Surviving an Open Records Attack on a Public Administrator's E-mail

A Proposed Solution That Allows a Practicing Administrator the Ability to Preserve E-Mail in Compliance with Ohio Open Records Laws

Stephen W. Wolf

Wolfs Signals, LLC
27132 Butternut Ridge Road
North Olmsted, Ohio 44070
(440) 823-4781
SteveWolf@WolfsSignals.com

Last updated: March 25, 2009

Abstract

It is just a matter of time. Eventually someone will file a public records request for your e-mail messages. Very few public admistrators are comfortable knowing we can properly reply. Although we can blame it on the IT department, it will be our name on the front page of the Plain Dealer, Dispatch, Enquirer, Daily News, Blade or maybe all of them. Let's fix this. The first part of this paper is a fussy rendition of our duties, where they came from and what will happen. The second part presents a solution.

The Author

The author is a traffic signal consultant and thirty year police officer with the North Olmsted, Ohio Police Department. He holds degrees in Public Safety Management, an MPA and a JD from Cleveland Marshall College of Law.

I. Introduction – An Open Records Attack

We first need to understand what we are up against. An open records attack occurs when a malevolent agent seeks to discredit an administrator based on that administrator's difficulty in complying with actual or perceived visions of the Ohio open records laws. Of the local governments in Ohio, only a few have information technology (IT) departments with the resources to prepare for an attack. Most of us have one or two IT employees. They are underpaid and are often replaced. Administrators realize they will face this attack alone. Administrators must undertake the responsibility to preserve e-mail messages themselves.

An example of an attack was seen when the White House was lambasted for circulating the backup medium used to archive their computers.[1] Best practice allows an agency to reuse whatever medium is used to back up agency data[2]. Yet in January of 2008 the White House was lambasted for "destroying e-mail." They were following the best practices that your agency and mine follow when backup data is made. While doing nothing improper, the White House administrator cannot win against the implication of impropriety. All the administrator can do is prepare to answer these attacks with supported arguments.

Time has taught most public administrators that e-mail is a public record and that there is a duty to preserve such records. There is motivation to insure this is done properly. There is a line waiting to read our e-mail. A would-be politician seeking an office needs to know who and what he or she can criticize. Losing the bid, a disgruntled contractor attacks the winner in an

1 Elizabeth Williamson and Dan Eggen, *White House Says it Routinely Overwrote E-Mail Tapes From 2001-2003,* Washington Post, January 17, 2008, at A5.

2 John Burnett, ACCESS TO GOVERNMENT IN THE COMPUTER AGE, AN EXAMINATION OF STATE PUBLIC RECORDS LAWS, 33 (Martha Harrell Chumbler, ed., 2007).

attempt to recover the work. An office competitor wants to gain an advantage with the boss. Once in a while a citizen wishes to insure the proper operation of government.

What has left administrators scratching their heads is what "duty to preserve" e-mail means. Preserve what? What do we need to provide to these people? Do we need to preserve some piece of hardware? Or is it that we need to preserve the computer file? How should that be done? A memorandum copied to every member of an agency must be saved—by every member of the agency? Must we print every e-mail? What needs to be preserved?

This paper is written from the viewpoint of the practitioner. It first explores e-mail, public records and privacy. It looks at the broader implications, such as open meetings and contractor requirements. An analysis asking what the administrator needs to preserve leads to the conclusion that there is no definitive law, no definitive policy, no guidance from the courts, legislature and probably their own agency. The practicing administrator is best prepared if he or she (1) understands open records law, (2) understands his or her agency's record retention policy and record retention schedule, and (3) can argue that best practice was achieved in how he or she preserved the records.

There are two primary texts available to Ohio public administrators studying electronic records. First is the *Ohio Sunshine Laws* published yearly by the Ohio Auditor of State and the Ohio Attorney General.[3] The second is the 2007 American Bar Association treatise on electronic records entitled *Access to Government in the Computer Age*.[4] One cannot write about issues on

3 Ohio Sunshine Laws 2008: An Open Government Resource Manual (Ohio Auditor of State & Ohio Attorney General ed., 2008).

4 Access to Government in the Computer Age, An Examination of State Public Records Law (Martha Harrell Chumbler, ed. 2007).

Ohio e-mail without absorbing and regurgitating both documents. This paper draws heavily from both texts. Every administrator should read them cover to cover.

II. E-Mail and E-Mail Messages

Neither the legislature nor the judiciary has sought to define e-mail. That job was left to the Ohio Historical Society, a non-profit contractor serving Ohio who defines preservation as it relates to governmental matters.[5] In order to get a handle on electronic records they formed the Ohio Electronic Records Committee to develop statewide policies regarding electronic records.[6] This committee met between 1998 and 2006.[7] A subcommittee was formed to examine e-mail.[8] This subcommittee explains that e-mail is not a record, but a method of transmitting a record.[9] Like a piece of paper handed between parties, "e-mail" represents only the medium upon which information is transferred.[10] It is the e-mail *message*, the information inside an e-mail transmission, that resolves into a document.

For their part, the legislature and judiciary fall back on Ohio public records law to then handle the electronic e-mail document as they would any other form of record. Ohio law defines a record to include "any document, device, or item, regardless of physical form or characteristic, created or received by or coming under the jurisdiction of any public office of the state or its political subdivisions, which serves to document the organization, functions, policies, decisions,

5 *Message from the Executive Director*, *available at* http://ohiohistory.org/etcetera/welcome.html
6 *Ohio Electronic Records Committee, About the ERC, available at* http://ohiohistory.org/ohiojunction/erc/abouterc.htm
7 *Ohio Electronic Records Committee, ERC Minutes, available at* http://ohiohistory.org/ohiojunction/erc/ercminutes.html
8 *Id.*
9 *Id.*
10 *Id.*

procedures, operations, or other activities of the office."[11] Ohio public administrators must preserve e-mail messages.

