Fair Credit Reporting Act	41
Health Information: HIPAA, HITECH, and GINA	42

Government: FOIA, the Privacy Act, and the PATRIOT Act	43
The Privacy Act of 1974	43
The Freedom of Information Act	44
FISA, the PATRIOT Act, and NSLs: Terrorism	
Investigations That Impact Privacy and Protections	45
Costs Associated with Information Breach	46
Conclusion	46
Notes	47
Bibliography	50
<b>4 Privacy Literacy</b>	53
Digital Literacy	53
Information Literacy	54
Privacy Education for Online Users	55
Patrons	55
Youth	55
Employees	56
Information Gathering Online	57
Cookies and Web Beacons	57
Internet Protocol (IP) Addresses	58
Data Mining	58
Search Logs and Email Scanning	59
Social Media Posts	59
Online Gaming	60
Enhancing Privacy Online	60
Phishing and Passwords	61
Public Wi-Fi Hotspots	61
Spying and Webcam Safety	62
Adjusting Browser Privacy and Security Settings	63
Mobile Devices and Information Privacy	64
Keep Abreast of Changes	65
The Promise of Safer Web Surfing	65
Conclusion	65
Notes	66
Bibliography	68
<b>5 Information Privacy in Libraries</b>	71
Greater Anonymity	71
Protecting Privacy and Confidentiality on the Front Lines	72
Patron Awareness	73
The USA PATRIOT Act	74
Minimizing Data Collection and Retention	74
Data Collection	74
Observability	75

RFID Systems in Libraries	75
Learning from Privacy Practices of Small and Medium-Sized Businesses	76
The Role of Privacy Professionals	77
Locating and Examining Privacy Laws	78
Dedicating Time for Privacy Review and Training	78
Conclusion	79
Notes	79
Bibliography	80
<b>6 Privacy Policies and Programs</b>	<b>81</b>
Privacy Policies	82
Start with the Law	83
Track and Evaluate Data Collection, Use, and Risk	83
Perform a Privacy Audit or Assessment	84
Explain What You Collect and How You Use Personal Data	84
Collecting and Sharing Information: Cookie Use and Third Parties	84
Contact Information	85
Plain Language	85
Visual Cues	85
Layered Policies (Also Known as Layered Notices)	86
Prominently Display Your Privacy Policy and Opt-Out Choice	86
Contract for the Same Level of Privacy	86
Review Good Examples of Privacy Policies	87
Get Key Employees and Executives Involved	87
Review, Approval, and Implementation	88
Privacy Programs	88
Support and Strategic Planning	88
Training and Awareness	89
Privacy Policies, Procedures, Checklists	89
Creating a Privacy Team	90
Challenges	90
Communication	91
Incident Reporting and Response	91
Data Breach	92
Library Privacy Policies and Programs	93
Language and Presentation Options	93
Considerations before Drafting	94
Data Flows and Retention	94
Data Collection, Use, and Third Parties	94
Awareness and Training	95
Considerations for Special Populations	95

ALA Guidance for Libraries	95
Conclusion	95
Notes	96
Bibliography	98
7 Global Information Privacy	99
Fair Information Principles	99
The Organization for Economic Co-operation and Development's Guidelines	100
Fair Information Practice Principles (USA)	102
European Privacy Protections and the Data Protection Directive	103
U.S.-EU Safe Harbor Program	104
Binding Corporate Rules and Model Contracts	106
APEC Privacy Framework	106
Canada's More Comprehensive Protections	107
Two Federal Laws	107
PIPEDA Privacy Principles	108
Conclusion	110
Notes	110
Bibliography	112
Glossary	113
Index	121
About the Author	129

## *Chapter One*

# **Introduction to Information Privacy**

Issues surrounding information privacy have gained prominence in recent years due to changes in technology and the rise of data mining. The increasing ability and efforts to gather data about individuals—including information about their health, finances, and online activities—have increased privacy concerns. Continuing reports of data breaches, secret data collections, deceptive privacy policies, and large-scale spying and data collection have made us a country weary of the efforts of companies, governments, and enterprising individuals to collect and analyze our private information. Concerns about information privacy are increasing globally. Americans' rising concerns about information privacy are evident in a July 2013 Pew report<sup>1</sup> that examines attitudes about the National Security Agency (NSA) surveillance program. Pew's national survey of 1,480 adults has found that the majority (70 percent), believe that the government uses data collected by the NSA for more than just the investigation of terrorism.<sup>2</sup> Findings in the Pew report also indicate that nearly half (47 percent) of Americans surveyed were concerned that government antiterrorism policies have begun restricting civil liberties.<sup>3</sup>

The privacy landscape continues to evolve with changes in technology, law, and in response to changing privacy concerns. What once was unthinkable, the ability of individuals, governments, and corporations to spy on an individual's activities both online and off, is now a reality. People make important decisions that impact their privacy on a daily basis, sometimes giving away privacy rights without realizing it. This can occur when doing such mundane things as automatically accepting the terms to download and use apps on smart phones without considering the terms of the agreement and browsing web pages or conducting transactions over the Internet without reading the privacy policies. In the United States the NSA surveillance pro-

gram; the use of domestic surveillance drones<sup>4</sup> ; and other devices used by governments, businesses, and enterprising individuals to track, monitor, and record personal information means that even those with a careful eye on securing their information privacy will experience limits to their protection. The growing concern about the loss of information privacy and its impact on our daily lives, professional reputations, and the free exercise of our civil liberties highlights the importance of understanding what information privacy is and why we must fight to preserve it.

