PRESERVING HISTORY, PRESERVING PRIVACY: E-MAIL, ARCHIVAL ETHICS, AND THE LAW

BY JORDON STEELE

ABSTRACT: This paper examines legal and ethical issues surrounding privacy in E-mail. The author attempts to identify the legal and ethical parameters that govern archivists when managing electronic correspondence (E-mail) within archival collections. The author then suggests criteria for organizations and individuals who wish to perform a "privacy audit" on E-mail accounts.

Introduction

In his 2000 Presidential Address to the Society of American Archivists, H. Thomas Hickerson cited electronic records management as one of the major challenges for archivists and records managers of the future.[1] Nearly a decade later, archivists continue to improve upon best practices for capturing, preserving, managing, and accessing electronic records, while creators continue to create electronic records on a daily basis. The adage that "if it's worth keeping, print it out" has been challenged as short-sighted and, in some cases, has tested compliance with the law.[2]

Many archives departments are adding staff for the sole purpose of managing digital resources, while others are sending their current staff to workshops and conferences to improve their knowledge of electronic records management. Practitioners and theorists are forming alliances to develop best practices for digital curation before electronic records of enduring value are lost to staff turnover, technological obsolescence, or the "Delete" key.[3]

Among electronic records, one of the most difficult subsets to manage is E-mail. What began as a way for computer scientists working for the government to exchange data sets and communicate with each other has become the primary means by which our culture exchanges ideas, enacts decisions, and creates records. E-mail messages are the handwritten letters and office memoranda of our era. As a result, archivists have a natural inclination to preserve these electronic exchanges, as they may contain

important information about the decision-making process of the people and institutions whose records they are responsible for maintaining.

On the other hand, the sheer proliferation of E-mail correspondence makes appraising the value of individual E-mails a tall order for many institutions. When confronted with thousands of E-mails, deciding what to keep and what to purge understandably strikes many archivists as an insurmountable task. A constant challenge for many archives is devising an effective way to integrate selective E-mail retention into a department's work flow. For the understaffed and underfunded, the task often is considered so overwhelming that some archives have decided to postpone the formulation of E-mail retention policies with the hopes that a more prominent institution (like the National Archives) will develop a practical solution.

Another important consideration when curating electronic communications is maintaining respect for an individual's privacy. There are both legal and ethical implications archivists must consider when granting access to the records for which they are responsible. Breach of privacy also is of particular concern in light of the volume of E-mail and the manner in which it is being used for public and private communications. E-mail has been widely employed for over 15 years and the number of electronic messages sent daily is difficult to quantify. Despite increasing public concern over the privacy of electronic communication, archivists must make themselves aware of cultural expectations of privacy when providing access to E-mail. Similarly, they must be sensitive to donor concerns over granting access to E-mail correspondence in the process of making his or her larger body of papers available to the research community. In short, as Heather MacNeil describes this condition, archivists have "the unenviable task of reconciling legitimate but conflicting interests—the individual's right to privacy and society's need for knowledge."[4]

The objective of this paper is threefold: to explain the legal and ethical underpinnings of privacy; to suggest reasonable obligations of archivists in upholding privacy; and, to offer "privacy audit" parameters for E-mail accounts.

Privacy and United States Law

In order for archivists to understand fully the issues surrounding privacy expectations and E-mail correspondence, it is helpful to look at the history of privacy and its relationship to United States statutory law and jurisprudence. Unlike some of its peer democracies, the United States Code contains no comprehensive law governing an individual's right to privacy. However, some protections against unauthorized government intrusion into an individual's personal life are embedded, albeit implicitly, in the Bill of Rights. The First Amendment protects an individual's right to freedom of speech, the Fourth Amendment guards against "unlawful searches and seizures," and the Fifth Amendment prohibits self-incrimination.[5] In addition to these constitutional provisions, the United States has assembled a patchwork of privacy laws specific to certain circumstances. The Health Insurance Portability and Accountability Act (HIPAA) and the Family Educational Rights and Privacy Act (FERPA) probably are best known by archivists, particularly those who manage health records and student

files. In the early 1990s, federal legislation was introduced to bolster employee privacy law, but the bill was never passed.[6] The United States' perspective on privacy largely has been developed in the courts. Due to the complexity of privacy law and its variation from state to state, it is important for archivists to familiarize themselves with privacy law in the state in which they work, particularly when dealing with electronic communication like E-mail.

