

William S. Wallace. The Perimeter of Security: Policy as the Bridge between Library Security Philosophy and Library Security Practice. A Master's Paper for the M.S. in L.S degree. April, 2008. 44 pages. Advisor: Mark Winston

This paper is a literature review and analysis of scholarship concerning library security. The paper was composed to present the idea that library security is, actually, composed of two parts: practical security and the philosophy of security. Furthermore, it is suggested that one meaningful way of understanding this idea is in terms of viewing library security policy as a conceptual bridge between the practical and philosophical dimensions of security.

Over twenty pertinent articles are incorporated into the review and synthesis of this paper. Furthermore, substantial supplemental materials are also mentioned. The intent of this review is to provide a detailed view of current scholarship, the terms which are widely used, and the places where a more unified and overarching theory – such as the one presented – might prove useful.

Headings:

Library Science - Philosophy

Library Security

Libraries Security – Measures

Library Security – Philosophy

THE PERIMETER OF SECURITY: POLICY AS THE BRIDGE BETWEEN LIBRARY
SECURITY PHILOSOPHY AND LIBRARY SECURITY PRACTICE

by
William S. Wallace

A Master's paper submitted to the faculty
of the School of Information and Library Science
of the University of North Carolina at Chapel Hill
in partial fulfillment of the requirements
for the degree of Master of Science in
Library Science.

Chapel Hill, North Carolina

April 2008

Approved by

Mark Winston

Contents

Introduction.....	2
Security	3
Security System	4
Threat and Risk.....	4
Security Policy	4
Mission.....	5
Questions and definitions.....	6
Current scholarship about library security	12
“Practice-related” literature	12
“Philosophy-related” literature	18
Security as a concept.....	25
Philosophy of Security	28
Conclusions.....	31
Bibliography	36
Appendix A: Selected policies and guidelines.....	42

Introduction

Libraries are, among other things, storehouses of knowledge. The defining characteristic of a storehouse is that there is a concept of creating and maintaining security; there are plans and structures in place which are designed to control and protect that which is stored. In other words, the goal of library security is to provide a safe environment for objects, people, and places which are held to be of value.

Threats to the idea of security come in many forms, and range from intentional acts such as book theft, vandalism, or identity theft to dangers which originate from unintentional factors such as flood, fire, and even the naturally depreciative processes of time. Library security is typically best understood as a system, one which reflects the strategies of planners to prevent or ameliorate the negative consequences of a realized threat.

In order to achieve this goal, a security system is composed of two elements: An actual, physical system, consisting of people, devices, and written instructions; and a conceptual mission which underlies it. In the most basic terms, this conceptual mission is exactly the goal mentioned above, “to provide a safe environment.” In a more sophisticated view, this “mission” actually reflects complex philosophical decisions about the value of knowledge, the purpose of its protection, and the role of librarians as its stewards. This paper presents the idea that one way of accessing, and exploring, the philosophical missions that support security systems is by looking closely at security policies.

The most basic reason for investigating this matter is to provide a better quality of service for both library patrons and for library collections. Although the specifics of security concerns are certainly evolving throughout time, the basic charge of a library to protect knowledge has not, and never will, change. For this reason, it is critical to the health of librarianship and library science that we deeply explore these matters of security, which lie so close to the very heart of our purpose.

In order to proceed, it is important to provide some working descriptions of useful terms. Throughout the course of this paper, all of these ideas will be expanded and developed, but these definitions will provide stable starting points, the first few of which are gathered from the work of Bruce Scheiner:

Security

Perhaps the most technical definition available can be found in the *Department of Defense Dictionary of Military and Associated Terms*, where security is explained as follows:

“A condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influences. 2. With respect to classified matter, the condition that prevents unauthorized persons from having access to official information that is safeguarded in the interests of national security. 3. Measures taken by a military unit, an activity or installation to protect itself against all acts designed to, or which may, impair its effectiveness” (DOD Pub 1-02, p. 2).

Although this gives a clear view, a slightly more nuanced definition can be found in Scheiner's *Beyond Fear*, where he writes, "Security is about preventing adverse consequences from the intentional and unwarranted actions of others" (Scheiner, *Beyond Fear*: p. 12).

Security System

"A security system is the set of things put in place, or done, to prevent adverse consequences." (Scheiner, *Beyond Fear*: p. 12). For the purposes of this paper (although the subject will be later addressed) I will largely overlook Scheiner's distinction between security and safety in the context of a security system: "Protecting assets from unintentional actions is safety, not security" (p. 12).

Threat and Risk

"A threat is a potential way that an attacker can attack a system... When security professionals talk about *risk*, they take into consideration both the likelihood of the threat and the seriousness of a successful attack" (Scheiner, *Beyond Fear*: p. 20).

Security Policy

For this paper, I will define a security policy, in the most basic sense, as a set of plans or guidelines intended to direct the response to potential and actualized threats.

Mission

Finally, the use of the word mission, here, is intended to provide a sense of not only intent or mandate, but also those parts of a set of decisions which are influenced by deeply held beliefs and ontologies.

This paper will explore these various ideas in terms of the most recent literature of library science, comparing and contrasting a number of approaches to both the practical and philosophical understandings of security. Following upon this, I will further develop the idea of security and advance the theory that library policy represents the most direct connection between the two poles of security as a mundane reality and security as a complex set of ideas. Finally, it is hoped that this process will present a more holistic and “three-dimensional” view of library security and, in so doing, provide a useful starting point for further research and scholarship.

Questions and definitions

The consideration of library safety and security has certainly been of critical importance since the earliest collections of recorded knowledge. In modern times, these issues are considered to be an important part of the discipline of preservation in libraries and archives, but related concerns impact all areas of librarianship. It is certain that every library in the world, whether tacitly or explicitly, has addressed the issues of protecting its collection, as well as its library facility, library staff, and library patronage.

Security is a multi-faceted concept, as it represents a number of ideas, including a state, a condition, a feeling, and a process. Each of these notions will be investigated throughout this paper, but the working definition in operation here is two-fold: One, security is the *practical*, physical, process of controlling the state of a library's collection, staff, patronage, and facility; Two, security is a *concept* which encompasses the emotional and rational process of doing the same.

In beginning to attempt to define security, it is a common approach to define the idea of a "threat." In the most concrete sense, a threat is any agent or condition which counteracts the process of controlling the state of a library's collection, staff, patronage, and facility. For the purposes of this paper, the idea of threats will not be closely examined, but the term will be used in a general sense to refer to criminal activity, natural disasters, inherent vice, and all of the other multifarious vectors of attack upon an instantiation of security.

Along with “security,” and “threat,” the third label which will be frequently used is “policy.” In the realm of the philosophy of security, as presented in this paper, policy refers to a strategy which bridges the conceptual structure of security with the actual, practical, implementation of security. This bridge is critical and will be addressed at length throughout this discussion.