This first chapter will examine the origins of the right to privacy in the United States and the meaning of information privacy and related terms. Privacy rights will be placed in context to understand their origins in U.S. law and in other countries. A brief introduction and roadmap will then be provided to the remaining information privacy topics examined in this text.

## ORIGINS OF PRIVACY RIGHTS

Peter P. Swire and Kenesa Ahmad explain that “the concept of information privacy as a social concept is rooted in some of the oldest texts and cultures.” They cite references to privacy in the Bible, the Qur’an, Jewish law, and the laws of classical Greece.<sup>5</sup> There also existed early formal legal protections for privacy in laws dating as far back as 1361 in England. Laws in other parts of Europe dating to the 1700s have been enacted to address privacy issues. Privacy rights in the United States, like the country itself, are more recent in their creation.

### U.S. Privacy Rights

#### *Privacy and the U.S. Bill of Rights*<sup>6</sup>

Though it is a common misconception, the term *privacy* does not appear in the *U.S. Constitution*. The *Bill of Rights* does contain language that reflects a focus on protecting certain aspects of privacy. Amendment I contains an implied privacy of religion or worship, providing that:

Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances.

Amendment IV reflects a concern for privacy of person, house, and belongings from searches and seizures. It provides:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and

no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Here, privacy is of a tangible nature.

Amendment V can also be seen as encompassing a privacy component, that of protection from intrusion. It holds in pertinent part that:

"No person shall . . . be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation." <sup>7</sup>

Amendment XIV<sup>8</sup> extends this protection specifically to states by forbidding the creation or enforcement of state laws that abridge these rights.

### *The "Right to Privacy" Is Recognized*

Nearly one hundred years after the *Bill of Rights* became law, Samuel Warren and Louis Brandeis (1890) published their seminal essay "The Right to Privacy" in the *Harvard Law Review*.<sup>9</sup> In it, they defined privacy as "the right to be let alone."<sup>10</sup> Warren and Brandeis wrote of the necessity of this protection because of the invasion of privacy by the press. While serving as Supreme Court Justice, Brandeis would affirm his definition of privacy in the context of government action in his dissent in *Olmstead v. United States*. In *Olmstead* Brandeis stated:

The makers of our Constitution . . . recognized the significance of man's spiritual nature, of his feelings, and of his intellect. . . . They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government, the right to be let alone—the most comprehensive of rights, and the right most valued by civilized men. To protect that right, every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment. And the use, as evidence in a criminal proceeding, of facts ascertained by such intrusion must be deemed a violation of the Fifth.<sup>11</sup>

Other cases have followed *Olmstead* that have also articulated privacy rights. Many definitions have been proposed for the meaning of privacy.

### **State Recognition of Privacy**

Many state constitutions also provide privacy protections. Ten states specifically address the right of privacy in their constitutions.<sup>12</sup> Others provide statutory privacy protections for specific types of information, such as medical and financial records. These often add to the protections afforded by



federal laws. Privacy protections may also be created through private contracts and privacy notices.

Invasion of privacy may be actionable under tort law. Tort law is state law and torts are civil wrongs that are recognized by law as a basis for lawsuits. These can include intrusion on seclusion, appropriation of one's name or likeness, public revelation of private facts, and false light in which the public disclosure of information is misleading. Lawsuits brought under state tort laws are different from those filed in response to large-scale personal data breaches, such as the Target breach of late 2013. The latter type are generally class-action suits for statutory damages, relying on provisions in federal laws that limit the circumstances in which certain types of personal data can be released.<sup>13</sup>

## INFORMATION PRIVACY DEFINED

A study of privacy, a fundamental interest that is potentially so broad in scope, requires a working definition. Dr. Alan F. Westin defined *privacy* as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."<sup>14</sup> Westin's definition is particularly relevant for our examination as it provides us with a working definition of *information privacy*, which can be thought of as a subset of the more general right to privacy.<sup>15</sup> Westin published this definition during a time period (1961–1979) that he identifies as "the first Era of contemporary privacy development." This period is marked by a rise in awareness of the importance of information privacy and concerns about the impact of technology on privacy. Information privacy became "an explicit social, political, and legal issue."<sup>16</sup>

Westin's definition most closely matches the contemporary understanding of the meaning of *information privacy*. Indeed, Westin's definition has been cited by Kris Klein to define the meaning of *information privacy*, one of three recognized categories of privacy in Canada.<sup>17</sup> Similarly, Peter P. Swire and Kenesa Ahmad identify four classes of privacy (information privacy, bodily privacy, territorial privacy, and communications privacy). They identify information privacy as being "concerned with establishing rules that govern the collection and handling of personal information."<sup>18</sup> This would include personal information of all kinds including medical and financial information.

### Personal Information

Certain terms are associated with information privacy and privacy law. It is important to have a basic understanding of the meaning of terms commonly used in discussions of information privacy, information privacy manage-