Any analysis of the jurisprudence of privacy should begin with the writings of Samuel D. Warren and Louis D. Brandeis. Precipitated by advances in technology, particularly with the invention of photography and the telegraph, Warren and his law partner, Brandeis, wrote an article that emphasized the importance of preventing unnecessary and unlawful intrusions into the lives of private citizens. "The Right to Privacy," first published in the *Harvard Law Review* in 1890, acknowledged that improvements in the government's ability to monitor its citizens' actions precipitated a need to redefine what constituted a breach of privacy.[7] As such, Warren and Brandeis broadly defined privacy as "the right to be let alone." Because technology only has improved in its ability to monitor the actions and behavior of its citizens,[8] the authors' core arguments provide an important framework for repositioning the role of privacy when providing access to E-mail.

In 1928, nearly 40 years after the publication of "The Right to Privacy," Brandeis, at the time, an associate justice of the Supreme Court, issued an influential dissenting opinion in *Olmstead v. United States*. In it, Brandeis proclaimed the right to privacy "the most comprehensive of rights and the right most valued by civilized men."[9] Brandeis's opinions have given privacy an important legal foundation, one that all information professionals, including archivists, should take seriously when providing access to materials originally meant for private communication and not public consumption.

Despite the transformative work on the part of Warren and Brandeis on the subject of privacy, their argument generally has not applied to Court rulings regarding electronic communication. To constitute a legitimate expectation of privacy, the plaintiff not only must establish that there was a subject expectation of privacy, but also that expectation must be one that society at large would find reasonable.[10] Based on the application of this definition, the courts largely have decided in favor of the employer over issues of E-mail monitoring in the workplace. In *U.S. v. Maxwell* (1996), the court declared that once an E-mail is sent, it is the recipient and not the sender who ultimately controls the item.[11] One early case before the courts, *Smyth V. Pillsbury Company*, found that even if an employer has stated it will not monitor employee E-mail, an employee still has no reasonable expectation of privacy.[12] Such an opinion generally has been followed in other cases before the courts. Exceptions generally favor circumstances where the employee is employed by a government agency, or if the employee conducted communication on E-mail systems not owned and operated by the employer.[13] Private employers almost always are exempt from claims of invasion of privacy, since American law typically reserves human rights for the public sphere only.[14]

Another concern surrounding the topic of privacy is libel. Organizations often tread cautiously with the understanding that the courts may award damages to an individual if it is decided that certain personal information, when made public, damaged the person's reputation. To complicate matters, it has been argued that the violator need

not exhibit intentional defamation in order to be found guilty of libel.[15] However, the courts consistently have ruled in favor of the employer in these cases on the logic that the infliction of emotional distress has not been proven to be extreme.[16]

Notable exceptions to these judicial trends include a handful of cases in which plaintiffs have invoked the National Labor Relations Act of 1935, which bars employers from prohibiting its employees to communicate freely for the purpose of union organizing.[17] In *Knopp v. American Airlines*, the court ruled in favor of the plaintiff on the grounds that by breaching his personal Web space, the employer committed an invasion of privacy.[18] And most recently, in *Quon v. Arch Wireless Operating Company*, the court held that an employee has a reasonable expectation of privacy when there is an informal practice of allowing personal text messaging on company pagers.[19] However, it should be emphasized that these are *exceptions* to the prevailing opinion in jurisprudence; generally, employees surrender their privacy rights once they use company E-mail in the workplace. McEvoy prioritizes privacy protections, from greatest to least protected, as follows: bodily fluids, personal tools provided by the employer (such as lockers, desks, and cabinets), and finally, shared employer tools (including office files and E-mail).[20]