The subject of library security has been outlined and surveyed in a variety of studies (Janus 2001, et. al.), often with the intent of suggesting ways and means of improving the quality of existing security (Nilsen 2003), or of designing improved security systems for future implementation (Scire 2003). These works are a critical part of the practice of librarianship.

This paper suggests that scholarship regarding this topic would be well-served and improved by a thoughtful consideration of the underlying principles which drive security policy decisions. It is very common that security policy is implemented in a developing or iterative manner, often without the exact reasoning behind that policy having been made clear to those who enforce it. A clearly presented analysis of the alignment between principle and practice might provide significant insight into the motivations and actions of policy-makers. In other words, it is important that librarians and library policy-makers alike understand *why* security decisions are made.

There are several standard approaches to considerations of security, most of which center upon the practical and pragmatic securement of physical assets. In contrast, this paper will address the concept of security in terms of the philosophy which underlies

it. In the case of library security, there are several levels of complexity which must be evaluated and appreciated for their unique character.

“Philosophy,” of course, literally means “love of wisdom.” It is also a notoriously evasive target for definition. So much so, in fact, that it is often best known in terms of its schools, such as objectivism or relativism. My use of the term here is intended to evoke some of the nuance which characterizes matters of mission, faith, intent, concept, and ontology.

The spirit of this investigation is largely informed by Michael Renner, who wrote in the Worldwatch Institute’s *State of the World 2005* that: “First, a... security policy needs to be transformative in nature... The second principle flows from this insight: a new security policy must above all be preventive in nature... The third principle is that a... security policy needs to be cross-cutting and integrative” (p. 16). The idea of integrative policy resonates closely with my idea that policy is that which integrates practice and philosophy in the realm of library security.

This paper will, as a matter of necessity, skirt the role of library mission statements (as expressed both directly and in terms of non-security-related standards, principles, and guidelines), as they determine library security practice and policy. Towards this end, the following supplemental research questions will be considered and, if not fully explored, at least acknowledged:

- How is library security defined?
- What are the purposes of library security?
- What measures are used for evaluating the quality of library security?

- How are instances of “better” library security caused by more direct correspondence to underlying library mission statements?

From that starting point, this paper will survey some of the pertinent literature in the field with an eye towards viewing the distinction between “practical” studies of security and the “philosophical” studies of security.

Concurrent with the review, we will explain the use of the term philosophy and address the importance of these concepts to essential library policy. Finally, this paper suggests that the best means of understanding security in a library is as a direct extension of the values which underlay policy. It is hoped that this process will emerge from the field which has been thus circumscribed – In fact, the true goal of this paper is to use fringe and outlying studies of library security to begin the process of defining the field of the philosophy of library security.

It is fitting to consider the question of “why” not only in terms of library security policy, but also in regards to this paper. Especially in the context of a post-9/11 United States, issues of library security have become increasingly discussed. Necessarily, as in articles such as Viscusi (2003) and any number of Brown-Syed’s insightful works, these studies often center upon ideas of privacy and information security. These ideas are quite evocative, eliciting the kinds of questions which lie at the heart of the study currently being outlined.

Perhaps one of the most poignant examples of this category of scholarship is, “The Safeguarding of Memory: The Divine Function of the Librarian and Archivist” (Owens 2003). This article, written by a rare books librarian, proposes a consideration of

the librarian as being a guardian of memory, especially in the face of tragedies such as genocide. The notion of “safeguarding” is the notion of security, eloquently expressed in a way which echoes both the pragmatic and philosophical architectures which direct it.

Alao’s (2004) “The Effectiveness of Library Measures Against Theft and Mutilation: An Opinion Survey” performed an analysis of African library security measures and concluded that, “diversification of library security measures should be based on considerations of cost-effectiveness” (p. 29). It is a significant idea, and one which drives much policy decision-making (indeed, perhaps *all* policy decision-making), that collections and – by extension – facilities, staffs, and patronages can be considered to be assets. In this context, it seems like a logical extension of policy analysis to look at philosophical decisions in the form of ideas about security missions and policies and, indeed, these themes of mission and purpose are at the heart of this paper. It bears mention for both this reason and also for its potential value as a piece of scholarship which can be seen as representative of the mainstream of security scholarship.

These works, however, from studies of privacy to reviews of mission statements, are insufficient for the particular quest to work towards completing our understanding of how philosophy and practice are connected. This paper will attempt to demonstrate that there is a correlation between library security philosophy and actual, practical, library security. Furthermore, this paper shows that the correlation is best mapped in terms of policy.

This process will be characterized by pointing to examples of existing efforts to chart this domain; much of this paper is a comparative literature review of the most

cutting-edge scholarship of library security. In presenting this review, and connecting some of the dots between the scholarship thus represented, it will endeavor to provide a clear connection between the philosophies which underlie security practices and provide a generative example for further study of this subject area.

Current scholarship about library security

Investigating the problem of how library security can be seen to succeed or fail in direct correlation to the degree of clarity which supports it; this literature review presents an overview of several pertinent research articles. The subject articles are separated into two broad categories, “practice” and “philosophy.”

“Practice-related” literature

An article by William E. Chadwick, “Special Collections Library Security: An Internal Audit Perspective” (1998), was written as a technical appraisal of the reported increase of theft and fraud in special collections libraries. Like Sowd (2003), he points out that there has been a dramatic increase in the market value of rare books during the 1980s, and cites this as one of the three primary reasons for an ever-growing number of instances of theft. The other, equally important, factors are the development of “user-friendly” environments (and the subsequent implementation of lax protective measures) and the practical difficulties of protecting the collection. Both of these two categories have led to poor “internal control” of library collections. This author defines “internal control” as being a collection of five activities: 1) controlling the collection environment, 2) risk assessment, 3) control activities, 4) information and communication, and 5) monitoring.

In his analysis of internal control, Chadwick notices that there is a shift away from acceptance and selective tolerance of white-collar crime. He states that libraries which

would once minimize outside perception of the frequency and impact of “gentlemen’s crimes” such as theft are now coming to an understanding of these kinds of crime as being, perhaps, the most dangerous of all security violations for the integrity of a collection.

In outlining his suggestions for improving special collections security, Chadwick distinguishes between Internal Audit and the role of library personnel concerning library control responsibility. The former, he explains, is a form of high-level practice which more closely aligns with the spirit of an institution’s security policy. The latter, then, is more a matter of actual, manifest, day-to-day activity. With this distinction, the author is highlighting a critical distinction that resonates with the topic of this literature review. Throughout the balance of the article, Chadwick uses a variety of engaging headings (“Fort Knox vs. User-Friendly”) to group and address topics such as causes of theft (using statistics collected from the Institute for Financial Crime Prevention), “Red Flags,” creating an Employee Code of Conduct and Business Ethics Policy, as well as practical issues such as library egress controls.