III. What Must be Kept and Employee Privacy

Not everything received via e-mail must be kept. Ohio law does not consider anything that is written or typed by or to an administrator to be a record.[12] A record must document the public business.[13] For example, the Ohio Supreme Court denied the request of a terminated sheriff's department employee who wished to gain access to employee e-mail messages she alleged contained evidence of racial slurs used against her.[14] The court refused the request as the requested e-mail messages did not "serve to document the organization's functions, policies, decisions, procedures, operations or other activities of the sheriff's department."[15]

With respect to employee privacy there is no case law in Ohio or the country as to whether a public employee has an expectation of privacy in his or her e-mail messages.[16] There is little or no protection against a government who reads an employee's e-mail on the employer's e-mail system.[17]

11 Ohio Rev. Code Ann. § 149.011(g) (LexisNexis 2008).
12 *Steffen v. Kraft* (1993), 67 Ohio St. 3d at 439, 440
13 *State ex rel. Fant v. Enright* (1993), 66 Ohio St. 3d 186, 188
14 *State ex rel. Wilson-Simmons v. Lake County Sheriff's Dept.* (1998), 82 Ohio St. 3d 37, 41
15 *Id.*
16 John F. Fatino and Erik S. Fisk, ACCESS TO GOVERNMENT IN THE COMPUTER AGE, AN EXAMINATION OF STATE PUBLIC RECORDS LAWS, 99 (Martha Harrell Chumbler, ed., 2007).
17 *Id.*

IV. Broader Implications

There are broader implications regarding e-mail. A flurry of e-mail activity between public officials can bring charges of a violation of open meeting laws as business meant for those meetings disappears into the ether. A contractor can unwittingly become entangled in open records requirements when performing certain governmental service.

A. Open Meetings

E-mail involvement as it relates to a violation of Ohio open meetings law has only been discussed in the Ohio district courts and then is rarely reported. If public officials "meet" over e-mail, it may violate open meetings law. The Eleventh District keyed on the difference between an e-mail used for deliberations and one used for fact gathering.[18] When an official, in this case a trustee, "meets in a ministerial, fact-gathering capacity" there is no application of the Ohio laws.[19] That court narrowly defined a public meeting as a "majority of board members . . . meeting and discussing public business with one another."[20] The Ohio Revised Code requires a person to be present, in person, at a meeting.[21] Meeting over e-mail is prohibited. Another district ruled that when an e-mail is (1) unsolicited, (2) was not responded to, and (3) did not discuss official business it does not represent a violation of Ohio open meetings law.[22] These decisions are too narrow to be more than general guidance. To the extent that an e-mail is a letter seeking input from an administrator, it appears to be allowed. To the extent that e-mail becomes a substitute for a meeting, it is not allowed.

---

18 *Holeski v. Lawrence*, 85 Ohio App.3d 824, 827 1(11th district, 1993).
19 *Id.*
20 *Id.*
21 Ohio Rev. Code Ann. § 121.22(C) (LexisNexis 2008).
22 *Haverkos v. Northwest Local School District Bd. of Education,* 2005 Ohio 3489 (1st Dist. 2005).

B. Contractors

Privatization imposes duties on contractors who perform the public business. A contractor doing work for an Ohio pubic agency is subject to Ohio Open Records law.[23] There are four ways to impose a duty.[24] If a contractor supplies the data to a regulatory agency as part of a regulation or procurement process, those records are public. The private agency itself can be deemed to be acting as a state agency--the work it does is public. A private agency working with another agency who is later deemed public could be subject to the law. Finally, if the government has an interest in or a right of access to the data, that data could be public.[25]

Records can become public even when in the control of a contractor.[26] The Ohio Supreme Court defined that three things must be true to involve a contractor's records. To be subject to Ohio Revised Code 149.43, the contractor must first prepare the records in order to carry out a public officer's responsibility. Second, the public office must monitor the activities of the contractor. Third, the public office must have access to the records.[27]

While it hasn't yet reached the Ohio courts, the privatization of an entire office would appear to make its records public. In North Carolina, the town of Kitty Hawk privatized the entire law department.[28] A newspaper sought records that, had the office been public, would have constituted public records. The private law firm denied the request. That state found that if

23 Christopher W. Jones, ACCESS TO GOVERNMENT IN THE COMPUTER AGE, AN EXAMINATION OF STATE PUBLIC RECORDS LAWS, 114 (Martha Harrell Chumbler, ed., 2007).
24 *Id.*
25 *Id.*
26 *Holeski v. Lawrence*, 85 Ohio App.3d 824, 827 1(11th district, 1993).
27 *Haverkos v. Northwest Local School District Bd. of Education,* 2005 Ohio 3489 (1st Dist. 2005).
28 *Womack Newspapers v. Town of Kitty Hawk*, 2007 N.C. App. LEXIS 81 (N.C. Ct. App. Jan. 2, 2007) where similar law in North Carolina is applied in the manner of Ohio law.

a city contracts out an entire department, the records pertaining to city business become public record.[29]

A government cannot protect records from public view by contracting a provision that claims to supersede Ohio Open Records law.[30] For example, the City of Columbus negotiated with their police officers that certain disciplinary records would not be kept longer than a certain period of time.[31] The officers wanted those records purged on a regular basis. But the time in the contract was in conflict with the time in the city's retention schedule. Columbus was prohibited from superseding their retention schedule through that language in the collective bargaining agreement.