Defining the Public versus Private Sphere

Archivists and records managers face the challenge of balancing privacy expectations with our professional responsibility to preserve records of enduring value. As illustrated in the previous analysis of case law, approaches to the conundrum of E-mail preservation and public access vary widely; however, common guidelines are emerging. Writing for the Web site "Government Computer News" in February 2009, Michael Daconta, former metadata program manager for the Department of Homeland Security, issued a bold proposal for dealing with the proliferation of electronic records in government agencies: keep everything. Daconta's central argument is that "The notion of trying to distinguish what constitutes a federal record could be a dying concept—as opposed to just marking, compressing and saving all non-duplicative data."[21] Michael Lesk[22] and Peter Lyman,[23] both respected scholars on the topics of digital preservation and information technology, provide technological support for this rationale in their studies of the totality of electronic information.

This solution is a seductive one. With the cost of storing electronic data becoming increasingly affordable, the notion of saving everything, formerly the realm of science fiction, has become a less fantastic proposal. However, for this proposal to become a reality among government agencies, important laws that were established to protect the privacy of governmental employees would have to be rewritten. As electronic records proliferate and archival appraisal becomes more challenging, it is important for archivists to be reminded of the legal and ethical theories underpinning what constitutes a record.

Although it was written over 20 years ago—when electronic storage was talked about in terms of kilobytes, not petabytes—Gary M. Peterson and Trudy Huskamp Peterson's book *Archives and Manuscripts: Law* remains an authoritative treatment

of how the law interprets and shapes records management. The authors defined two sets of categories to help archivists appraise what to keep and what to destroy: record versus nonrecord, and official versus personal.

For the sake of efficiency, one legitimately may claim that any material created in the workplace can be considered an organizational record, since the document is being created on the time of the employer. However, Peterson and Peterson argued that not everything created at a job ought to be considered a record of that organization. They enumerated three types of materials that the federal government classifies as nonrecord: reference material, publications, and copies of original records.[24] A commonality of all three categories is that they do not necessarily reflect business transactions; rather, they are materials that support or duplicate those actions.

The debate over what qualifies as "working papers," however, proves to be more complicated. Archivists traditionally have argued that documents without enduring value should not be preserved in perpetuity, lest they distract from the important documents. (This "signal-to-noise" ratio is one of the more persuasive points cited by those who argue for appraising and weeding electronic records like E-mail, even considering the time required to perform these tasks). To combat the accumulation of documents of dubious importance like "scraps of paper with hieroglyphic notes, half completed and rejected drafts, and telephone numbers," Peterson and Peterson provided the National Archives' set of five questions for archivists to ask when determining record and nonrecord status:

1) "Do the papers form a unique part of an adequate record of an agency's organization, functions, policies, decisions, procedures, operations, and other activities?
2) Were the papers controlled, maintained, preserved, processed, filed, or otherwise handled following usual agency methods and procedures?
3) Were the papers produced by an individual in official capacity?
4) Do the papers relate to official functions of the agency?
5) Were the papers communicated or used or intended for communication or use by agency personnel other than the employee who generated them?"[25]

NARA recommends that if any of these questions generated a "yes" response, the document should be considered to have record status.

These criteria prompt a couple of general considerations. The first is that a record is a document that was intended by its creator to be for more than personal use. An internal memorandum is a good example of this type of document: although access was restricted, the document was drafted for other people to read it. The second defining quality of a record is that it directly reflects the actions, policies, and organizational culture of the institution in which it was generated. To use an extreme example, a grocery list prepared by an individual in the course of business may be an ineffective use of work time, but it is not an institutional record. To use a more complicated example, it could be argued that a form of correspondence—print or electronic—whose subject matter is personal and irrelevant to the mission and activity of an institution is a nonrecord, even if it was sent during the course of business.

Although the National Archives' questions are posed for public agencies that have strict laws governing the accountability of publicly-funded agencies, one might apply them beyond their immediate use. The five preceding questions can help

archivists working for nongovernmental and private organizations determine what sorts of documents generated by their parent institutions are worth saving and restricting. Even if a private organization considers everything created by its employees in the course of a workday to be its property, if the document does not reflect critical actions and activities of an institution, the case for permanently retaining that document and making it available to future generations of researchers becomes much more difficult to make. There are just too many real records worth keeping to spend time maintaining nonessential, nonrecord material.

