Managing Email and E-Records

Unique Challenges for State and Local Governments

Randolph Kahn, ESQ.
Barclay T. Blair

City Plans to Archive Email
Fredericksburg Free Lance-Star, August 2003[1]

Meltdown at County Recorder's Office
Headliner News, August 2003[2]

Staff Grilled on Records Fray
Gurnee Review, October 2003[3]

FOI: E-mails Should Be Public
Record-Journal, October 2003[4]

E-Mail Gray Area of Virginia's FOI Act
Times-Dispatch, October 2003[5]

State Sued For Deleting E-Mails
Sacramento Bee, February 2003[6]

County Can't Deliver E-Mail to Public
St. Petersburg Times, September 1999[7]

Records Purged From Computer
Fayetteville Online, August 2003[8]

Not a legal opinion or legal advice.

WHERE LAW & TECHNOLOGY MEET

KAHN CONSULTING INC.

157 LEONARD WOOD NORTH • HIGHLAND PARK IL • 60035
PHONE: 847.266.0722 • FAX: 847.266.0734 • EMAIL: INFO@KAHNCONSULTINGINC.COM

I. Introduction

State and local governments, like many any other organizations, have a legal obligation to properly retain and manage certain records relating to their operations and activities. However, unlike most organizations, state and local governments also have a legal obligation to provide the *public* with *access* to many, if not most, of the records that they create and are required to retain. The principle of access is fundamental to information and records management at state and local governments, and has been codified in state "public records, "open records," open meetings," "freedom of information" ("FOI") and similar statutes across the country. Such statutes have existed for many years (for example, the Arkansas Freedom of Information Act[9] was passed in 1967 - the same year the federal FOI law went into effect), and the courts in many states have upheld the public's right to access certain state and local government records long before the existence of such laws.[10] Over the years state and local governments have developed detailed procedures and systems for fulfilling public access requirements.[11]

However, the adequacy of these procedures is increasingly being challenged by a growing reliance upon email and other information technology to conduct the business of government. While governments have adopted email and information technology with much the same enthusiasm as private entities, their unique legal obligations also create unique records management challenges. While the Internet allows many state and local government services – such as the issuance of permits and licenses – to be delivered more efficiently and cost effectively, the use of the Internet to provide access to public records raises a host of legal issues. In a post-9-11 world, many public records (such as those containing information about public utilities or roadways) that seemed innocuous in past take on new significance and require fresh investigations into balancing the public's right to know, personal privacy, and state security. Many states are currently re-examining the way that they provide access to such records as a result.[12]

In 2002, the US federal government conducted a major study of how well it was managing electronic records. The study found major flaws in the government's ability to properly retain and manage email and other digital information, stating that "records management guidance is inadequate in the current technological environment of decentralized systems creating large volumes of complex electronic records."[13] State and local governments face the same challenge, and in many cases have substantially smaller resources at their disposal to address it adequately. Further, state laws may mandate that email and e-records be made available to the public irrespective of budget restraints or technological limitations.

The public's right to access public records is only as real as the controls that governments have in place to ensure that records are first retained and managed properly, and then remain available for future access and retrieval. The growing volume, complexity, and diversity of email and other digital information in the possession of state and local governments makes this task more difficult than ever before.

This paper identifies key issues facing state and local governments in the management of email and e-records, and explores ways that these issues can be addressed through policy and technology-based controls and management.

2. E-Mail & E-Records Legal Foundation

State and local governments, like organizations in the private sector, have invested heavily in email systems and other types of information technology. Analysts have estimated that, despite tight budgets overall, state and local government spending on IT is growing (from $40.4 billion in fiscal 2003 to $41.5 billion the following year, according to one estimate).[15] Although this spending is undoubtedly being driven by the same factors as those that drive IT investment in the private sector – operating faster, better and cheaper – state and local governments are also being driven by a general movement towards electronic government.