Steven J Herman’s “Developing a Plan for Collections Security: The Library of Congress Experience” (2003) is an insightful walk through his personal experience with the Library of Congress’s comprehensive security plan revision of 1997. He provides a very detailed description of the process by which the Library of Congress outlined their security situation and needs, planned for improvements, and then implemented those improvements.

The article describes the four areas which were considered crucial for developing a satisfactory security plan: Physical security, Preservation, Bibliographic control, and Inventory control. In a nicely systematic fashion, the library then created a schema for prioritizing protection across five tiers of risk and five collections cycles. As an example of how to design security systems, Herman demonstrates exactly how principles of security can be directly represented in a system's design. For the purposes of the topic being considered by this review, this conceptual prototype may prove to be quite valuable and this detailed description even more so.

Herman, subjectively, considers the Library of Congress security plan revision project to have been a success. He mentions a variety of advantages of the new system over the one which it replaced: Namely, that it represents a number of ideas which may be considered tenets of a good security plan, such as "Collaborative effort, Shared vocabulary, an approved and understandable plan, a blueprint for action, and a synergistic approach." Although these are all interesting, evocative, ideas, Herman provides slight evidence and explanation of why they are essential. Nonetheless, this article provides a template for looking at specific standards which meld practice and philosophy, as well as very clearly describing the fact that employee "buy-in" and perception are essential to a successful plan implementation.

Kristin M. Janus's "Securing Our History" (2001) is an historical overview of the library literature and media coverage of thefts from rare book rooms. Using this survey as a sort of rallying cry, she challenges practitioners and scholars to press for more severe

legal penalties, to raise awareness of the seriousness of thefts, to keep inventories up to date, and to incorporate the possibilities of theft into disaster plans.

Focusing upon the twin threats of theft and mutilation, Janus proposes the idea that improved inventory and collection control procedures are insufficient for the task of preventing theft. One way that awareness of the problem was raised arose from the publication of lists of missing and known stolen materials from victimized institutions, but she states that that awareness of – and candor regarding – theft did not eventually begin to spread until as late as 1982: “Better late than never, concern began to mount from this point forward as the reality of library, archive and special collection theft became increasingly acknowledged and efforts to combat the growing problem began to truly increase” (p. 6).

She identifies and categorizes common library thieves, while bemoaning the fact that most U.S. law enforcement agencies apparently do not have the understanding, time, staff or training to properly deal with the theft of unique library materials from their various depositories. This leaves libraries to address the special nature of their own library concerns while, ironically, they are often the “last to know” when a large theft occurs.

She writes extensively about the myths surrounding thieves such as Martin Strich, Ted Donson, and Stephen Blumberg as examples of the fanciful ideas that undercut attempts to publicize and describe the dangers posed by art and rare book thieves, advancing a public and policy-maker perception that clouds any knowledge of the threat being presented. According to Janus, “In the United States, and elsewhere in the world,

some of the most valuable and intrinsically worthwhile materials will most certainly be lost forever if timely action is not taken to seriously minimize occurrences of theft in libraries, archives, museums and special collections” (p. 12). She argues that an increase in the penalties attached to these thefts, reflective of the value of the items stolen, would provide a better deterrent to prospective thieves than that presented under current legislation.

On balance, this article is a nice survey which participates nicely in the stream of scholarship that acknowledges the critical importance of perception in matters of risk, threat, and security assessment.

Thomas Latusek, Jr. is an important voice in the discussion of security matters, and his “Library Security: A Growing Awareness” (2000) is an excellent article which describes incidents with problem patrons in libraries while stressing the importance of security plans. Latusek discusses the current trend toward extended hours of operation for academic libraries and, with such emerging changes in the security landscape in mind, offers first-hand experiences with security planning.

Latusek’s discussion focuses on planning measures primarily as a means to create a heightened consciousness of library security, emphasizing technological questions and policy concerns. In this way, he anticipates more sophisticated ideas such as those of Herman, Janus, and Sowd, who explicitly expanded upon the implications of the interactions between these themes. Alongside others such as Levett (1992) and Shuman (1997), Latusek represents part of the foundation of thought and scholarship in the field.

“As Strong as Its Weakest Link: The Human Element” (2003), by Laurie Sowd, points out that, “Too often, we fail to give full weight to the importance of our people – the human element” (p. 29). Her article looks at the motivations of the staff which is responsible for realizing security plans and policy: Why do they do what they do? What do they seek in a work environment?

Sowd’s idea is that a sense of purpose is one of the most important ways of understanding why security fails or succeeds at its intended mission. She states that the components of a security program are three-fold: staff, technical systems, and policies and procedures, with training “tying these components together.” Given that, in her view, security is reduced (or, I might offer, *elevated*) to its human components, she considers several social and emotional attributes of library staff: as well as the aforementioned “sense of purpose,” she lists social interaction, “Clarity of role,” and opportunities for advancement as the four central areas for evaluating the potential security-related strength of library employees.

As she builds her recommendations for ways to address these ideas in an applied manner, Sowd cites the *United States @ Work 2000* study, and the seven “key ways by which a company can build employee loyalty” (p. 31). Here, the article becomes something of a how-to guide in terms of motivating employees, such as granting additional responsibility and opportunities for advancement.

Sowd provides the example of the Huntington library, where the staff was presented with a security policy that outlined five broad objectives for self-assessment:

1. The library experiences no loss that could have been reasonably expected.

2. Staff perceive that they add value.
3. Visitors perceive that security adds value.
4. Management believes that security is efficient and effective,
5. Security officers believe that the library, itself, adds value to their lives.

Sowd's work is included here because it is an interesting example of holistic thinking in terms of policy meeting practice. She acknowledges the importance of the human factor in security systems and states that, in focusing upon that factor, security systems can be measurably improved.

“Philosophy-related” literature

Stacie Conchie's article, “Trust: Missing Piece(s) in the Safety Puzzle” (2006), does not directly address security, within or without the context of a library setting. But it is worth considering in the body of this review because of her investigation of the human element in designing and considering safety (a ready substitute for security) systems. She focused her article (which, in fact, serves as an introduction to a sequence of other articles) on the issue of trust. She states that “while trust is increasingly recognized as a factor that impacts on safety behavior, the exact nature of trust and its role in shaping organizational safety is poorly understood” (p. 1097). Similar to authors such as Rogers (2007), who are, in fact, librarians, Conchie sees the complex nature of trust and the positive and negative roles that trust can play in shaping an organization's safety (security) culture.

Conchie, like Sowd, sees that researchers and practitioners have started to examine the impact of interpersonal processes on employees' safety-related behavior. In her case, she focuses on trust, defined as "an individual's willingness to rely on another person based on expectations that he or she will act safely or intends to act safely" (p. 1097). Although she uses examples such as the safety analyses of disasters like the North Sea Piper Alpha explosion, the parallels to security system analysis are very clear.