A contractor needs to understand with whom it is contracting. By understanding open records law they can work to protect their information.[32] They can segregate their data from public record to protect it from being swept public with the other data. They can limit ownership interest in the data to themselves. They can agree with the agency that the data, while not confidential, does qualify for a public records exception. They can require the public agency to provide notice when the contractor's records are released.[33]

29 *Id.*
30 *Keller v. City of Columbus*, 100 Ohio St. 3d 192 (2003).
31 *Id.*
32 Christopher W. Jones, ACCESS TO GOVERNMENT IN THE COMPUTER AGE, AN EXAMINATION OF STATE PUBLIC RECORDS LAWS, 128-129 (Martha Harrell Chumbler, ed., 2007).
33 *Id.*

V. The Duty to Preserve

The duty to preserve records comes from four sources.[34] It can be contractual, an agreement between parties perhaps assented to as part of a procurement process. It can come from common law, when the courts issue specific instructions ordering an agency to protect records. Important in this section are the duties that arise from statutes and those that arise from an agency's rule-based requirements.

Ohio statutory requirements demand the preservation of e-mail messages.[35] They must be available on the same medium used by the public officer.[36] Ohio has not yet determined the meaning of this provision. The plain text appears to indicate that if the record is originally preserved as a digital record, then the provided record should be a digital record.

A 2007 change in public records law requires that the Attorney General provide training for most elected officials.[37] Further, it demands that each agency adopt a public records policy.[38] The Attorney General is directed to provide a model policy.[39] A copy of the Attorney General's Public Records Policy is included as Appendix A. Agencies, in order to comply, typically make minor changes to the model policy and adopt it as their own.[40] In adopting such a policy, that policy then defines and has the force of law within that agency.

In order to comply with public records law, the administrator must comply with the agencies public record policy. That policy is likely the model policy provided by the Ohio

34 John Burnett, ACCESS TO GOVERNMENT IN THE COMPUTER AGE, AN EXAMINATION OF STATE PUBLIC RECORDS LAWS, 27 (Martha Harrell Chumbler, ed., 2007).
35 Ohio Rev. Code Ann. § 149.351(A) (LexisNexis 2008).
36 Ohio Rev. Code Ann. § 149.43(B)(1) (LexisNexis 2008).
37 Ohio Rev. Code Ann. § 109.43(E)(1) (LexisNexis 2008).
38 Ohio Rev. Code Ann. § 149.43(E) (LexisNexis 2008).
39 Ohio Rev. Code Ann. § 149.43(E)(1) (LexisNexis 2008).
40 See CITY OF NORTH OLMSTED PUBLIC RECORDS POLICY, 2007, attached as Appendix B.

Attorney General. Section four of that policy deals with e-mail. It imposes the following duties on a public administrator:

- Section 4 – Preamble
    - Duty to treat e-mail as a public record
    - Duty to follow the same retention schedule
- Section 4.1 – Duties of the employee with respect to records in private e-mail accounts
    - Duty to disclose to the records custodian
    - Duty to retain
    - Duty to copy them either
        - to their business e-mail accounts
        - to the office's records custodian
- Section 4.2 – Duties of the records custodian with respect to private e-mail accounts
    - Duty to file in an appropriate way
    - Duty to make them available for inspection and copying

In an attack on an administrator, the question will likely be whether the organization and the administrator understood and complied with the retention policies.[41] The attack will do a frame-by-frame analysis of each duty and determine if the duty was breached.

VI. What to Preserve

When discussing what to preserve, the issues become what type of data should be preserved, what type of e-mail systems is used, what medium should be used and what format should be used to preserve the data.

41 John Burnett, ACCESS TO GOVERNMENT IN THE COMPUTER AGE, AN EXAMINATION OF STATE PUBLIC RECORDS LAWS, 35 (Martha Harrell Chumbler, ed., 2007).

A. Types of Data

E-mail resides on a computer in one of three ways.[42] First is primary data. That is the data actually in possession of the administrator and which he or she can manipulate. This primary data is the e-mail message that is under the control of the administrator. Secondary data is backup and other data made in order to protect against failures. Outside of a judicial or discovery order, there is no duty to preserve this data.[43] Tertiary data is normally inaccessible and recovery requires technical resources. Data that remains on the hard drive after a file is erased is an example. The forensic imaging of a complete hard drive is another example. Access to this form of data must be justified and a search warrant is often required to gain access to this level of information.

B. Types of E-Mail Systems

E-mail access is accomplished mainly through one of two processes.

Web-Based E-mail Systems – E-mail retrieval can be web-based, using a web browser to access a website that displays the information. For example, when one uses a Hotmail, Gmail, Webmail or other such account, he or she is working through a website. This data never leaves the hosted site. If the website exists on agency equipment, the data is in the possession of some agency administrator. More likely, an Internet Service Provider (ISP) hosts the web site. While the e-mail messages are manipulated by the ISP, the message is never under the control of the agency. Should the agency change ISPs, the e-mail must be somehow retrieved and placed on the new ISP's server. This is call *migration*. Migration is technically complicated, expensive

42 *Id.* at 24.
43 *Id.* at 33.

and prone to error.[44] Should the ISP go out of business or be destroyed, the data is lost. An administrator cannot argue that a web-based e-mail system allows the administrator control over the primary data.

Many administrators must admit another problem relating to web-based systems. Information Technology (IT) positions are often unstable appointments and victim to a high turnover rate. This makes preservation tenuous. IT employees are not often trained in the legal requirements of public records. Should an IT person change e-mail systems, he or she may not understand the duty to preserve. The administrator can attempt to fault the IT position for a loss of public records but Ohio law does not absolve the administrator. It is unlikely the administrator cannot shirk the duty to preserve by blaming an incompetent IT employee.