The Government Paperwork Elimination Act (GPEA),[16] signed into law in 1998, was a major force in ushering in this movement. GPEA, among other things, clarified that federal agencies could use electronic records and signatures, and moreover required agencies to provide citizens with the option of transacting business with them electronically by 2003. Although state agencies were not bound by GPEA's mandate, many state governments have adopted similar "e-government" initiatives. For example, Louisiana opened its "Louisiana E-Mall" in 2001, a central website for state citizens to get information and conduct electronic transactions with a variety of agencies.[17] Many states have similar online services.

"The management of e-mail systems touches nearly all functions for which a government agency is dependent on recordskeeping: privacy, administration, vital records management, administrative security, auditing, access, and archives. The need to manage e-mail messages and systems properly is the same as for other records keeping systems--to ensure compliance with California laws concerning the creation of, retention of, and access to public records."

State of California Electronic Records Management Handbook[14]

Another law, the Uniform Electronic Transactions Act ("UETA"), versions of which have been passed by a majority of states,[18] clarified the legality of electronic records and signatures within state law, and as a result has worked to promote the use of, and reliance upon, electronic records by state and local government. At the same, time, many states have amended their Freedom of Information laws, and similar statutes, to make clear that citizens may request access to records that are electronic form.

The requirement for state and local governments to retain records is typically found in state "public records acts" or similar statutes.[19] Such laws provide a definition of "record" that places the emphasis on the value of the information in the record, and not on the format of the record. In some cases, such as in Illinois[20] and Texas,[21] such definitions specifically include e-records; in other cases the definition has been interpreted by the state to include all electronic information.

Many states provide guidance and policies that further clarify the interpretation of such definitions and their application to the retention and management of email. For example, New York State clarifies that "e-mail messages are official records when created in the course of business and retained as evidence of official decisions or actions."[22] The Florida Department of State's email policy makes clear that "the information generated on e-mail is a public record subject to public inspection and is not confidential, unless specifically cited by statute."[23] Colorado states that agencies must "take appropriate steps to treat the Electronic Messages just as they would any other form of information."[24] In Maine, "e-mail is subject to the same retention requirements as is paper correspondence."[25] In California, email is "a record if it meets the recordskeeping criteria established within an organizations records management plan."[26] In Texas, "all e-mail sent or received by an agency is considered a state record."[27]

The use of email and other information technology, and the requirement to retain and manage email as a record, has impacted state and local government information and records management in several major ways, including:

- **Retention and access may be harder to guarantee.** Capturing, retaining, and maintaining the integrity and accessibility of electronic records over time is simply more challenging than with paper records. Special knowledge, hardware, software, and procedures are required. State and local governments that use email for official purposes and without a corollary investment in e-records initiatives may be at risk of failing to meet their legal recordkeeping obligations.
- **The volume of information is itself a threat.** Information technology allows organizations to harness information in new and powerful ways. However, it also results in the creation of more recorded information than ever before. In 2003, 800 megabytes of new information was created for each man, woman and child on the earth – with 92% of it stored on magnetic media, primarily hard drives.[28] The growing volume of email and other electronic records can make proper records management a monumental task, particularly when public access requests are made for large volumes of electronic records and state and local governments have not invested in the search and retrieval technology that would expedite the fulfillment of such requests.
- **New types of records are created**. Information technology creates unique forms of records that require special hardware or software in order to be retrieved and viewed. State and local governments generating proprietary electronic records from e-procurement, payroll, and other applications must ensure that they can cost-effectively find, retrieve, and provide access to such records as required by law.

3. Classifying and Managing Electronic Records

State public records laws (including those laws that specifically apply to local governments), generally are built upon the principle that *all* government records should be available to the public. From there, certain types of records are exempted. For example, the California law quoted at the beginning of this paper states that "every person has a right to inspect any public record, except as hereafter provided," and goes on to list several types of records that are exempt."[30] This does not mean, of course, that every piece of information generated or received by state and local governments must be retained. In fact, a major tenet of most state records laws is that the state is able to lawfully dispose of records according to a published retention schedule and related procedures.