Ethical Issues for Archivists Concerning Privacy

Any profession distinguishes itself from mere occupation by inviting its members to adhere to a code of ethics. Ethics go beyond the letter of the law to reflect the moral principles that support and add value to the professional services provided. As detailed above, with limited exceptions, individuals can expect few legal protections from the ways in which their electronic communication is archived and subsequently used. Archivists have an opportunity to fill this legal void. For guidance, they can look to professional codes of responsibility, but they also can draw upon broader intellectual discussions regarding the privacy expectations of private citizens.

In the age of on-line scrutiny, it is common to encounter public expectations that every move will be cataloged, chronicled, and communicated on-line. Helen Nissenbaum, professor at New York University and senior faculty fellow of the Information Law Institute, rejects this view, arguing that public policy should accommodate the sophisticated assumptions people hold about the ways in which they control access to what John Palfrey calls their "digital dossier."[26] Nissenbaum refers to this context-based understanding of privacy as "contextual integrity."

Contextual integrity moves beyond the textbook definition of what is and is not private. Rather, the concept "involves a far more complex domain of social spheres (fields, domains, contexts) than the one that typically grounds privacy theories, namely, the dichotomous spheres of public and private."[27] Contextual integrity is interested in more than the various statutes that protect privacy. Rather, Nissenbaum's research analyzes the cultural norms that govern what is and is not an acceptable use of private information.

Negotiating divergent concepts of privacy often is difficult. One particular area of contention that Nissenbaum cites is on-line privacy in the workplace.[28] Before the digital age, it was not possible or practical for employers to monitor or record many employee activities and behaviors. Now, with advances in technology and the shift from virtually all activity in a workplace from off-line to on-line, employer surveillance of employees' on-line activity has increased steadily.[29]

Nissenbaum argues that "norms of information flow" are essential to understanding contextual integrity.[30] There are appropriate and inappropriate venues for sharing private information—and, much like citizens in the era of Brandeis's seminal remarks on privacy rights—individuals should control that flow. A violation of privacy, Nissenbaum argues, depends on a range of factors, in particular the situational circumstances

under which the potential breach has occurred.[31] Archivists and records managers can apply contextual integrity to their daily obligations by endeavoring to understand the circumstances under which private communication was created, and to be sensitive to personal and cultural norms governing the flow of information.

In addition, the establishment of robust ethical obligations has added benefits for information professionals. In arguing for a mature approach to ethical behavior among librarians, Randy Diamond and Martha Dragich encourage their colleagues to "articulate the principles and practices ensuring that members of the profession function at the highest level."[32] This acceptance of professional responsibility not only better serves the patron, but it also helps to promote the "professional viability" of librarianship when compared to more established professions like medicine and the law.[33] By taking ethics seriously, librarians have emerged as trusted leaders within the community.

American archivists have a similar, though less established, professional code of ethics to that of librarians. While neither are as proscriptive (nor as convoluted) as the American Bar Association's Model Rules of Professional Conduct,[34] the Society of American Archivists' (SAA) Code of Ethics outlines how its members should serve their patrons and their profession ethically. The SAA Code of Ethics describes archivists' ethical obligations regarding privacy as follows:

> Archivists protect the privacy rights of donors and individuals or groups who are the subject of records. They respect all users' right to privacy by maintaining the confidentiality of their research and protecting any personal information collected about them in accordance with the institution's security procedures.[35]

SAA provides little advice on this issue beyond this one-sentence charge. For this reason, it is helpful for archivists to be aware of other professional literature on privacy, and more broadly, to understand the importance of ethics in developing a practical framework for respecting privacy.

Glenn Dingwall's article on archival codes of ethics is one exception. In "Trusting Archivists: The Role of Archival Ethics Codes in Establishing Public Faith," Dingwall describes the primary tension between an archivist's professional responsibility to provide access to information while protecting privacy and serving the interests of the parent institution.[36] In real-life scenarios, these responsibilities may have conflicting interests.

