

at a time anyway" without providing any documentation to support his claim. *No one* reads more than three or four pages? An informal survey of the undergraduates in my library quickly put this notion to rest. In a discussion on online commerce, he states as inevitable "the sad conclusion is that if one chooses to use the Web as his or her preferred means of doing business, he or she *will* eventually become a victim of Internet fraud of some kind," as if this were some law of economics.

Herring's conservative viewpoint dominates these pages, and he often states his opinions as fact. "Democratic capitalism has proven to everyone (save a few political science professors working at American universities) to be the best form of economic government," he asserts with certainty. He uses the term "First Amendment absolutists" with nothing less than disdain, and pretty much equates anyone who is against Internet filtering as being pro-pornography. By his own admission, Herring is a cultural warrior, and at times this book feels far more like an extended, clever rant intended to rally the faithful and alienate the opposition. As such, it reads like more like a guest editorial on *Fox News* or an op-ed piece in *The Washington Times* than a solid work of scholarship. —Gene Hyde, Radford University.

**Woodward, Jeannette A.** *What Every Librarian Should Know about Electronic Privacy*. Westport, Conn.: Libraries Unlimited, 2007. 222p. alk. paper, \$40 (ISBN 1591584892). LC 2007-13566.

After reading this book, some users will likely throw away their computers, regress to communicating through smoke signals, and toss their underwear out the window. Why? The reason is because "Big Brother" is watching you. Most Americans know that the possibility of their electronic communications being read by a third party is very likely in today's tech-savvy world, but what does underwear have to do with "Big Brother"? At least one underwear manufacturer was caught imbedding traceable RFID (radio

frequency identification) tags in their underwear. While this company and others, including libraries, only use these tags in their products to trace shipments and for inventory, there is the possibility of using RFIDs for tracking people.

Yet, what happens when some unscrupulous person gets hold of the means to use RFID tags to trace someone? An RFID tag in a library book could be used to trace a library user anywhere. Imagine what happens when this same patron is using a public library computer that happens to have key logging software on it? Everything they type is conveyed to another party who is stealing this patron's information. Then there are also legal ways of data mining in which third-party vendors sell information retrieved from online searches. Each of these intrusions into an individual's right to privacy is appalling, but imagine combining all of them together.

Examples such as these are Jeannette Woodward's reason for reminding librarians that their task is not only to provide public access to information but also to protect patrons from those who manipulate them in the world of electronic information. Woodward, herself a former public library director, academic library assistant director, and author of several books, has most likely dealt with electronic privacy issues herself and as a director, has been a decision maker on privacy policy. Understanding that there is no guaranteed method of protecting electronic information, she contends that librarians need to be proactive in informing their users how to protect themselves. Current privacy legislation is outdated by more than twenty-five years; and, until legislation catches up with changes in communication technology, data brokers will continue to mine data from online searches and sell it to interested parties, and hackers will continue to steal information. There are tactics available to library users to guard their information and to protect it from online predators. Libraries should collect and store only

the personal information on their patrons that is absolutely necessary; when libraries collect data for the sake of collecting, it puts their patrons at risk.

This book addresses many forms of privacy invasion and the parties who are responsible for them. It includes an index and glossary of terms and acronyms. Phishing, key loggers, and spyware are covered in a chapter on identity theft, while another chapter documents privacy threats from the business world. A chapter is devoted to the online threat to children and teens with a special focus on the online social networking scene. No treatment of electronic privacy would be complete without a study of government privacy intrusions; Woodward provides a critical analysis of the U.S. government's track record on privacy invasion, noting how the government's overdependence on technology has led to inefficient and inadequate law enforcement. One chapter addresses complications with the PATRIOT Act and how librarians find themselves at odds trying to cooperate with law enforcement while also protecting their patrons' privacy rights. RFID tags are discussed in a separate chapter.

Woodward includes numerous real-world examples. Some demonstrate what can actually happen when the system fails and information is accidentally exposed or lost. Other examples deal with subpoenas for library records and how some libraries deal with warrants. Librarians will find the last two chapters particularly helpful for establishing procedures and programs of education for library users and employees and for determining ways to keep our patrons' information safe.

Every library should have a copy of this book. It is an excellent guide to the kinds of privacy intrusion that libraries and those who frequent them experience and how to avoid them. In the post 9/11 environment, privacy has become a more precarious civil liberty, and librarians need to be more diligent than ever in ensuring its protection.—*Brian J. Sherman, McNeese State University.*

*Books on the Move: Tracking Copies through Collections and the Book Trade.* Eds. Robin Myers, Michael Harris, and Giles Mandelbrote. New Castle, Del.: Oak Knoll Press (*Publishing Pathways*); London: British Library, 2007. 164p. alk. paper, \$49.95 (ISBN 1584562196;0712309861). LC2007-41192.

This latest volume in Oak Knoll Press's *Publishing Pathways* series offers the proceedings of the twenty-seventh annual conference on book trade history sponsored by the Antiquarian Booksellers' Association in London. While the title of the collection itself, and the editors' introduction, make the conference theme clear, it is contributor Pierre Desaerdt who most clearly expresses the importance of provenance research: it is not simply a game for bibliophiles (or bibliomaniacs), but one way "to assess the representative quality of research based on collections of printed books." Tracing the moves of collections, and individual items within those collections, tell us something about the number and genres of books published in certain locales, the forces that shaped the preservation or destruction of books and how the transfers of books and manuscripts from individual owners to large public repositories occurred. Unless we understand how public collections came to be, says Desaerdt, we cannot judge the value of the research that builds upon these collections.

The essays in this volume are, for the most part, case studies of particular titles or the collections of individual persons. Peter Beal, author of the monumental *Index of English Literary Manuscripts*, opens the volume with his musings, entitled "Lost: The Destruction, Dispersal, and Rediscovery of Manuscripts." He lays out several reasons for the loss of manuscripts: war, the dissolution of monasteries (a theme that other contributors to the volume will elaborate on); intentional destruction (for example, the burning of the Earl of Rochester's letters by his pious mother); theft; vandalism; and, most