Client-Based E-Mail Systems – Client based e-mail access requires that a program be run on the administrator's computer. Popular clients include Mozilla Thunderbird, Microsoft Outlook and Outlook Express. E-mail is copied from ISP-based e-mail servers onto the administrator's local server or local computer. It becomes primary data on that computer. The administrator then has control of the primary data. Were the web-based ISP to change, the e-mail would continue to exist on the administrator's computer. Client-based e-mail systems are systems that allow the public administrator to argue that he or she has control over the data so that legal responsibilities can be accomplished.

C. The Medium Used in Preservation

Archiving of data requires that the message be saved on a static hardware medium that protects the document for the time required on the retention schedule. Expected lifespans of a

44 See the later case study which documents extreme recovery costs associated with damaged data.

compact disc (CD) and a DVD, when handled properly, are at a minimum twenty years and can be as long as 200 years.[45] Magnetic tape can last up to 20 years.[46] Tape, however, requires the support of a proprietary system for reading the data from the tape--you must save the hardware with the tape or you can't later play the tape. DVD and CD storage are not proprietary and are the defacto standard.[47]

D. The Format for Preservation

Data stored on a DVD or CD can normally be read by any other computer. However, if the format of the data stored is dependent on the software used to store it, then that data is of no use without the program that wrote it. For example, e-mail stored in Microsoft Outlook cannot be read except by using the Microsoft Outlook program to read it. If preservation data is written in a non-standard format and the program used to store it is lost, that data is unreadable except through extraordinary efforts. One may try to solve this problem by archiving the program with the data. For example, one might archive e-mail from Microsoft Outlook and then copy the Microsoft Outlook program with the data. But in doing that, the administrator must also insure that the computer hardware and operating system software are able to run the preserved program. A current version of Microsoft Outlook specifies a range of operating systems and hardware that will allow it to operate. If, years into the future, you don't have that hardware, the program won't run and the e-mail will be lost. A program that runs only on an old and outdated operating system must be preserved with an old and outdated computer running an old and outdated

45 Fred R. Beyers, The Care and Handling of CDs and DVDs, a Guide for Librarians and Archivists (National Institute of Standards and Technology, Washington, D.C., 2003) page 13

46 Van Bogart, John W. C. Magnetic Tape Storage and Handling (Washington, DC: Commission on Preservation and Access and St. Paul, Minn.: National Media Laboratory, 1995) available at http://www.clir.org/pubs/reports/pub54/index.html.

47 Fred R. Beyers, The Care and Handling of CDs and DVDs, a Guide for Librarians and Archivists (National Institute of Standards and Technology, Washington, D.C., 2003) page 13

operating system so the old and outdated data can be recovered. The format of the preserved data must be carefully chosen to eliminate the need for preservation of what is called *legacy* hardware and software.

Migration – When an agency decides to change e-mail systems, it must work to migrate the e-mail messages from the old system to the new system. As there is no standard, such migration changes the data so that it can move from one proprietary system to another. If the agency changes from Microsoft Outlook to some other program, the e-mail from Outlook must be converted for use in the new program.

A Chosen Standard Format – If the data is stored in a standard format, a format readable by any computer, then the program that stored the data need not be preserved. The text data standard for computers is the American Standard Code for Information Interchange or ASCII (pronounced "as-kee") standard.[48] It is, simply, a text file. Even non-text data attachments can be stored as ASCII text using encoding.[49] In a text file an attachment looks like an almost never ending series of letters and numbers.[50] This is how e-mail is sent, in ASCII. The e-mail is changed by the program used and stored in its own format.

VII. Case Study

In *State ex rel. Wilson-Simmons v. Lake County Sheriff's Dept.* a county agency found their duty to preserve e-mail was under attack and found themselves in gross violation of their

48 X3.4-1963, AMERICAN STANDARD CODE FOR INFORMATION INTERCHANGE, American Standards Association (1963), available at http://www.wps.com/projects/codes/X3.4-1963/index.html.

49 See Internet Message Formats RFC 2822, P. Resnick ed. (2001) available at http://www.ietf.org/rfc/rfc2822.txt which extends into RFC2045, RFC2046, RFC2047, RFC2048, and RFC2049 which describe the Multipurpose Internet Mail Extensions (MIME) format for representing binary attachments to e-mail through ASCII text.

50 *Id.*

duty.[51] They won the case and escaped criticism through an alternate interpretation of what must be saved. The court never reached the point of assessing if their duties were met.

In that case a female correction officer employed by the Lake County, Ohio Sheriff's Department filed to obtain e-mail messages of five co-workers that were contained in the Lake County Sheriff's e-mail system. She alleged that those e-mail messages were used to make racial slurs against her. In response to her request for those e-mail messages, she was informed that while public record, she would have to pay $2,521.40 plus the cost of copying the messages. That cost would be used to pay a specialist who would have to work for 140 hours at a rate of $18.01 per hour. The agency tried to justify the requirement as follows:

- The messages are not readily available
- The messages must be reconstructed
- The computer system must be shut down and used only for reconstruction
- E-mail older than one day is relegated to a backup system which requires reconstruction
- During the period in which the messages were stored, the system was unstable and e-mail was lost
- No matter, as e-mail over a week old is on a backup that is overwritten--it was never saved for longer than a week.

The plaintiff failed in her goal, but not for the above reasons. The e-mail requested was found not to document the business of the department and the Ohio Supreme Court refused her request, at least under the public records law.