Dingwall proposes two frameworks useful for understanding archival ethics: deontological and teleological.[37] Deontological theory, popularized by philosophers like Kant, posits that moral acts are applied universally, regardless of outcome. Generally, Dingwall argues, archival ethics tend to follow the Kantian model.[38] Teleological ethics, on the other hand, are carried out to produce the best possible outcome for all parties involved. Any practicing archivist likely could cite an instance in which teleology has played a role in departmental decision-making.

Understandably, the multiple relationships archivists maintain on a daily basis may create friction among these ethical frameworks. One might argue that archivists should take a teleological approach to privacy: providing access to information to potentially thousands of researchers trumps the injury to one individual if that information is sensitive to him or her. On the other hand, arguing from the deontological perspective,

one might submit, like Brandeis, that privacy is an inviolate right that should be respected and upheld at the expense of all other issues. It is likely that archivists must and will call on both philosophical arguments depending on the situation. On the whole, Dingwall argues that these are the very sorts of issues with which archivists should wrestle, because public acknowledgement of ethical obligations helps indicate to the public that archivists take these issues very seriously.[39] This, in turn, suggests to the public that archives is a serious profession, willing and capable to debate, and shape, matters of larger cultural implication.

A reasoned, intelligent response to privacy concerns also might position archivists to become trustworthy advisers as nonarchivists increasingly assume greater responsibility for curating their personal information. Technological innovation has yielded more tools and services that allow nonprofessionals to preserve digital information. While it has been argued persuasively that many of these tools are not ideal solutions to ensure the sustainability of digital objects, the reality is that people increasingly are taking responsibility for saving what they would have otherwise discarded or surrendered to an archives.[40] Furthermore, research suggests that average people indeed are cognizant of digital preservation challenges traditionally thought to be merely the concern of information professionals.[41] As digital curation becomes a more distributed cultural practice, archivists very well may shift from gatekeepers to advisers. In the wake of this trend, there likely will emerge a need for archivists to display a proficiency in the intricacies of not only the technological concerns with long-term digital preservation, but also the ethical considerations.

Developing a "Privacy Audit" of E-mail Accounts

As mentioned above, although private institutions lawfully may be permitted to declare all of their employees' documents available for permanent retention, both practical and ethical reasons complicate this broad-brush approach. From the practical perspective, simply keeping everything makes retrieving relevant records more difficult. And ethically, institutions would do well to consider and respect the assumptions of their employees that not everything they create during a work day is subject to scrutiny by their employers and, later, outside researchers.

Therefore, it is worth establishing a model to determine to what extent work E-mail accounts do contain material that may violate both legal and ethical rights to privacy. A useful start in developing a series of questions to consider is the National Archives' list of questions to determine a record status of a document. Modifying this list, one can create a list of questions for records managers, archivists, and individual records creators to ask when auditing E-mail accounts for private and sensitive information:

1) Does the E-mail contain sensitive identification information, such as social security numbers, dates of birth, or credit card information?
2) Does the subject of the E-mail reflect official institutional business?
3) Does the E-mail contain any flags that indicate its creator considered it confidential? This can include a header as formal and declarative as "CONFIDENTIAL"

as well as more subtle indications of confidentiality, such as "Please refrain from mentioning this information to anyone. . . ."

4) Is the E-mail a link to a resource (a Web site, news story, or other on-line resource) that exists outside of the institution's Web site?
5) Does the E-mail include a file attachment that does not relate to official institutional business?

If any of these questions are answered positively, the E-mail may be of nonrecord status and may include private information that its creator never intended to disclose. Therefore, the E-mail may be considered a candidate for restriction or disposal. This model is flexible enough to be applied to a range of situations, whether for personal papers or organizational records. It also has the potential to keep pace with innovations in electronic communication, including chat logs, blogs, social networking sites (like Facebook), and microblogging services (such as Twitter). With the understanding that this type of granular appraisal is, in practice, difficult for many archives departments, some of these questions may be automated. For instance, search parameters may be applied to textual patterns in records management systems such as the National Archives' ERA system[42] and products approved according the Department of Defense 5015.02-STD Records Management Application Design Criteria Standard,[43] which can automate privacy audits.