Exempting certain records from public access is generally based on the reasoning that the public's "right to know" is overruled by other rights or obligations, such as protecting personal privacy, not compromising law enforcement activities, and keeping trade secrets confidential. For example, the Illinois Freedom of Information Act provides 36 categories of exceptions, which fall into six general categories: Personal Privacy, Law Enforcement, Education, Legal Proceedings, Internal Operations, Business, and Finance.[31] Other states use similar exceptions.

"When agencies decide to upgrade or obtain a new computer system, they're looking at the most effective way to process and store knowledge. The demands of the public records law aren't generally considered early during the process."

"County Can't Deliver Email to Public," St. Petersburg Times[29]

Although such exceptions may seem straightforward on their face, in practicality, determining which records are subject to public access is often a complex and expensive process, especially in the electronic world. In particular, balancing the protection of personal privacy with the public's right to access is a growing challenge in an environment where state and local government employees increasingly rely on email to conduct government business. This is explored in detail below.

Like most private organizations, state and local governments have a need to classify and categorize records according to business, legal, and other criteria in order to ensure that they are properly managed and retained for the period required by practice or law. There is a number of information technology tools designed to assist organization with these tasks. However, state and local governments also have unique classification needs, driven by their mandate to provide public access to certain records, and to withhold other records. This additional layer of classification, and the legal complexities that it entails, require state and local governments to seek out software applications and other tools that meet their specific records management needs, which include the following:

- **Classifying records when they are created**. State and local governments that fail to adequately classify and otherwise identify public records at the time of their creation and/or retention and storage are inviting expensive problems down the road. Up-front classification can minimize the impact of broad public records requests by making the retrieval of relevant records faster and more accurate.
- **Provide ready access to redacted records.** Documents and other records often contain information that is subject to public access and information that is exempt. As such, state and local governments require systems that allow records provided for public inspection or copying to be redacted in a manner that protects the integrity of the original and ensures that protected information is not revealed. Certain types of records, such as databases, and data streams generated from online transactions, may be difficult to properly redact and specialized tools for doing so may be required.

- **Classify information that must be publicly accessible, but for which special procedures for access may be required or advisable.** This includes information regarding public utilities and other infrastructure that is subject to public records laws but which also raises security and other important concerns.
- **Classify information that may require case-by case review.** Some state public records laws require case-by-case review of information before it can be released to the public. For example, until recently in Wisconsin, requests for most of the records within the personnel files of public employees could not be released before the employee was notified.[32] Classifying such information can speed the process of review and expedite the public access request.
- **Provide cost-effective copying capabilities**. Many state and local governments have a mandate to provide citizens with copies of public records at reasonable cost. This mandate can only continue to be fulfilled in the digital world if state and local governments have tools which allow them to cost-effectively retrieve and provide full and accurate copies of electronic records required to be released.

4. Providing Access: Inspection, Examination and Copying

State and local governments face the challenge of providing the public with adequate access to email and e-records – a challenge that will only grow in complexity and cost as governments increasingly rely on information technology.

Some state and local laws addressing public records laws allow flexibility in how agencies can comply with public access requirements, whereas others provide detailed procedures and requirements. For example, North Carolina's Public Records Act (G.S. § 132) states that "no public agency shall purchase . . . any electronic data-processing system for the storage, manipulation, or retrieval of public records unless it first determines that the system will not impair or impede the agency's ability to permit the public inspection and examination, and to provide electronic copies of such records."[34] This statute and its related guidelines provide detailed requirements related to the operation and management of such systems. Other states provide similar guidance, and recommend or require adherence to industry standards for e-records management systems (such as AIIM TR31-1992, in the case of Illinois).[35] In California, agencies are provided with detailed guidance on the selection, configuration, and management of government email systems, including the requirement that such systems "should retain all data and audit trails necessary to prove its reliability as part of the normal course of agency business," and that "the record copy of a message is identified and maintained appropriately." [36]

"Instead of obtaining a copy of all e-mail files, county staffers suggested that residents interested in public officials' e-mail would need to sit at each official's computer and manually check the e-mail received."