In a manner similar to Herman, Conchie develops the idea that trust is a synergizing element of a system, yet one which has been incompletely investigated and mapped: "One consequence of this absence of direct empirical attention is that the relationship of trust with safety is poorly understood" (p. 1098). In order to correct this, Conchie writes about the three dimensions of trust: trust, mistrust, and creative mistrust, the last of which is precisely the nature of security system design and consideration.

This article is included because of the process-focused manner in which Conchie suggests advancing empirical, quantitative, studies of trust in the workplace: "Through a mapping sentence, the abstract nature of trust, which many researchers grapple with (Gambetta, 1988), can be clearly defined and a move can be made toward a single definition of trust... (A) move away from conceptualizing trust as a single construct and show some of the different effects that trust can have on safety within highrisk (sic) contexts... To achieve this, programs might focus on improving beliefs and feelings about another's trustworthiness" (p. 1103).

Brian M. Owens, the author of "The Safeguarding of Memory: The Divine Function of the Librarian and Archivist" (2003), states as a matter of fact that archivists

and librarians are entrusted with the responsibility of preserving manuscripts, books and electronic format. Beyond this, however, his article describes this function as being almost akin to a kind of spiritual cultural stewardship, and one which is being dramatically challenged by the threats of terror, violence, and cultural genocide which plague the modern world. It is not misrepresenting Owens's thesis to quote him thusly: "In essence we (librarians) are charged with the maintenance and preservation of memory. We have been assigned with a divine act" (p. 11).

His article explores the destructive acts which have destroyed books and manuscripts, "and hence, have assisted in the eradication of social memory" (p. 12). In doing so, Owens outlines not only his somewhat romantic view of libraries, but also the real spiritual undercurrents that support it.

Owens invokes Owen Feltham, who "acknowledged in *The Face of the Book, Unmasked*, the codex, or its primogenitor, the electronic book, sustains the truth; the whole of the Universe is embodied and ignorance is distracted" (p. 34). Despite the lack of concrete empiricism in this article, Owens lends a powerful voice to the discourse of library security and, in so doing, speaks directly to the questions which undergird this literature review.

Gary P. Radford's "Positivism, Foucault, and the Fantasia of the Library: Conceptions of knowledge and the modern library experience" suggests that perceptions of library environments, from both observers and participants, are, historically, informed by a particular kind of positivism. Specifically, Radford proposes that our ideas about neutrality and access to information reflect "twentieth-century" ideas that scientific

knowledge is not only inherently superior to other kinds of knowledge, but should be used as a model for understanding how to construct and manage systems to organize data. Radford, instead, follows the ideas of Michel Foucault to offer the idea that the library can be seen as a dynamic space, one which encompasses a librarian role as both “an eager seeker of knowledge and... as a quasi-mystical guardian of a great temple of knowledge” (p. 409). Although Radford writes in more general terms of the library “experience,” there are clear extensions into particular topics such as library security, especially as framed as a matter of mission.

Eric Sheffield’s “Beyond Abstraction: Philosophy as a Practical Qualitative Research Method” stretches the limits of this paper’s porous perimeters, in that it is even more removed from the matter of library security than almost any other article herein addressed. Nonetheless, the thesis of Sheffield’s work is very evocative and pertinent. *Beyond Abstraction* makes use of a specific example to illustrate Sheffield’s effort to redeem philosophy as a powerful tool for qualitative research. He provides a cogent and comprehensive overview of the idea of philosophy as a social practice, tracing the methodological tools and subject matter involved. Importantly, Sheffield works with the ideas of John Dewey who wrote extensively about the nature of philosophy as being grounded in lived experience. Sheffield’s interpretation of this idea is clear: “Philosophers have the particularly important chore of clarifying our thinking as to constructs that both clarify experience and direct practice. That methodological purpose is important not simply as a means for philosophers to understand concepts, language,

and logic as they operate in real, lived, experience, but it provides a necessary discussion that can become the basis for other kinds of research.” (p. 765)

Sheffield, in other words, sees philosophy as a valuable tool for understanding study and practice and that conclusion finds common voice in the effort represented by this paper. His idea is echoed and amplified by Michelle M. Byrne, author of “Linking philosophy, methodology, and methods in qualitative research.” Byrne extends the idea of philosophy’s utility into explicit categories including phenomenology and hermeneutics, drawing clear lines between the methods and means of philosophy and those of qualitative research. Similar efforts can be found in the writings of Frank Crossan, but it is not the agenda of this paper to outline these terms in exhaustive terms, but it is the agenda to point out that these kinds of connections are known, are accepted to be useful, and are being explored by meaningful scholarship.

Finally, David E. Woolwine, in “Libraries and the Balance of Liberty and Security” (2007), states that, the USA Patriot Act has presented librarians in the United States with a dilemma. According to him, there is a need to balance national security against values embedded in a long-standing American understanding of civil liberty and human rights.

He refers to the discussion of the problem created for libraries by the USA Patriot Act and Foreign Intelligence Surveillance Act by Jaeger, Bertot, & McClure, 2003 and Jaeger, McClure, Bertot, & Snead (2004), Martorella (2006), addressing the idea that the “balance of liberty and security, and how to argue for such balance, remain as permanent features of our times... security ethicists can begin to address this issue by examining

limited and specific responses to the need for balance and then subjecting these responses to an ethical critique” (p. 1).

He presents this kind of critique in an ethical analysis of the deliberations of non-governmental organizations, such as the American Library Association. Woolwine is approaching the exact theme of this review’s topic here, as his is a study in professional ethics related to the reasoning of the ALA as contained in their security and privacy policies.

Woolwine, in his analysis of the ALA, explains the two forms of ethical arguments by the ALA: 1) types of utilitarianism and, 2) forms of rights discourse that are asserted rather than argued for. He sees arguments of both types as being insufficient. In his article, he provides an analysis of modern and postmodern conceptions and applications of the idea of “privacy,” suggesting that a synthesis might be the most useful means for moving into a more functional argumentative space. This amalgam of the modern and postmodern views first argues that autonomous selves require access to information and culture in order to be autonomous -- in order to choose what types of lives they hope to live or in order to give true internal assent to what they take to be truth. Secondly, however, the synthesis relies heavily upon the notion of dialogue.

“The members of modern societies should, inasmuch as they are in fact choosing, or assenting to, their values be sufficiently sophisticated to know what they are choosing, or assenting to, and why. Here there is a need for a public dialogue and for an informed and cultured public. The need for dialogue is grounded, however, in something other than, but similar to, utilitarianism. It is in the public dialogue that one connects up, in critical ways, with larger narratives and where one works to change or refine both oneself and such narratives. Freedom of access to information and to cultural products are required for this dialogue, consistent with

national security needs. This is not an absolutist position on either side” (p. 9).