51 *State ex rel. Wilson-Simmons v. Lake County Sheriff's Dept.* (1998), 82 Ohio St. 3d 37

VIII. How to Preserve and How to Destroy

To preserve e-mail records, the administrator must first understand how to store a particular e-mail so that it is queued for preservation. In most cases, an administrator will create a set of folders or directories into which e-mail messages are placed after having been read and acted upon. Those folders correspond to record titles that exist on the employee's record retention schedule. When an e-mail is no longer of value to the administrator and if the records retention schedule allows, the e-mail can be deleted. Otherwise, the e-mail must be preserved.

The administrator must understand his or her agency's public records retention policy and his or her public records retention schedule for e-mail. Those two documents will define what must be preserved. But what is preservation? Typically, e-mail will be listed on a retention schedule with a requirement that it be preserved until "of no administrative value".[52] Typically, a retention schedule offers no guidance as to how to preserve e-mail. There is no guidance as to how an administrator should preserve e-mail offered in statute or in the common law. We again must turn to the E-mail Subcommittee of the Ohio Electronic Records Committee.[53] They define four categories of e-mail messages: non-record messages, transitory messages, intermediate messages and permanent messages.

Non-Record Retention – There is no requirement to keep non-record e-mail. Personal correspondence, publications, newsletters, vendor solicitation, spam and many other categories can be immediately deleted. Care must be taken that the e-mail does not provide the basis for

52 See CITY OF NORTH OLMSTED SCHEDULE OF RECORDS RETENTION AND DISPOSITION, 2001, attached as Appendix C.

53 http://www.ohiohistory.org/ohiojunction/erc/e-mail/e-mailguidelines.html

which public work was done. For example, a vendor solicitation used to justify the purchase of that product does become public record and must be preserved.

Transitory Messages – Transitory messages "do not set policy, establish a guideline or procedure, certify a transaction or become a receipt."[54] E-mail messages documenting telephone messages, drafts of papers, or notices of meetings have no value after the subject event passes. Typically, they need only be kept "until no longer of administrative value".[55]

Intermediate Retention – For records that have more value, you transcend the e-mail category on the record retention schedule and categorize the record as appropriate. If the record is "correspondence" then you follow the requirements for "correspondence" on the record retention schedule.

Permanent Retention – E-mail that has significant value should be kept. Again, the administrator can determine the retention period based on the records retention schedule.

The following is a sample filing scheme suggested by the E-mail subcommittee. While a suggestion, it is unlikely that this example fits any particular administrator.

- Non Record Messages – delete at will
  - Personal messages from family, friends and other miscellaneous messages
- Transitory Messages – delete when no longer of administrative value
  - Drafts of publications, reports and memos
  - Meeting notices
- Intermediate Retention – held until no longer of administrative value
  - Budgets
  - Payroll
  - Vendors
  - Correspondence and memos
  - Reports

54 *Id.*
55 *Id.*

- Minutes

- Permanent retention per the agency retention policy

After the period required for retention passes, the user can destroy the record.[56] But, if the retention period is much longer than the period when the message was of value, then maintaining the record challenges the hardware, software and user of the system. For example, on most record retention policies, pre-employment investigative records require a very long retention time. There comes a time when moving the message off of the computer will better insure its preservation. It will protect against hardware or software change. It is at this point an administrator must find a retention procedure.

IX. A Proposed E-mail Record Retention Procedure

This is a proposed method whereby the administrator can take control and archive data subject to Ohio Open Records laws and the best practices as described by the Ohio Historical Society. It uses a free, open source e-mail client to take control of the e-mail. It then archives the e-mail using a free utility designed specifically for the purpose.

Open source software is that which is designed and implemented in a corroborative environment.[57] It is a participatory venture between both the developers of the software and the end users. Cost disappears as most open source software is free. Reliability and flexibility increases due to there being a wider influence on the authors. Predatory vendors are no longer able to define update schedules.

56 Ohio Rev. Code Ann. §§ 149.351, 121.211 (LexisNexis 2008).

57 See http://www.opensource.org which hosts the Open Source Initiative, the standard body for open source software.

Mozilla is an open source concept that was launched by Netscape in 1998.[58] It is now an independent, mature open source support organization. Its purpose is to provide free software tools that would make the Internet a better place in which to communicate. A major Mozilla project is Thunderbird, its open source e-mail client. Thunderbird has all the functionality of any other e-mail client. In Thunderbird, e-mail messages are already stored in ASCII text. As described earlier, ASCII text is a standard that is readable across hardware and software platforms. ASCII text is the baseline, the standard. Thunderbird easily replaces e-mail clients that must be purchased.

Because Thunderbird is an open source project, it involves much more collaboration between developers and users. This results in a more robust and useful user help interface. Installing and setting up the program is well supported through on-line help. The biggest administrator hurdle is finding the addresses of the e-mail server where the client will retrieve the e-mail.

Once installed, the user builds a series of folders or directories that mimic the particular retention policy and schedule to which he or she is accountable. After a message is read and acted upon, the message is moved by dragging it to the particular folder. For example, the user might have:

- Inbox
  - 2008
    - Correspondence
    - Transitory Storage
    - Long Term Storage

Each outgoing message should be stored into the appropriate folder after it is sent.

58 See http://www.mozilla.org/about/

The remaining issue is how to preserve data that is no longer necessary for operation but that must be retained. To this end, I have provided a free program that, given the location of the mail directory, preserves it. Given the location of the "correspondence" directory, it will preserve all e-mail messages in that directory onto a CD or DVD.