"County Can't Deliver Email to Public," St. Petersburg Times[33]

Irrespective of specific guidance provided by law there are several issues that all state and local governments must consider when developing procedures for the inspection, examination and/or copying of public records. These issues are explored below.

Search and Retrieval

Although many organizations of all types are struggling to address the realities of doing business electronically, in the often politically-charged environment of state and local government, coordinating efforts to provide public access to electronic records can be especially challenging – especially when the IT budgets available to many companies are not available to state and local government IT departments.

"Department official say that . . . email wasn't turned over . . . because the agency didn't have a system in place to uniformly search electronic files."

"E-mail Retrieval to Cost State Unit $10,550," Des Moines Register[37]

For example, a local newspaper in Iowa recently used that state's Open Records Law to request access to all email messages possessed by the governor's office that related to a bonus paid to a state official.[38] Employees in the governor's office were instructed to search their computers for relevant email, and less than a dozen messages were provided. The governor's office subsequently agreed to search the backup system for relevant email messages. However, before the search was conducted, the backup tape potentially containing relevant email messages was purged according to a 30 day backup tape recycling policy. When the paper alleged that allowing the tapes to be purged was tantamount to deliberate destruction, a new search was conducted by the state's information technology department. This search – conducted at an estimated cost of more than $10,000 – resulted in hundreds of email messages being turned over. The newspaper complained

that the new search results were still largely irrelevant to their investigation. Another state agency involved in the case failed to provide any email at all because they lacked the capability to do so.

This case is not unique. Across the country many state and local governments struggle to respond to requests for email and other electronic records in a timely, cost-effective, and comprehensive manner. And, as email use and volume continues to grow, the problem is likely to only get worse before it gets better.

Many of the problems faced by state and local governments in this regard could be minimized by the use of tools designed to enable the central coordination of efforts to accurately search, retrieve, and produce relevant email messages. State and local governments should investigate available search and retrieval tools available, and ensure that existing policies, reporting relationships and organizational structures enable a coordinated and comprehensive approach to finding and producing required email and other electronic records.

Methods of Access: Onsite Computers

In Topeka, Kansas, citizens can go to the city council office and use a computer terminal to view certain city procurement records. When the program was first instituted, access was unsupervised, but city official grew concerned about the possibility of information security breaches and began charging citizens $13 per hour to cover the cost of a supervisor to oversee the use of the terminal.[40] Many other local governments fulfill their open records obligations in this way. There have even been accounts of local governments inviting citizens to sit at officials' desks and browse through their email program as a means of fulfilling public access mandates.[41]

As Topeka city officials suspected, providing access to computers that are unsequestered from mainline, operational government systems does present major information security risks and other problems. The use of such techniques should only be considered as a temporary, ad hoc solution. Providing access to public records on onsite terminals can be a viable strategy, if several factors are considered, including:

"According to the survey, [a state official] swore at [the] student . . . when she requested public records. The survey also said [the official] grabbed her arm and threatened to call police."

"Few Connecticut State Agencies Comply With Records Laws," Associated Press[39]

- **Segregating public records access terminals and systems**. Ideally, access should be limited to separate, self-contained systems that contain copies of the public records redacted as required. The separation of public access systems from mainline system will help to prevent the authorized access of non-public records and protect operational systems for possible corruption and performance degradation due to malicious or inadvertent acts of those using the terminals.
- **Limit searches**. Limit the ability to search records on the public terminals only to those records the public are entitled to view.
- **Protect from alteration**. Where possible, present records using images, encryption, or other technology that can work to prevent the unauthorized alteration of records.

