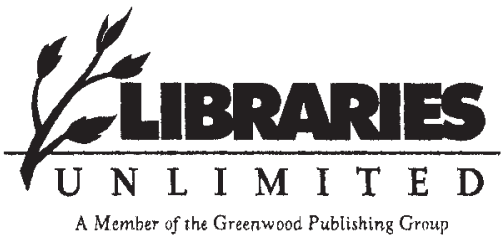
What Every Librarian Should Know about Electronic Privacy

Jeannette Woodward

WHAT EVERY LIBRARIAN SHOULD KNOW ABOUT ELECTRONIC PRIVACY

WHAT EVERY LIBRARIAN SHOULD KNOW ABOUT ELECTRONIC PRIVACY

Jeannette Woodward



A Member of the Greenwood Publishing Group
Westport, Connecticut • London

Library of Congress Cataloging-in-Publication Data

Woodward, Jeannette A.
What every librarian should know about electronic privacy / Jeannette Woodward.
p. cm.
Includes bibliographical references and index.
ISBN-13: 978-1-59158-489-6 (alk. paper)
1. Public access computers in libraries—United States. 2. Internet access for library users—United States. 3. Confidential communications—Library records—United States. 4. Computer security—Law and legislation—United States. 5. Data protection—Law and legislation—United States. 6. Privacy, Right of—United States. I. Title.
Z678.93.P83W66 2007
025.50285—dc22 2007013566

British Library Cataloguing in Publication Data is available.

Library of Congress Catalog Card Number: 2007013566
ISBN-13: 978-1-59158-489-6

First published in 2007

Libraries Unlimited, 88 Post Road West, Westport, CT 06881
A Member of the Greenwood Publishing Group, Inc.
www.lu.com

Printed in the United States of America

The paper used in this book complies with the Permanent Paper Standard issued by the National Information Standards Organization (Z39.48–1984).

10 9 8 7 6 5 4 3 2 1

To Lowell, Laura, Chris, and John with all my love.

Contents

Introduction

Few professionals are as concerned about the privacy of their customers as librarians. We want our libraries to be places where they can explore ideas of all persuasions and need never worry that big brother is looking over their shoulders. Just consider, for example, our spirited opposition to the Patriot Act. While the librarians collectively known as "John Doe" made national news when they refused to surrender library records without a warrant, the American Library Association challenged the constitutionality of the law (Cowan 2000). Again and again, librarians have defended the right of citizens to read and inform themselves, free from intrusion and free from censorship.

Because librarians believe that citizens in a democracy need unrestricted access to information, we have also been leaders in providing public access computers. Our commitment to an information literate society has led libraries to make computers available to those who lack either the financial resources or the technical sophistication to purchase and maintain their own machines. In fact, computers have totally transformed libraries in recent years. They are now used to perform a wide variety of clerical and administrative tasks. In addition, they have replaced the old card catalogs with much more efficient online public access catalogs, and provide access to thousands of digitized journals. Computers are ideally suited to the library environment, and we have embraced them enthusiastically. We may, however, be allowing our computers to inadvertently jeopardize the privacy of our users.

THE LIBRARY'S RESPONSIBILITY

The ALA Council's, "An Interpretation of the Library Bill of Rights" adopted June 19, 2002 makes clear the position of the library community regarding individual privacy. "Privacy is essential to the exercise of free speech, free thought, and free association … In a library (physical or virtual), the right to privacy is the right to open inquiry without having the subject of one's interest examined or scrutinized by others … When users recognize or fear that their privacy or confidentiality is compromised, true freedom of inquiry no longer exists" (American Library Association 2002).

The fear of Islamic terrorism pervades much of contemporary American life. As has occurred repeatedly throughout our history, fear sometimes causes people to temporarily devalue their freedoms and those of their fellow citizens. Readers of the well-written and informative book *Jihad: the Rise of Militant Islam in Central Asia* by Ahmed Rashid have experienced some of the overreaction that inevitably occurs when people are frightened. The book jacket displays the single word Jihad in very large letters, large enough that they are visible from a considerable distance. Commuters on subway trains have reported their fellow passengers to the police, simply for carrying or reading the book (Robinson 2006).

In such an environment, protecting the freedom to read and to seek out information becomes much more difficult. The role of librarians does not end with simply making information available to users. It must extend to protecting those users from overzealous or paranoid elements of our society who equate ignorance with patriotism. In his article "Librarians at the Gates," Joseph Huff-Hannon summed up this responsibility: "Be it in the capacity of archivist, reference librarian, or information technology professional, a common thread is the profession's dogged commitment to safeguarding books, research, and information to make knowledge more widespread, not less" (Huff-Hannon 2006).