I provide this lengthy quote, rather than a paraphrase, to provide additional insight into the character of this argument, as well as its content. Woolwine’s focus is upon access rights, rather than security, but he is treading upon the same territory as this review’s topic, especially when he combines this rather philosophical view with a critique of the ALA’s form of reasoning in formulation of policy. He suggests that there is a sort of placatory inconsistency in the ALA policy, something which necessarily weakens the strength of that policy.

Woolwine’s thesis is that the ALA, as a policy-making entity, needs to pursue a vigorous and nuanced internal dialog in order to precisely articulate the reasoning which underlies its policy. This work is an excellent example of the kind of research which addresses my topic.

This literature review provides the context in which this paper operates. Although the precise subject area has yet to be fully charted, these important pieces of scholarship will assist my work by providing examples of methodological approaches, important indicators for additional references, and a sense of the community of scholarship which attempts to investigate intersections of philosophy and practice.

Security as a concept

By its very nature, the American Library Association is the prime creator and arbiter for matters of library policy (at least in this country). Although the earliest attempts to codify policy matters seem to have been quite basic in formulation – The aim of the Association, in that resolution, was to “enable librarians to do their present work more easily and at less expense” (p. 1). – The modern ALA Policy Manual is a fairly extensive document. It is intended to provide a framework for understanding the role and manifest practice of librarianship in the context of American libraries. In pursuit of this goal, the ALA Policy addresses a number of key concerns, including Personnel and Professional Resources, support of legislation which strengthens library services, and matters of Intellectual Property. It also outlines the ALA’s attitude as regards the access to information, both as a sort of spiritual ideal and as a matter of practical application.

It may or may not be an acceptable standard to assume that library security can be seen to succeed or fail in direct correlation to the degree of clarity which supports it, but for the purposes of this paper, I will assume this to be the case. What is certainly acceptable standard is the common use of statements of a kind or like to the ALA Policy. In a slightly revisionist mirror, this policy – and, indeed, all security polices – should be seen as participating in an essential dilemma:

- One: Access to information is about letting people at it.
- Two: Security is about keeping people away from it.

Of course, we know that the reality – even the desired, utopian, reality – lies in the middle of these two points, a floating balance. Just as a chaotic free-for-all of information would mean madness, so would a draconian, glacial, lockdown of information mean intellectual absolute zero. The skill of an information professional lies in developing and explaining the space between the two, for access is about control and control is about security.

So, just what triggers concern about security? There is some truth to the idea that it is the most primal of impulses to protect things of value. Security, following this idea, can be seen as a responsive set of constructs which are designed to allow for this protection.

Security is the condition of being protected against danger or loss. In the general sense, security is a concept similar to safety. The specific nuance between the two is an added emphasis that the former constitutes a state of being protected from dangers that originate from outside. Individuals or actions that encroach upon the condition of being protected are responsible for a breach of security. To elaborate further, the word "security" in general usage is synonymous with "safety," but as a technical term "security" means that something not only *is secure* but that it *has been secured*. Security might fruitfully be compared and contrasted with other related concepts: safety, continuity, reliability. While safety was mentioned above, continuity also has its place as the idea of a given environment possessing a resolute and continuing state – The goal of security is to provide continuity so that the state of a library can be maintained in accordance with its mission. The key distinction between security and the idea of

reliability is that security must take into account the actions of active malicious agents attempting to cause negative or undesired effects.

It is quite often true that people's perception of security is not directly related to actual security. For example, a fear of being a passenger in an airplane is far more common than a fear of riding in a car; however, automobile transportation is generally far more dangerous than travel by plane. A similarly common kind of security misperception is that a tool may be mistaken for the effect, for example when multiple computer security programs interfere with each other, so the user assumes the computer is secure when actual security has vanished. There are a wide-ranging number of non- and irrational security perceptions that color every aspect of everyday life, including the life of a collection or an institution.

Another important facet of security is the phenomenon known as “security theater,” wherein demonstratively ineffective security measures (such as screening of library patrons in based on posted, static, lists of known thieves) are introduced with little real increase in security-- or even with an actual *decrease* in real security.

The interesting nature of security theater, however, is that if it is perceived that there is security then there will be an increase in actual security, even if that perception of security is mistaken. If signage warns that video surveillance is observing an area -- even if there is no actual visual surveillance -- malicious agents will often be deterred by the belief that there may be. Furthermore, when there *is* actual security present in an area, such as video surveillance in a reading area, an alarm system in a special collection, or an anti-theft system such as tattletape, signs advertising this security will increase its

effectiveness, protecting the value of the secured holding or area itself. Since some intruders will decide not to attempt to criminally penetrate such areas, there can actually be less damage to the surrounding environment in addition to protection of valuable objects inside. Without such advertisement, a book-thief might, for example, attempt to remove a book from the building and then flee in response to an alarm being triggered.

In either eventuality, whether or not a negative act has been committed, *perceived security* has the net effect of improving *actual security*. It is important, however, for signs advertising security not to give clues as to how to subvert that security, for example in the case where a home burglar might be more likely to break into a certain home if he or she is able to learn beforehand which company makes its security system.

Philosophy of Security

Security, as a concern, is among the most basic organic impulses. Technically, I've offered several different definitions for what I mean by my use of the term, with the most basic being something along the lines of what can be found in a dictionary (in this case, <http://www.Merriam-Webster.com>, accessed March 12, 2008):

1: the quality or state of being secure: as a: freedom from danger : safety
 b: freedom from fear or anxiety c: freedom from the prospect of being laid off <job *security*> 2 a: something given, deposited, or pledged to make certain the fulfillment of an obligation b: surety 3: an instrument of investment in the form of a document (as a stock certificate or bond) providing evidence of its ownership 4 a: something that secures : protection b (1): measures taken to guard against espionage or sabotage, crime, attack, or escape (2): an organization or department whose task is security.

With this in mind, the other part of my binary realm is that of philosophy. In the simplest terms, I have herein misused the term philosophy to refer to the value theory of security. This is to say, how people positively and negatively value things and concepts, the reasons they use in making their evaluations and the scope of applications of legitimate evaluations across the social world.

Really, what I am talking about here is the idea of a security mission: The policy which reflects the constellation of decisions which address the diverse field of access/prevention and concept/practice. As mentioned previously, the ineffable center and fringe of this field is, in fact, the sphere of human influence and practice, the decisions and actions of real human participants in a security environment. And, not to put too fine a point on it, but this is also the ultimate reality of security that we can see demonstrated in the dynamic between security and security theatre.

Brigham Young University offers a nice example of a library security mission statement thusly: “The mission of the library security department is to protect the patrons, employees and collections of the library; while creating a secure and peaceful environment to enhance educational and professional pursuits of all persons within.”