Methods of Access: Special Procedures

In the wake of 9-11, some state and local governments moved to restrict access to public records that contained information regarding public utilities, waterworks, sewers, emergency response plans and other information that could be useful to those planning terrorist attacks. Although the reasons for such restrictions are clear, the blackouts experienced in the northeastern US in 2003 also provide an understandable motivation for public interest in records that provide insight into the operation and regulation of electrical utilities, for example.

This situation illustrates an important challenge that state and local governments face in the digital world. While the Internet can provide the public with a level of access to records that was previously unimaginable, the public Internet simply may not be the best method for providing access to all records - especially those that contain information for which the clear possibility of dangerous misuse exists. In this case, where basic assumptions about national security have been challenged, new methods for providing public access in a more restricted fashion may be justified. State and local records management departments should work with their information technology, legal, and security departments to investigate methods for providing qualified access to such records where required and/or appropriate.

"The rules of engagement changed on 9-11."

"After Attacks, State Agencies Trim Access To Records," Associated Press[42]

Such methods may include qualifying individuals who wish to access such records or otherwise keeping records of records access. Virginia Beach, for example, recently began requiring citizens wishing to access land records from the city's website to first register by filing notarized copies of a registration form with the court clerk.[43] Such procedures may require changes to existing processes or even to open records statutes themselves. For example, under New York State's Freedom of Information Law, "an agency cannot ask a requester why he or she wants records or what the intended use of the record might be," with some exceptions.[44] Similarly, in Ohio, "a person may inspect and copy a public record . . . irrespective of his or her purpose for doing so."[45]

Controlling Fees and Ensuring Consistency

"The lawsuit . . . claims the county's new method of making records public over the Internet restricts dissemination of those documents."

"Public Records Case Set for Nov. 3 Trial," Hollister Freelance News[46]

Another challenge facing state and local governments in providing access to records is controlling the costs related to searching and copying records. While the amount that can be charged for copying records is often controlled by law (especially in the case of court records, for example), some counties, and other jurisdictions, charge varying amounts for the same service. For example, a recent study in Montana found that fees varied wildly, from 15 cents for a page of city council minutes in one county, to $5 per page for sheriff's office incident report in another.[47]

Consistent procedures and technology platforms can help to ensure that the cost of providing copies and related services is minimized and is relatively consistent.

Accountability for Private Digital Information

A recent state law passed in California, SB 1386, signals what may be an emerging trend in the way that government agencies and other entities are held accountable for their information and records management policies and programs. SB 1386 was developed in part in response to an incident where hackers accessed California state government computers containing information

on over 200,000 state employees, after which the government took weeks to notify the employees about the incident.

The law requires any "state agency, or a person or business that conducts business in California, that owns or licenses computerized data that includes personal information" to notify California citizens if their personal information is "acquired by an unauthorized person." Personal information includes social security and driver's license numbers, and account numbers and passwords for accessing financial accounts. It does not include "publicly available information that is lawfully made available to the general public from federal, state, or local government records." Affected parties may bring civil actions to recover damages.

This law clearly highlights the need for state agencies to have adequate policies and procedures in place for protecting private citizen information.

Consistent Application of Policy to Email and E-Records

Directives regarding retention and disposition need to apply equally to electronic records. This was clearly demonstrated in a complex case in Columbus, Ohio, that addressed allegations of excessive force against the city police force.[48] A local newspaper requested certain police records, including complaints against city police officers. The city was required to retain disciplinary records under the state's public records laws, and their retention rules stipulated that the records in question be retained for three years. Although the paper records had been destroyed in accordance with the retention rules, the city had not destroyed the electronic versions of these records. As a result, disciplinary records dating back almost 10 years were available in electronic form.[49]

A lengthy legal battle ensued over the release of the electronic records, with the court ultimately deciding that the city's failure to dispose of the records according to their own retention rules did not change the fact that the older records were still records that the public had the right to access. As such, the records were released to the newspaper.

State and local governments need to ensure that paper and electronic records are being managed consistently, and that retention rules are followed regardless of where records reside or the medium upon which they are stored.