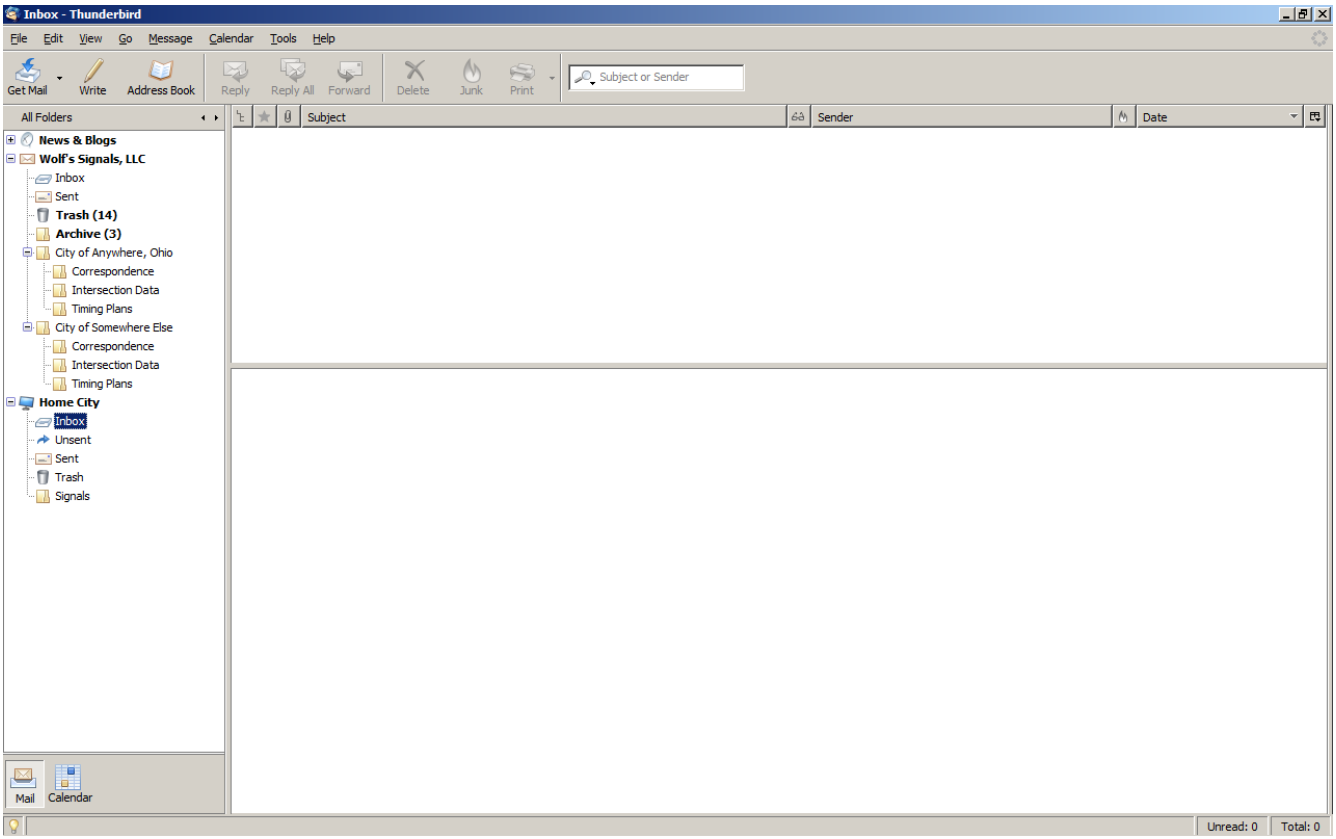
The Thunderbird e-mail file is a long ASCII text file that represents the mail and attachments in a particular directory. It is a compendium of all the messages and attachments in one file, one after the other after another. The utility first archives the original Thunderbird ASCII e-mail file in its entirety. Additionally, that file is dissected and each message is extracted and saved in its own file. The subject line of each message file is a combination of the date the file was received and the subject line. The date is formatted to allow sorting by chronological order; by year, month and date. For example, the file named "20060309 Re: New Hire John Doe.txt" would result from a message received on March 9, 2006 and having the title, "Re: New Hire John Doe". In this way, an administrator seeking a particular message within a preservation is not required to wade through all the messages in search of a particular item.

The administrator is left with a CD or DVD which contains the contents of however many directories he or she chose to preserve on that CD or DVD. This CD or DVD can then be preserved for the required time. It can, if it is the policy of the agency, be turned over to the agency's records custodian.