To take a different approach, consider Beth Patkus, who asks the following questions: “What benefits will there be to collections if librarians, archivists, and security personnel are encouraged to consider security in a more holistic way? Can an understanding by security staff of collection preservation activities make it easier to begin and maintain preventive activities and help create more comprehensive and effective security *and* preservation programs? Why are existing policies to deal with theft and

vandalism so difficult to enforce? Can cooperation between staff responsible for preservation and for security improve this situation?" (p. 68)

Conclusions

This brief paper has presented material which is unified in general subject matter, if not technique. The thoughts represented in the literature review reflect and refract issues of modern security and the policy which precede, support, and follow from them. In reviewing the differing strategies which various authors have employed, one can see similarities in approach: most authors feel compelled, for example, to create a list of security principles. Further, most have created at least one additional list of characteristics, whether as observations or as guidelines, which describe a philosophical or humanistic view of security matters.

The shadow of the current political and social climate is long, indeed, and scholarship of library security reflects the realities of an environment which contains real concerns about terrorism, identity theft, and the loss of privacy and identity in an increasingly technological world. It is perhaps this reality, more than any other, which might explain the motivation to quantify the philosophical and spiritual facets of library science.

Looking forward, we can see that there is still much work to be done in defining this subject area. Comparative studies of the “security principle” lists is one area which might provide fruitful scholarship, as would be an investigation into the budgetary decision-and-implementation processes that are involved in library security policy development. This proposal demonstrates that there is also scholarship yet to be done in outlining a method for evaluating the effectiveness of a security system and, moreover,

that one means of developing such a method would be considering the human elements which are so intrinsic to security interests.

So, to step back, my essential question was this: “What connects philosophy and practice -- What is the point of security policy?”

Woolwine’s two ideas of how people answer the question (Utilitarianism and Rights discourse) is one of the most thoughtful starting points, but I feel like there are a host of other important issues that orbit around this topic:

What is the space between policy and practice? Is it *people*? What kinds of questions should we be asking? What is the value of this inquiry? Why does it *seem* like such an important thing to think about (we hear a lot about policy and mission, after all)? Looking forward, I begin to consider the other places to investigate; places like Gap Theory, Liminal Theory, Metaphor Theory, Risk Assessment Study, and even areas as large as the whole field of Psychology. Needless to say, I am ill-equipped to really, critically, evaluate so many subject areas. However, to beg your indulgence for yet another list, I began to assemble a set of working concepts to use as guideposts in my investigation. Specifically, I believe the following maxims to be true:

- It’s important to separate issues of the current political climate from this particular discourse
- It is critical to know *why* we do things
- There *are* ways of looking at and mapping the gap between policy and practice
- That gap is actually part of a continuum
- We need to be explicit as we write policies

- We need to be iterative and evolving as we write policies
- We need to be collective and cooperative as we write policies
- We need to understand the expectations of readers, patrons, and people as actors
- We need to understand policy to be organic

All of which inexorably moves one to the stance that I need to reconsider the most basic and human processes of assessing risk and security as I try to think about what policy means. So, finally, I arrived at the theory which I have been investigating, perhaps best exemplified by Bruce Scheiner's "The Psychology of Security."

Scheiner's essential observation is that. "Security is both a feeling and a reality. And they're not the same" (p. 1). He explains that the reality of security is a matter of mathematics, a series of calculations based on cost/benefit analysis. These computations are actually rather statistically measurable, but the tricky part of understanding and evaluating security is that reality that it is also an emotional quantity. Furthermore, it is not simply emotional, but, rather, a complex amalgam of judgment, experience, and pre-rational assumptions – often informed by primal urges – which often work in direct opposition to the "statistical reality" of any given circumstance.

Scheiner uses a survey of four fields of research as a map for looking at the issue of the psychology of security: behavioral economics (also known as behavioral finance), psychology of decision-making (especially the idea of bounded rationality), direct research into the psychology of risk, and neuroscience.

Scheiner admits that his proposed unifying field is very large, very complex, and still unclearly-bounded:

“In some ways I feel like a magpie, and that much of this essay is me saying: "Look at this! Isn't it fascinating? Now look at this other thing! Isn't that amazing, too?" Somewhere amidst all of this, there are threads that tie it together, lessons we can learn (other than "people are weird"), and ways we can design security systems that take the feeling of security into account rather than ignoring it” (p. 2).

However, he does an excellent job of building a language for his theory, one which I find very useful. Although the limits of this summary preclude an exhaustive outline of his theory, some of the key ideas include the trade-offs of risk, the physical processes of the human brain in risky situations, and prospect theory. Scheiner uses a variety of specific examples, most notably from the work of authors such as Paul Samuelson and Robert Cialdini.

You, dear reader, will remember at the outset of this paper that vague claims were made about control and access and security. Really, there should have been some claims about preservation thrown in there, explicitly, as well, for there is an important sense in which that is part of the same continuum, as well. But what is the objective? What is the mission? This is purpose of policy and this is the point of Woolwine’s “synthesis.” But, more than a synthesis, I think that there are richer, more fertile, metaphors: Dance, balance, storytelling. Of course, there is more to explain, more to develop, but we can consider ourselves exercised and bettered, perhaps, by this trip, if we can look back over our path and notice the scenery.

This kind of study is important because the issues of risk and security are eternally topical and endlessly poignant. In terms of the design, administration, and management of a library or information-focused environment, risk and security are

subjects which have traditionally factored into decisions about both policy and practice in a variety of manners. This paper suggests that an understanding of these topics is, in fact, central to the study and profession of librarianship. I believe that a profession or vocation requires clarity about its own purpose in order to justify its continued existence, and advancing a body of work which will contribute to that clarity could provide benefits throughout the spectrum of library and library science professionals. One concrete example of the value of this clarity is the matter of employment and compensation for that employment; if librarians can explain why their work matters, it is easier for their institutional and municipal peers and superiors to support that work.

Although perhaps not as ambitious as William McGrath's "Explanation and Prediction: Building a Unified Theory of Librarianship, Concept and Review," we can – and, perhaps, should – embrace his idea of drawing together disparate fields of study for the purposes of advancing the theory of our discipline. While McGrath boldly draws allusions to Copernicus, who followed upon such luminaries of physics as Kepler, Galileo, and Newton, we can consider Woolwine and Scheiner, or Dewey and Ranganathan, as resources to unify a theory of library security.

In exploring the established scholarship of library security, I have to come to see a close correlation between security practices and the philosophies of library and information professionals on the most fundamental level. The link between these two is made manifest in the form of policies. It is without question that all can be improved through further study.