5. Public Records & Personal Privacy in the Email Environment

Open records laws and similar statutes are largely based on the principle that, unless there is a reason to otherwise protect its confidentiality, a record should be made available for inspection, examination, and/or copying by the public. Although there a number of reasons for records to be withheld from the public, privacy protection is moving to the forefront as a key exception, and key challenge, as state and local government increasingly rely on email for conducting the business of government.

Email has many benefits for state and local governments. It can improve communication between citizens and elected representatives and lower the cost of service delivery. It can speed decision making among government employees and officials. However, state and local governments are not exempt from the risks and liabilities associated with email use, and in fact may incur additional, unique risks.

Email encourages informality and a conversational style of communication. Email policies reduce – but do not entirely prevent – employees from using the email system for personal correspondence or for providing opinions and other information that may prove damaging or at least embarrassing to themselves and their employer. At the same time, state records laws generally regard email as a form of written correspondence which must be retained according to its content with the same formality and care as correspondence in paper form. In addition, email messages generally must be made available to the public upon request.

"E-mail may include transmissions that are clearly not official business and are, consequently, not required to be recorded as a public record."

State v. City of Clearwater, 2003 Fla. LEXIS 1534 (Fla., 2003)

The result is that many state and local government email systems increasingly contain an intermingling of private and public email records – records that may subject to FOIA requests, and records that must be examined and judged based on their content before being released to the public; records that must be examined not only for their relevance to the request, but also for the possibility that they contain private or other information that cannot legally be released. This process can be laborious, expensive, and can contribute to complex litigation.

A recent case involving hundreds of sexually explicit and romantic email messages sent and received by local government employees illustrates the challenges that may arise.[50] In this case, the emails were sent and received by the elected Arapahoe County, Colorado clerk and a female employee under his supervision with whom he had a sexual relationship. A Colorado trial court had found that the email messages, which formed a portion of the evidence in a trial involving sexual harassment and other allegations, could be released to the public. The clerk and his girlfriend appealed the release of the email messages on several grounds, including the argument they were not public records and that releasing them would infringe on their personal privacy.

The courts considered the issues and found that some of the messages could be released to the public, in part because they were deemed to be public records despite their private content. Under Colorado's Open Records Act, public records include "the correspondence of elected officials, except to the extent that such correspondence is . . . without a demonstrable connection to the exercise of functions required or authorized by law or administrative rule and does not involve the receipt or expenditure of public funds . . . ."[51]

Despite the fact that most of the email messages did not relate to county business, the court found that they did qualify as public records because the "e-mails involve[d] the expenditure of public funds, and thus, are public records subject to disclosure under CORA." The court made this determination because the email messages were sent while the individuals were working; were

sent over a county email system for which the county paid monthly fees to use; and were sent over county-owned pagers - all activities that incurred the expenditure of public funds.

Among other things, this case demonstrates the complexity that can result in the email environment, and demonstrates the need for state and local governments to take steps to minimize the cost and disruption that can occur as a result of improper or unmanaged email use. State and local governments should consider the following issues when implementing and managing email systems:

- **Policies**. Implement and enforce email policies that minimize the use of the email system for personal use and provide directives on the type of content that is appropriate for email messages. Tools such as content filtering can assist in controlling inappropriate content.
- **Classification**. Limit the use of the email system for transmitting private, confidential, and other information that the public may not be entitled to access. Alternatively, employ tools that will allow employees to easily designate and classify email messages that contain information that is covered by an exception. These strategies will help to minimize the cost of fulfilling FOIA requests and of records management obligations generally.
- **Establish formality regardless of the size of government**. In small counties and towns there may be less formality in the way that email is used and managed. In Fredericksburg, Virginia, "most members of council use their personal e-mail accounts, rather than the ones set up by the city, to receive and send electronic communications about council issues."[52] That is, until, a massive FOIA request required the City Clerk to spend a week sorting through 5000 email printouts spread throughout her home, trying to determine which messages were relevant to the request. The city planned to resolve the issue by providing an email address that counselors could send messages pertaining to government business too for recordkeeping purposes. While the cost of using email may seem insignificant, the cost of complying with access requests can result in significant unbudgeted expenses.
- **Establish rules for email devices**. Email increasingly resides in multiple locations, including mobile devices. PDAs and other devices designed to send and receive email and keep schedules are likely to contain both personal and government-related information. Further, it is increasingly likely that the information contained on such government-supplied or supported devices could be included in public access requests - creating further headaches for administrators charged with assessing privacy issues.