LIBRARY COMPUTER USERS ARE AT RISK

Although it may not be immediately obvious, our determination to protect our users' privacy can sometimes conflict with our commitment to provide the public with access to online resources. The public library probably provides more opportunities for free Internet

access than any other organization. We encourage our patrons to use our computers to satisfy their information needs, and most libraries allow them to take advantage of e-mail and/or other recreational resources. The access we provide, however, is necessarily limited. Because they have fewer opportunities, our users tend to be less informed and more at risk than computer owners.

For example, most of the millions of people who use the library's public computers have signed up for e-mail accounts like Hotmail and Yahoo. Their e-mail messages are stored on the computer servers of those service providers, and their accounts are accessed in much the same way that computer owners access the e-mail programs on their personal computers. However, those messages and other documents that comprise "Web mail" receive only weak privacy protection. Government agencies do not need search warrants to access personal Web mail as they would to search privately-owned computers.

Library computer users are often novices and may not be aware that even seemingly innocuous information supplied to Web sites can be mined by both government agencies and unscrupulous businesses. The recent discovery that online service providers have been supplying vast quantities of data to government agencies without the public's knowledge has highlighted the threat.

Comparing Libraries of Yesterday and Today

This era in which libraries and their users are now struggling, is different in one way from any other period in human history. Never before was it possible to gather vast quantities of personal information, and bring it all together to create a detailed profile of each and every individual. It was common knowledge that our Social Security numbers and driver's license information were available to various government agencies. In fact, quite a lot of personal information was filed away somewhere, but it was difficult to locate and gain access to it. There was no way that one careless individual could take home the Social Security numbers of the 26 million veterans and make them available to thieves, as happened in a 2006 laptop theft (Lemos 2006).

Privacy threats posed by overzealous marketers are also relatively new. We have known that businesses collect information about us for some time. Some kept our names and addresses in their records, sending us sales promotions. Today, however, marketers have created

vast databases full of highly confidential information about our personal habits. For example, the mammoth data broker ChoicePoint inadvertently gave an identity thief access to the personal information, including Social Security numbers, of 145,000 people (Zeller 2005). Their goals are essentially the same as they always were: to sell us more of their merchandise and services. However, the techniques they employ are just as invasive as those used by government agencies, and they cannot be justified by threats to national security.

Laws Must Catch-Up with Technology

Technology has progressed much more rapidly than state and federal privacy legislation. Both marketers and overly enthusiastic government officials are unconstrained by the usual laws, regulations, and ethical guidelines that would normally prevent the misuse of personal information. Additionally, there has been a dangerous confluence of disaffected, highly skilled computer specialists and cyber-thieves. Both legislators and law enforcement agencies are slow to respond, leaving millions of individuals open to attack. Only recently have we fully realized how dangerous personal information can become in the wrong hands. Not only do thieves steal billions of dollars, obtaining loans and charging merchandise against the credit cards of innocent people, but they have also committed violent crimes in their names, literally stealing their homes and abducting their children.

Privacy is not a Political Issue

In our private lives, we librarians bridge the full political spectrum from right to left. It is important that we not view privacy as a political ping pong ball, bounced back and forth between parties when it suits their purposes. Privacy is much more than political rhetoric; it is a cornerstone of our professional ethics. It does not matter which party is in power; we have an obligation to protect the privacy of our users as a matter of principle. It is essential that our enthusiasm for our cause not wax and wane, depending on the occupant of the White House or the composition of Congress.

Perhaps Justice Louis Brandeis put it best when he called privacy "the right to be left alone." Without well-considered legislation, there is nothing to stop marketers and government agencies from keeping track of the books people buy, the illnesses they suffer, the checks

they bounce, the places they visit, or the personal problems they endure.

Searching for Terrorists

It has recently become clear that the National Security Agency (NSA) is monitoring millions of telephone calls, theoretically intended to help fight the war on terror. Concurrently, NSA and other government agencies have developed vast databases of personal information to be used for data mining (the trolling of billions of bits of personal information) searching for patterns that match government profiles of the typical terrorist.

The problems with such a strategy are numerous. First, there really is little scientifically reliable evidence that such profiling can effectively identify terrorists. Sadly, government workers have repeatedly identified innocent people who happen to share names, personal habits, travel destinations, and financial activities with the few known terrorists whose biographies are available. Too many intelligence agency projects appear to be the product of overly imaginative government functionaries who were influenced by fictional exploits like those portrayed in the movie "Mission Impossible."