Bibliography

- Alao, I. A. (2004). The Effectiveness of Library Measures Against Theft and Mutilation: An Opinion Survey. *Library & Archival Security*, 19(1): 29-37.
- Allen, S. M. (1998). Theft in Libraries and Archives: What to Do During the Aftermath of a Theft. *Journal of Library Administration*, 25(1): 3-13.
- Antwi, I. K. (1989). "The Problem of Library Security: The Bauchi Experience." *International Library Review*, 21: 363-72.
- Bass, R. W. (1984). "Collections Security." *Library Trends*, 33: 39-48.
- Belanger, T. (1983). "Oberlin Conference on Theft Calls for Action." *Library Journal*, 108: 2118.
- Bello, M. A. (1998). "Library Security, Materials Theft and Mutilation in Technological University Libraries in Nigeria." *Library Management*, 19(6): 379-83.
- Bergerson, J. (1999). *Manual for South Carolina Religious Archives and Recordkeeping*. Columbia, South Carolina: South Carolina State Historical Records Advisory Board.
- Bier, V. M. (2007). Choosing What to Protect. *Risk Analysis*, 27(3): 607-620.
- Billington, J. A. (1996). "Here Today, Here Tomorrow: The Imperative of Collections Security" *American Libraries*, 27: 40-41.
- Boss, R. W. (1984). "Collection Security." *Library Trends*, 33(1): 39-48.
- Brand, M., ed. (1984). *Security for Libraries: People, Buildings, Collections*. Chicago: American Library Association.
- "Library Security." Brigham Young University. 3 April 2008.
<http://www.lib.byu.edu/departs/security.html>
- Brown-Syed, C. (2004). Law Enforcement Agencies and Library Records. *Library & Archival Security*, 19(1): 53-57.

- Brown-Syed, C. (2004). Preparing for the Worst, Planning for the Best: Protecting out Cultural Heritage Disaster. *Library & Archival Security*, 19(1): 73-74.
- Burke, Robert S., and Sam A. Adeloje. (1986). *A Manual of Basic Security*. Leicester, England: ICOM.
- Canal, B.A. (1998). "Libraries Attract More Readers: Investing in Library Safety". *Indiana Libraries*, 17(1): 15-17.
- Chadwick, W. (1998). Special Collections Library Security: An Internal Audit Perspective. *Journal of Library Administration*, 25(1): 15-32.
- Christian, J. F. and S. Finnegan. (1974). "On Planning an Archives." *American Archivist*, 2(4): 573-578.
- Conchie, S. M., Donald, I. J., & Taylor, P. J. (2006). Trust: Missing Piece(s) in the Safety Puzzle. *Risk Analysis*, 26(5): 1097-1104.
- Cox, R. J. (1995). "Collectors and Archival, Manuscript, Rare Book Security." *Focus on Security* 26: 19-27.
- Crossan, F. (2003). Research Philosophy: towards an understanding. *Nurse Researcher*, 11(1): 46-55.
- Cummin, W. B. (1984). "Institutional, Personal Collection & Building Security Concerns." *Security for Libraries: People, Buildings, and Collections*. Edited by Marvin Brand, 24-50. Chicago: The American Library Association.
- Daniels, M. F. and T. Welch. (1984). *A Modern Archives Reader: Basic Reading on Archival Theory and Practice*. Washington D.C.: National Archives Trust Fund Board.
- Dow, C. (1999). "Library Rules, Policies, and Library Security." *Nebraska Library Association Quarterly*, 30(1): 16-26.
- Duggar, D. C. (1999). "Security and Crime in Health Sciences Libraries in the Southern United States." *Medical Reference Services Quarterly*, 18(1): 37-48.
- Ellis, J. Ed. (1993). *Keeping Archives*. Brunswick, Australia: D.W. Thorpe in Association with The Australian Society of Archivists Inc. Impact Printing.

- Erway, R., & Schnaffer, J. (2007). *Shifting Gears: Gearing Up to Get into the Flow*. Report produced by OCLC Programs and Research. Published online at: www.oclc.org/programs/publications/reports/2007-02.pdf.
- Fennelly, L. J. (1983). *Museum, Archive and Library Security*. Boston: Butterworth Publishers.
- Garnet, S. R. (1982). *Protecting Your Collection: A Handbook, Survey, and Guide for the Security of Rare Books, Manuscripts, Archives, and Works of Art*. New York: Haworth Press.
- Genco, B., & Kuzyk, R. (2007). 20 Maxims for Collection. *Library Journal*, 32-35.
- Goldberg, M. (1993). "The Never-ending Saga of Library Theft." *Library & Archival Security*, 12(1): 87-100.
- Herman, S. J. (2003). Developing a Plan for Collections Security: The Library of Congress Experience. *Journal of Library Administration*, 38(1/2): 39-48.
- Hutcheson, C. (1998). Interlibrary Loan Borrowing Policy Comparison. *Journal of Interlibrary Loan*, 8(3): 7-42
- Jackson, M. (1991). "Library Security: Facts and Figures," *Library Association Record*, 93: 384.
- Jaeger P.T., Bertot, J.C., & McClure, C.R. (2005). The impact of the USA Patriot Act on collection and analysis of personal information under the Foreign Intelligence Surveillance Act. *Government Information Quarterly*, 20 (3): 295-314.
- Jaeger, P.T., McClure, C.R, Bertot, J.C., & Snead. J.T. (2004). The USA Patriot Act, the Foreign Intelligence Surveillance Act, and information policy research in libraries: issues, impacts, and questions for libraries and researchers. *Library Quarterly*, 74 (2): 99-121.
- Janus, K. M. (2001). Securing Our History. *Library and Archival Security*, 17(1): 3-15.
- Jenkins, J. H. (1982). *Rare Books and Manuscripts Thefts: A Security System for Librarians, Booksellers, and Collectors*. New York: Antiquarian Booksellers' Association of America.
- Keller, S. R. (1988). *The Most Common Security Mistakes that Most Museums Make*. Deltona, FL: Steven R. Keller and Associates.
- Kelly, Melody. (2003). Revisiting C.H. Milam's What Libraries Learned from the War and Rediscovering the Library Faith. *Libraries & Culture* (a.k.a. *Libraries & the Cultural Record*), 38(4). Available online.