6. Conclusion

Failing to retain, preserve, and make available the records of government, even if in email form, undermines the foundation of good government: transparency and public trust. State and local governments face many unique electronic records management challenges. Not only must they properly capture and retain electronic records, but they must also provide efficient and cost-effective methods for the public to lawfully access those records. In the face of the growing volume and value of email and other forms of electronic records, these challenges are only increasing. State and local governments need to act today to ensure that plans to deliver government services electronically and conduct business using email and other digital communications technologies are backed up by plans to invest in policies and technologies that will ensure that their records management obligations are met. Failing to do so will only increase the costs and disruption that will inevitably result in the future. Conversely, acting proactively can diminish the likelihood of future problems and allow governments to take advantage of operational efficiencies that result from information and records management activities.

7. Endnotes

[1] "City Plans to Archive Email," Elizabeth Pezzullo, Fredericksburg Free Lance-Star, August 7, 2003.

[2] "Meltdown at county recorder's office," Donna Osborn, Ozarks Headliner News, August 15, 2003.

[3] "Staff grilled on records fray," Angela D. Sykora, Gurnee Review, October 23, 2003.

[4] "FOI: E-mails should be public," Christopher Symington, The Wallingford Post, October 9, 2003.

[5] "E-mail gray area of Virginia's FOI Act," Jason Wermers, Times-Dispatch, October 26, 2003.

[6] "State sued for deleting e-mails," Sacramento Bee, Denny Walsh, February 14, 2003.

[7] "County can't deliver e-mail to public," Amy J. Schatz, St. Petersburg Times. Sep 19, 1999.

[8] "Records purged from computer," Alice Thrasher, Fayetteville Online, August 8, 2003.

[9] Arkansas Freedom of Information Act, Ark. Code Ann. §§ 25-19-101--25-19-107.

[10] For example, cases such as Weinstein v. Rosenbloom, 59 Ill. 2d 475, 482 in Illinois recognized the public's right to access certain state records a decade before the state passed its Freedom of Information Act in 1984.

[11] The majority of states provide information on these procedures, including the text of relevant statutes, on state archives websites.

[12] For example, according to an Associated Press story of November 23, 2001, entitled "After attacks, state agencies trim access to records," several Massachusetts state agencies "have begun restricting access to internal records that were easily available before the Sept. 11 attacks."

[13] "Information Management: Challenges in Managing and Preserving Electronic Records," General Accounting Office GAO-O2-586, June 2002. Available online, http://www.gao.gov/new.items/d02586.pdf

[14] Available online, http://www.pd.dgs.ca.gov/recs/erm-toc.htm

[15] Federal Sources, Inc., as quoted in "New priorities in IT spending mix," Dibya Sarkar, FCW.com, March 19, 2002.

[16] P. L. 105-277, Title XVII

[17] See, http://laemall.com/emall/message.html

[18] As listed by NCCUSL on their website: http://www.nccusl.org/nccusl/uniformact_factsheets/uniformacts-fs-ueta.asp

[19] Some states, such as Illinois, also have "Local Records Acts" that apply specifically to local, and not state, governments.

[20] Illinois State Records Act, § 5 ILCS 160/2.

[21] See Texas Public Information Act, § 552.002. Definition of Public Information.