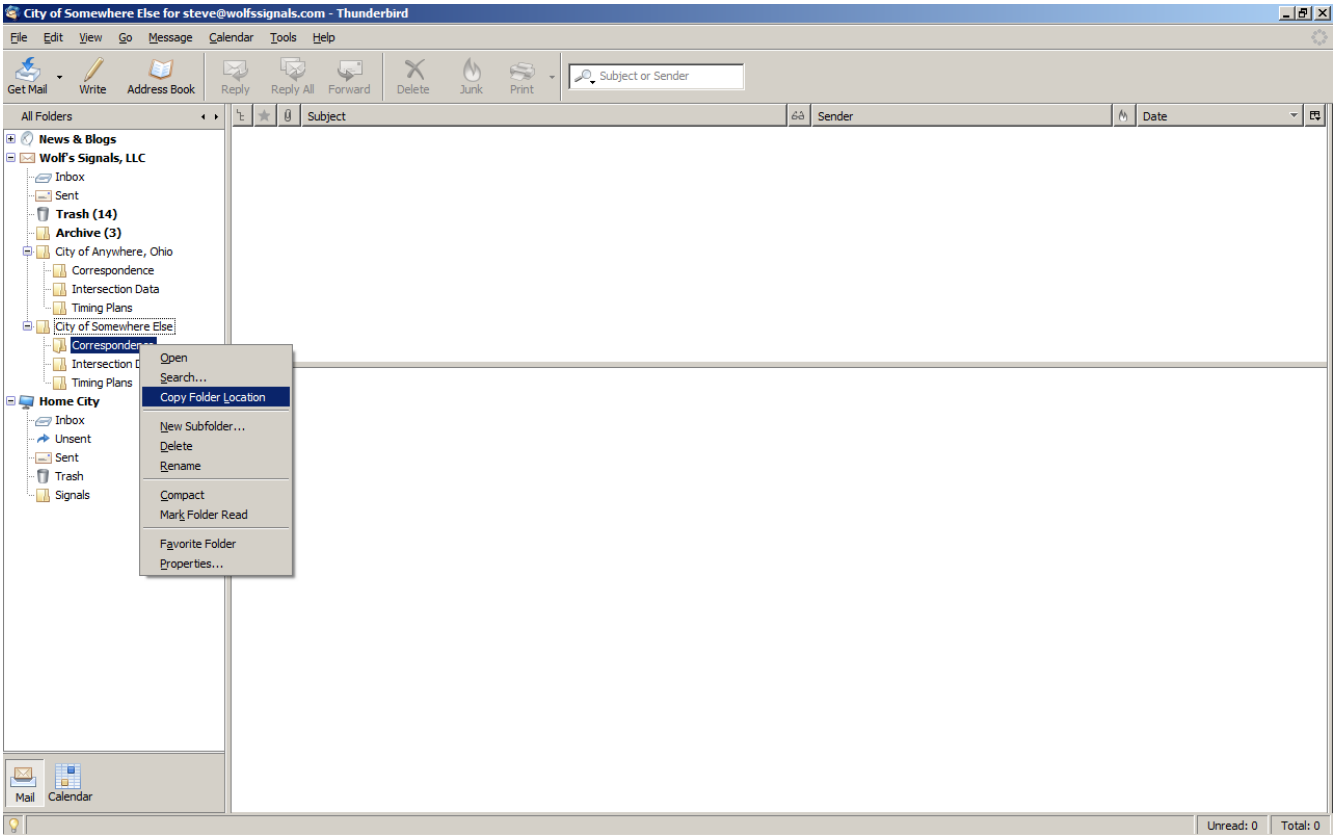
X. Using the Public Record Preservation Utility

The current Windows-only version of the Public Record Preservation Utility can be downloaded from http://www.wolfssignals.com. The program can be run from any directory.

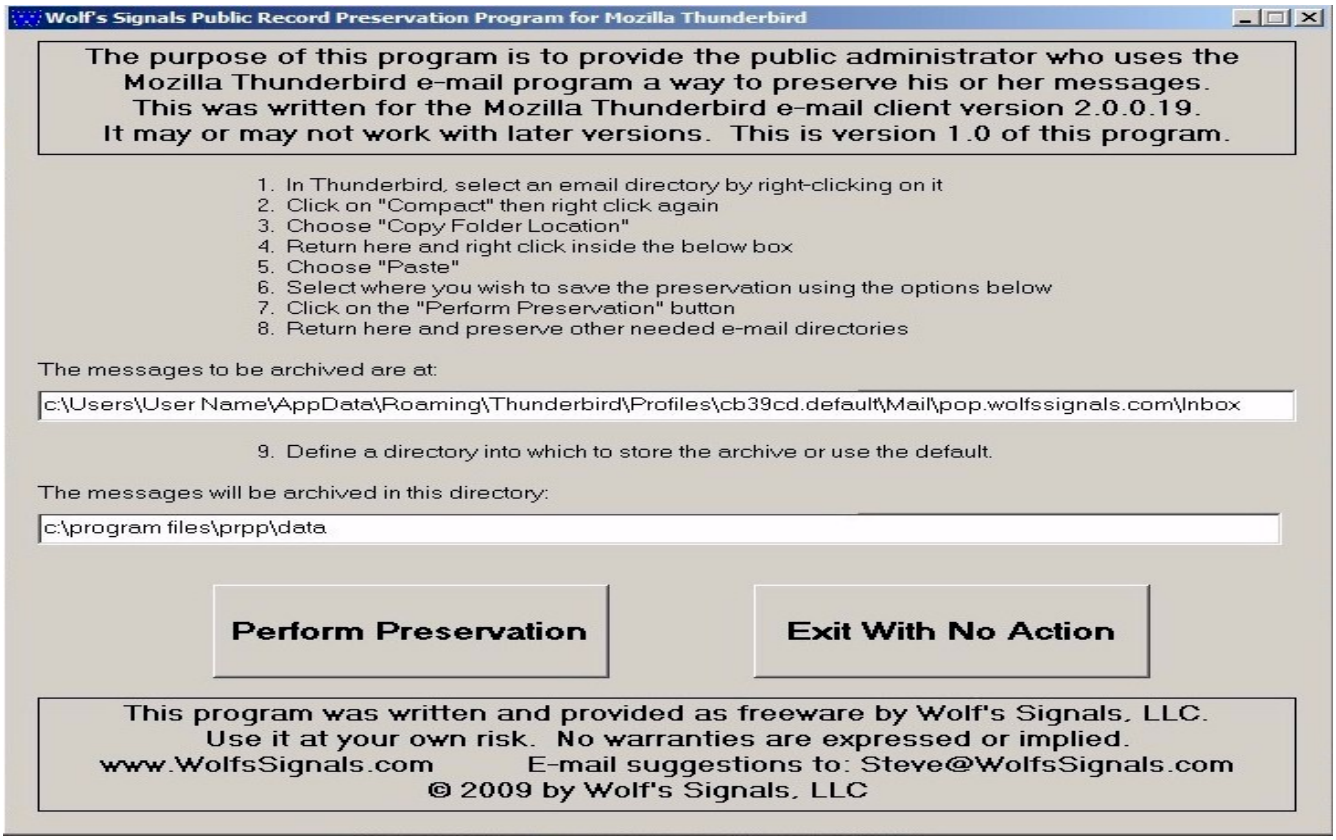
When using the Thunderbird E-mail client, you will see a screen such as that in the figure below.