Furthermore, as was made clear in the incident of the 26 million Veteran's records, the people who staff those government agencies are fallible human beings. People often take shortcuts, become careless, or put their personal needs above the demands of their jobs. In the case of the veterans' records, the practice of copying personal data to agency laptops and home computers had been widespread for years. It was considered more convenient to do so. In other government agencies, access to personal records has been so widely available, and supervision so lax, that staff members actions have led to numerous felony charges.

Collecting Data Just in Case

As we in libraries know, there is a natural urge to collect data just in case we need it someday. Our patron information records contain fields that no library should ever use, but blame cannot be placed entirely at the door of our vendors. As we work with them in developing more functional library systems, the thought keeps recurring: "That would be interesting to know." We are charmed by all the

reports that can be produced with the click of a mouse and we imagine that we could do our jobs better if we knew more about our patrons. That's true, but at what price do we collect this unneeded data? Almost every library has discovered, especially when faced with a search warrant or other request for information by a law enforcement agency, that it has inadvertently collected far too much data from its users.

Keeping Up with Breaking News

As this book goes to press, news concerning the Patriot Act, data mining, and other privacy matters is breaking daily. With the recent changes in Congress have come numerous investigations into the way the Justice Department and other federal agencies have used or misused their authority. It is inevitable that the investigations will result in new policies and even new laws. Similarly, upcoming court decisions will profoundly affect privacy issues. Since these developments will be of great interest to readers, Libraries Unlimited will add a new section to its Web site to update you on breaking news, legislation, court decisions, and new information regarding upcoming investigations. You will find more information about these updates at the end of the book.

Computers in the Library

This book is intended for librarians and library supporters representing most types of libraries. Public, school, and academic libraries routinely provide public computers to meet the needs of their users. Libraries of every type including medical, law, and corporate libraries, use computers to maintain records of both their patrons and their materials. This means that the information stored in library staff computers could compromise the privacy of many individuals by revealing personal information about their lives and their reading habits. Although librarians are committed to protecting the privacy of their users, they may not be aware of the broad range of privacy issues that surround electronic data. Patrons may be subjected to unnecessary and unwanted threats to their personal privacy.

This book is intended to be a practical guide on the issue of electronic privacy in the library. It focuses on real library users rather than on abstract concepts. It is not intended to be a comprehensive

or technically sophisticated overview of the issues. When technical strategies are mentioned, they are never described in detail, leaving it to you, the librarian, to bring such matters to the attention of technical staff.

Although we may find it difficult and demanding to protect our users, we have no choice but to do so. Jonathan Turley, law professor at George Washington University, sums up our responsibility succinctly when he writes, "It is only in the assurance of privacy that free thoughts and free exercise of rights can be truly exercised. Such privacy evaporates with doubt; it is why the Constitution seeks to avoid the chilling effect of uncertainty in government searches and seizures."

REFERENCES

American Library Association. 2002. Privacy: An Interpretation of the Library Bill of Rights. Adopted June 19, 2002, by the ALA Council. http://www.ala.org/ala/oif/statementspols/statementsif/interpretations/privacy.htm.

Cowan, Alison Leigh. 2006. U.S. ends a yearlong effort to obtain library records amid secrecy in Connecticut. *New York Times*, June 27. http://select.nytimes.com/search/restricted/article?res=FA0C1EFD3C540C748EDDAF0894DE404482.

Godwin, Jennifer. 2000. Librarians at the gate. *Forbes*, July 24, p. 184.

Huff-Hannon, J. 2006. Librarians at the gates. *Nation Magazine*, August 22. http://www.thenation.com/doc/20060828/librarians/.

Lemos, R. 2006. Veterans Affairs warns of massive privacy breach. *Security Focus*, May 22. http://www.securityfocus.com/news/11393.

Robinson, Eugene. 2006. Fear is driving U.S. public opinion. *LJ World*, May 18. p. B6. http://www2.ljworld.com/news/2006/may/18/fear_driving_us_public_opinion/.

Turley, Jonathan. 2006. "Big brother" Bush and connecting the data dots: the total information awareness program was killed in 2003, but its spawn present bigger threats to privacy. *Los Angeles Times*, June 24. http://www.commondreams.org/views06/0624-29.htm.

Zeller, Tom. 2005. Breach points up flaws in privacy laws. *New York Times*, February 24, p. C1. http://www.nytimes.com/2005/02/24/business/24datas.html?ei=5088&en=1a34f1accdb516d9&ex=1267160400&partner=rssnyt&pagewanted=print&position=

For the latest updates on Electronic Privacy in the Library, please visit this book's companion Web site at the Libraries Unlimited Web site, www.lu.com/e-privacy.