- Kenney, B. J. (2001). Central Libraries in Uncertain Times. *Library Journal*: 36-38.
- Kinney, J. M. "Archival Security and Insecurity." *American Archivist* 38 (1975): 493-497.
- Latuszek, T. (2000). Library Security: A Growing Awareness. *Library & Archival Security*, 15(2): 3-8.
- Lave, L. B., & Apt, J. (2006). Planning for natural disasters in a stochastic world. *Journal of Risk and Uncertainty*, 2006(33): 117-130.
- Lincoln, A. J., and C. Z. Lincoln. (1987). "Library Crime and Security: An International Perspective." *Library & Archival Security*, 8(1/2): 14-7.
- Mason, P. (1975). "Library and Archival Security: New Solutions to an Old Problem." *American Archivist*, 38(4): 477-492.
- Mazur, A. (2004). *True Warnings and False Alarms: Evaluating Fears about the Health Risks of Technology, 1948-1971*. Washington, DC: Resources for the Future.
- McGrath, William. (2002). Explanation and Prediction: Building a Unified Theory of Librarianship, Concept and Review. *Library Trends*, 50(3): 350-70.
- Nilsen, K. (2003). Library Security And Safety Handbook: Prevention, Policies, And Procedures (Book). *Library & Archival Security*, 18(1): 63-64.
- Owens, B. M. (2003). The Safeguarding of Memory: The Divine Function of the Librarian and Archivist. *Library & Archival Security*, 18(1): 9-41.
- Paris, J. (2000). "Conservation and the Politics of Use and Value in Research Libraries," in *Book and Paper Group Annual*, 19: 61-65.
- Patkus, B. (1998). Collections Security: The Preservation Perspective. *Journal of Library Administration*, 25(1): 67-90.
- Patkus, B. (2003). *Assessing Preservation Needs: A self-survey guide*. Northeast Document Conservation Center, MA: NEDCC.
- Radford, G. (1992). Positivism, Foucault, and the Fantasia of the Library: Conceptions of Knowledge and the Modern Library Experience. *Library Quarterly*, 62(4): 408-24.
- Rendell, K.W. (1977). "Problems of Archival Security." *AB Bookman's Weekly*, 59: 3719-3723.

- Renner, Michael (2005) 'Resource Wealth and Conflict', in Worldwatch Institute (ed.) State of the World 2005, New York: W.W. Norton & Co.
- Robertson, G. (2002). Investigating Risk: Assessing and Analyzing Trouble. *Feliciter : Journal of the Canadian Library Association*, (1): 30-32.
- Rogers, M. (2007). Case Study: Insecurity. *Library Journal*. Online.
- Rude, R., and R. Hauptman. (1989). "Theft, Dissimulation and Trespass: Some Observations on Security" *Library and Archival Security*, 12(1): 17-22.
- Scheiner, Bruce. The Psychology of Security. Available online: <http://www.schneier.com/essay-155.html>.
- Schneier, B. (2003). Beyond Fear: Thinking About Security in an Uncertain World. New York, NY: Copernicus Books.
- Scire, T. (2003). What's Next for the Radio Frequency Library. *Library & Archival Security*, 18(2): 51-58.
- Sheffield, Eric. (2004). Beyond Abstraction: Philosophy as a Practical Qualitative Research Method. *The Qualitative Report*, 9(4): 760-769.
- Shuman, B. (1999). Library Security and Safety Handbook: Prevention, Policies, and Procedures. Chicago: American Library Association.
- Smith, F. E. (1984). "Questionable Strategies in Library Security Studies." *Library & Archival Security*, 6(3): 43-53.
- Sowd, L. (2003). As Strong as Its Weakest Link: The Human Element. *Journal of Library Administration*, 38(1/2): 29-37.
- Stielow, F. J. (1989). "Archival Security." *Managing Archives and Archival Institutions*, James Gregory Bradsher, ed. Chicago: University of Chicago Press: 207-217.
- Storey, R., A.M. Wherry, and J.F. Wilson. (1989). "Three Views on Security" *Journal of the Society of Archivists*, 10: 108-14.
- Strassberg, R. (2000). "Library and Archives Security," in *Preservation: Issues and Planning*, ed. Paul N. Banks and Roberta Pilette. Chicago and London: American Library Association: 166-184.
- Taylor, D. (1981). "Enemies of Books." *College & Research Libraries News*, 42(9): 317-9.

- Thomas, D.L. (1987). *Study on Control of Security and Storage of Holdings: A RAMP Study with Guidelines*. Paris: General Information Program and UNISIST, United Nations Education, Scientific, and Cultural Organization, Feb. 1987. PGI-86/WS/23.
- Traister, D. (2000). "Is There a Future for Special Collections? And Should There Be? A Polemical Essay." *RBM*, 1(1):54-76.
- Trinkaus-Randall, G. (1989). "Preserving Special Collections through Internal Security." *College & Research Libraries*, 50(7): 448-54.
- U.S. Department of Defense. Joint Pub 1-02 (DOD Joint Staff Publication No. 1-02, 1994), Department of Defense Dictionary of Military and Associated Terms.
- Van Nort, S. (1994). "Archival and Library Theft: The Problem That Will Not Go Away." *Library & Archival Security*, 12(2): 25-49.
- Viscusi, W. K. (2006). Natural disaster risks: An introduction. *Journal of Risk and Uncertainty*, 2006 33: 5-11.
- Viscusi, W. K., & Zeckhauser, R. J. (2003). Sacrificing civil liberties to reduce terrorism risks. *Journal of Risk and Uncertainty*, 26(2-3): 99-120.
- Walch, T. (1977). *Archives and Manuscript: Security*. Chicago: Society of American Archivists.
- Weiser, C. (2003). Library Collection Security. *Media & Methods*, 39(4).
- Welch, E. (1976). "Security in an English Archive." *Archivaria*, 1(2): 49-54.
- Woolwine, D. E. (2007). Libraries and the Balance of Liberty and Security. *Library Philosophy and Practice*. Online.
- Worldwatch Institute. (2005). *The State of the World*. New York, NY: W.W. Norton & Company.
- Wyly, M. (1987). "Special Collections Security: Problems, Trends, and Consciousness." *Library Trends*, 36: 241-256.
- Zeidberg, D. (1984). *Collection Security in ARL Libraries*. Washington, D.C.: Association of Research Libraries.
- Zika, J. (1999). "Library Security = Eyes Wide Open." *North Carolina Libraries*, 57(3): 118.

Appendix A: Selected policies and guidelines

ACRL Guidelines Regarding Thefts in Libraries. (1994). Association of College and Research Libraries.

<http://www.ala.org/ala/acrl/acrlstandards/guidelinesregardingthefts.cfm>.

ACRL Code of Ethics for Special Collections Librarians. (2004). Association of College and Research Libraries. http://www.rbms.info/standards/code_of_ethics.shtml.

ALA Code of Ethics of the American Library Association. (1995). American Library Association.

<http://www.ala.org/ala/oif/statementspols/codeofethics/codeethics.htm>.

ALA Guidelines for Developing a Library Privacy Policy. (2003). American Library Association.

<http://www.ala.org/ala/oif/iftoolkits/toolkitsprivacy/guidelinesfordevelopingalibraryprivacypolicy/guidelinesprivacypolicy.htm>.

ALA Guidelines for the Security of Rare Books, Manuscripts, and Other Special Collections. (2006). American Library Association.

www.ala.org/ala/acrl/acrlstandards/guidelinessecurity.cfm.

American Library Association Policy Manual. (2007). American Library Association.

<http://www.ala.org/ala/ourassociation/governingdocs/policymanual/librarypersonnel.htm>.