Conclusion

As E-mail communication proliferates, there is legitimate concern that the amount of electronic documents may preclude substantive appraisal on the part of records managers and archivists. After all, appraisal is but one of an archivist's duties. However, the right to privacy is a core liberty enjoyed by free societies and an individual's expectation of privacy merits the respect of archivists. Practically speaking, there are ways in which privacy concerns can be mitigated. Perhaps the most important tool is employee education. Reminding an employee to use E-mail prudently may help reduce the likelihood that he or she will use E-mail to communicate a private matter. Also, clearly stated retention policies can help communicate the mission of an organization's records policy and retention schedules to its employees. If an employee is aware of the types of documents an institution permanently retains, the employee can keep this in mind when communicating over E-mail. Furthermore, if an individual has set up personal folders to organize E-mail, identifying groups of sensitive E-mails is much easier for the records manager. It may be useful, therefore, for an institution to establish guidelines to help employees more effectively organize and manage their E-mail. Finally, privacy audits like the one suggested in this essay can provide empirical data that may serve to allay employees' fears that their work E-mail contains sensitive information at all.

Understanding the legal and ethical issues governing privacy can help archivists avoid potential litigation and public scorn when preserving and making accessible E-mail of an institution's employees. Moreover, exhibiting sensitivity to and mastery of the issues regarding privacy in E-mail can help archivists cultivate trust and promote

the seriousness of the professional role of archivists as society's stewards of history, both in analog and digital form.

ABOUT THE AUTHOR: Jordon Steele is archivist at Biddle Law Library, University of Pennsylvania Law School. He received his graduate degree from the School of Information and Library Science at the University of North Carolina–Chapel Hill. While his article analyzes the law's relationship to primary source material, Jordon is not a lawyer and his article is not offering legal advice.

NOTES

1. H. Thomas Hickerson, "Ten Challenges for the Archival Profession," *American Archivist* 393 (2001): 7.
2. While recent laws governing electronic records have expressly avoided a preference for preserving records in print or electronic format, preserving the record in its native format is likely the easiest way to verify its authenticity because of time stamps, digital signatures, and other evidentiary metadata that automatically are preserved in a digital file. Should an organization choose to convert an electronic record to print format, additional safeguards must be met in order to preserve its authenticity. For further analysis of electronic records management and the law, see David O. Stephens, *Records Management: Making the Transition from Paper to Electronic* (Lexena, Kan.: ARMA International, 2007): 84–92.
3. Three examples of such partnerships include the InterPARES project (http://www.interpares.org/), DigCCurr (http://www.ils.unc.edu/digccurr/), and the European Union's MoReq metadata specifications for electronic records management (http://www.moreq2.eu/).
4. Heather MacNeil, *Without Consent: The Ethics of Disclosing Personal Information in Public Archives* (Metuchen, N.J.: The Society of American Archivists, 1992): 5.
5. "Legal Perspectives," *Privacy & Confidentiality Perspectives: Archivists & Archival Records*, ed. Menzi L. Berhnd-Klodt and Peter J. Wosh (Chicago: The Society of American Archivists, 2005): 13–14.
6. Mark S. Kende, "The Issues of E-mail Privacy and Cyberspace Personal Jurisdiction: What Clients Need to Know About Two Practical Constitutional Questions Regarding the Internet," *Montana Law Review* 63:2 (2002): 307–308.
7. Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy," *Harvard Law Revie*w 4:5 (1890): 193.
8. Heather MacNeil, *Without Consent: The Ethics of Disclosing Personal Information in Public Archives* (Metuchen, N.J.: The Society of American Archivists, 1992): 2.
9. *United States Reports,* 277: 471.
10. Mitchell Waldman, J.D., "Expectation of Privacy in Internet Communications," *American Law Reports* 5th:92, ed. Jason B. Binimow et al. (Rochester, N.Y.: Lawyers Co-operative Pub. Co., 2001): 22.
11. Ibid., 23.
12. Sharlene A. McEvoy, "E-mail and Internet Monitoring and the Workplace: Do Employees Have a Right to Privacy?" *Communications and the Law* 24:2 (2002): 76.
13. Waldman, 25.
14. Karen Eltis, "The Emerging American Approach to E-mail Privacy in the Workplace: Its Influence on Developing Case Law in Canada and Israel: Should Others Follow Suit?" *Comparative Labor Law and Policy Journal* 24:3 (2003): 492.
15. William L. Prosser, "Privacy," *Privacy and Confidentiality Perspectives: Archivists and Archival Records*, ed. Menzi L. Berhnd-Klodt and Peter J. Wosh (Chicago: The Society of American Archivists, 2005): 50.
16. Jay M. Zitter, J.D., "Claims for Vicarious and Individual Liability for Infliction of Emotional Distress Derived from Use of Internet and Electronic Communications," *American Law Reports* 6th:30 (Rochester, N.Y.: Lawyers Co-operative Pub. Co., 2008): passim.