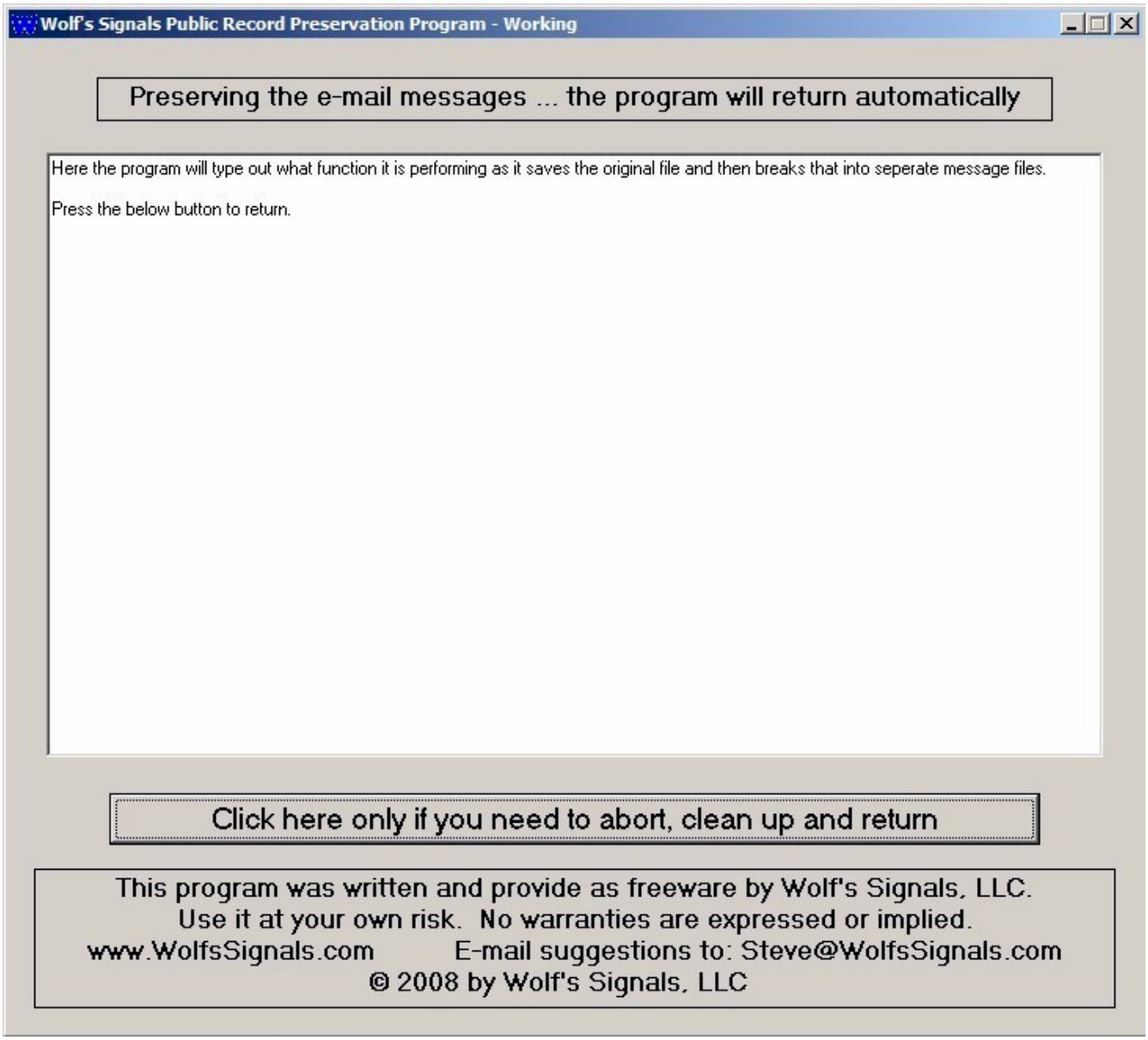
To begin, the administrator needs to compact then copy the location of the directory to be preserved. He right clicks on that directory and then clicks on “Copy Folder Location”.



He now runs the preservation utility which will instruct him to right-click in the white box and paste the location of the folder into the utility.



He now determines where the preservation should be placed. If it is to be on a CD or DVD already placed in the computer for this purpose, he clicks “Perform Preservation” to begin. He will be presented with a screen which shows the progress of the preservation.



The program will then report if the preservation was successful and close.

XI. Conclusion

Faced with a public records request, the administrator can return to the preservation, extract the required messages by copying them to another CD or DVD and then give that to the person who requested the information. If the record is unavailable, the administrator will be in a good position to argue as to why it was unavailable. Either it was not a public record or the retention period expired and the record was discarded. The administrator can argue that the form of the record was proper, it was that used by the administrator. It included all original data, including the internal notes about the message--the information called meta data. The requester can print or extract MIME data from the provided records. The administrator has met the requirements of Ohio Public Records law.

The administrator can argue compliance with Ohio open records law, his or her retention policy and schedule and provide those messages in a way the comports with both law and policy. The administrator is in the best possible position to survive an open records attack on his or her e-mail. Problem solved.