[22] "Managing E-mail Effectively," New York State Archives Technical Information Series #62, 2002. Available online, http://www.nysarchives.org/a/nysaservices/ns_mgr_pub62.shtml

[23] "The Electronic Mail Policy of the Florida Department of State." Available online, http://dlis.dos.state.fl.us/barm/emailpol.pdf

[24] "Colorado State Archives Records Management Manual, Appendix C - Electronic Messaging Guidelines (E-Mail)." Available online, http://www.colorado.gov/dpa/doit/archives/rm/rmman/index.htm

[25] "Electronic and Voice Mail 2.0, A Management Guide for Maine State Government," Maine Records Management Services. Available online, http://www.state.me.us/sos/arc/general/admin/email.htm

[26] "State of California Electronic Records Management Handbook." Available online, http://www.pd.dgs.ca.gov/recs/erm-toc.htm

[27] "Email Policy Model for State Agencies," Texas State Library and Archives Commission. Available online, http://www.tsl.state.tx.us/slrm/recordspubs/email_model.html

[28] Lyman, Peter and Hal R. Varian, "How Much Information," 2003.

[29] "County can't deliver e-mail to public," Amy J. Schatz, St. Petersburg Times. Sep 19, 1999.

[30] California Public Records Act (Government Code, Section 6253(a)).

[31] "A Guide to the Illinois Freedom of Information Act," Office of the Illinois Attorney General. Available online, http://www.ag.state.il.us/foia/foia.htm

[32] "Records Fix Was the Right Thing to Do," Jeff Hovind, Waukesha Freeman, August 26, 2003.

[33] "County can't deliver e-mail to public," Amy J. Schatz, St. Petersburg Times. Sep 19, 1999.

[34] North Carolina General Statute § 132-6.1.

[35] "Electronic Records and the Illinois Local Records Act, Guidelines for Using Electronic Records," April 2001. Available online, http://www.sos.state.il.us/departments/archives/records_management/electrecs.html

[36] "State of California Electronic Records Management Handbook." Available online, http://www.pd.dgs.ca.gov/recs/erm-toc.htm

[37] "E-mail retrieval to cost state unit $10, 550," Clark Kauffman and Lee Rood, Des Moines Register, August 24, 2003.

[38] Ibid.

[39] "Few Connecticut State Agencies Comply With Records Laws," Associated Press, November 23, 2001.

[40] "Public must pay for access," Alicia Henrikson, The Capital-Journal, August 8, 2003.

[41] "County can't deliver e-mail to public," Amy J. Schatz, St. Petersburg Times. Sep 19, 1999.

[42] "After attacks, state agencies trim access to records," Associated Press, November 23, 2001.

[43] "Courts struggle with public access, privacy," Ellyde Roke, The Virginian-Pilot, October 28, 2003.

[44] "Freedom of Information Law," New York State Department of State, Committee on Open Government. Available online: http://www.dos.state.ny.us/coog/foil.html.

[45] State ex rel. Wilson-Simmons v. Lake County Sheriff's Dep't, 82 Ohio St. 3d 37, 40 (Ohio, 1998).

[46] "Public records case set for Nov. 3 trial," Kollin Kosmicki, Hollister Freelance News, October 14, 2003.

[47] "Fees charged for records vary by county," Cheryl Sabol, The Daily Inter Lake, October 22, 2003.

[48] State ex rel. Dispatch Printing Co. v. City of Columbus, 90 Ohio St. 3d 39 (Ohio , 2000).

[49] "Contract to shred documents doesn't trump records law," The News Media & The Law, Fall 2000 (Vol. 24, No. 4), Page 35.

[50] In re Bd. of County Comm'rs, 2003 Colo. App. LEXIS 1151 (Colo. App. , 2003).

[51] Colorado Open Records Act Section 24-72-202(6)(a).

[52] "City Plans to Archive Email," Elizabeth Pezzullo, Fredericksburg Free Lance-Star, August 7, 2003.