17. McEvoy, 73.
18. Kende, 306–307.
19. Mark E. Schreiber and Barbara A. Lee, "New Liabilities and Policies for Incidental Private Use of Company Electronic Systems and PDAs," *The Computer and Internet Lawyer* 27:7 (2009): 17.
20. McEvoy, 83.
21. Michael Daconta, "One Way to Solve the Federal Records Puzzle," *Government Computer News*, 4 February 2009, <http://gcn.com/Articles/2009/02/09/Reality-check-The-records-puzzle.aspx> (28 June 2009).
22. Michael Lesk, "How Much Information is There in the World?," 1997, <http://www.lesk.com/mlesk/ksg97/ ksg.html> (28 June 2009).
23. Peter Lyman and Hal R. Varian, "How Much Information 2003?," <http://www2.sims.berkeley.edu/research/ projects/how-much-info-2003/> (28 June 2009).
24. Gary M. Peterson and Trudy Huskamp Peterson, *Archives and Manuscripts: Law* (Chicago: The Society of American Archivists, 1985): 13. Available at: <http://www.archivists.org/publications/epubs/Archives&Mss-Law.pdf>
25. Ibid., 15.
26. John G. Palfrey and Urs Gasser, "Dossiers," *Born Digital: Understanding the First Generation of Digital Natives* (New York: Basic Books, 2008).
27. Helen Nissenbaum, "Privacy as Contextual Integrity," *Washington Law Review* (2004): 106.
28. Ibid., 115.
29. McEvoy, 69.
30. Nissenbaum., 115.
31. Ibid., 127.
32. Randy Diamond and Martha Dragich, "Professionalism in Librarianship: Shifting the Focus from Malpractice to Good Practice," *Library Trends* 49:3 (2001): 396.
33. Ibid., 396.
34. "Model Rules of Professional Conduct," <http://www.abanet.org/cpr/mrpc/mrpc_toc.html> (28 June 2009).
35. "Code of Ethics for Archivists," <http://archivists.org/governance/handbook/app_ethics.asp> (14 March 2009).
36. Glen Dingwall, "Trusting Archivists: The Role of Archival Ethics Codes in Establishing Public Faith," *American Archivist* 67 (2004): 12.
37. Ibid., 15.
38. Ibid., 15.
39. Ibid., 29.
40. Richard J. Cox, "Digital Curation and the Citizen Archivist," 27 May 2009, <http://d-scholarship.pitt.edu/2692/> (7 December 2009).
41. Carolyn Hank et al, "Blogger Perceptions on Digital Preservation," *Proceedings of the 7th ACM/IEEE-Joint Conference on Digital Libraries* (New York: Association for Computing Machinery, 2007): 477.
42. "ERA System Design Information and Documentation," <http://www.archives.gov/era/about/documentation.html> (7 December 2009).
43. "Joint Interoperability Test Command: Records Management Application (RMA): DoD 5015.02-STD RMA Design Criteria Standard," <http://jitc.fhu.disa.mil/recmgt/standards.html> (7 December 2009).