

KNOW WHAT TO KEEP

Preserving Electronically Stored Information for Litigation and Investigations

Everyone knows that our world is digital. We are so dependent on technology in order to perform our job responsibilities that we have a computer at the office, multiple computers at home, and handheld devices so we can be reached via e-mail, text and voice mail where ever we go. And if we are smart, we have backup copies of our digital materials stored on external hard drives, CDs or DVDs in case our original files become destroyed or inaccessible. We communicate via multiple e-mail accounts (I have 7), instant messaging and chat. We generate numerous memos, documents, spreadsheets and presentations. On top of this, our digital materials can be found on corporate servers and back-up tapes.

Knowing how widely disseminated our data has become is frightening enough, but add to that the data that computers create in the background during use and it becomes apparent that controlling access to our data has become nearly impossible. The vast amount of data we generate has created a dilemma for many organizations. Those with security and privacy concerns want to delete as much data as possible to prevent inadvertent security breaches and loss of proprietary information. Those with their eye toward litigation and investigations want to keep everything because digital data can help support or defend specific claims and provide an accurate view of employee activity. Trying to strike a balance between what to keep and what to destroy (and when) has proven a difficult task for many organizations.

Every organization must retain materials for a variety of reasons. There are state and federal laws as well as regulatory requirements that impact how long an organization should retain specific records. There are business requirements that impact how long records should be kept. As an example, colleges and universities must permanently retain student transcripts. Although I have been out of college for nearly 30 years, I still must provide a college transcript every time I apply for a teaching position. Medical organizations must keep medical records in perpetuity.

But the retention of digital data is now being scrutinized due to the fact that on December 1, 2006, the Federal Rules of Civil Procedure were modified to require that attorneys address electronically stored information (ESI) as part of the discovery process. The Federal Rules of Civil Procedure are the rules governing civil litigation in U.S. federal courts. The rules governing civil litigation in state courts generally parallel the Federal Rules to some degree.

Understanding the Legalities

While no one expects security professionals to understand all the legal aspects of the Federal Rules of Civil Procedure, it is important to understand the legal requirements of preservation of materials relevant to current litigation. When an organization is served notice of litigation, it has a duty to preserve all materials — both in paper and digital format — which may contain information relevant to the lawsuit. This process is called a “litigation hold” or “preservation hold” and is a critical part of the litigation process.

The penalties for not putting a preservation hold in place can be severe. An organization can even be sanctioned by the court for having an inadequate preservation hold in place. The reason for this is that all relevant materials need to be preserved so an informed decision can be reached during litigation. If relevant materials are not properly preserved, it becomes difficult, if not impossible to understand the underlying facts of the litigation. A fair trial is no longer a possibility.

When data gets destroyed in civil litigation, it is called “spoliation” and can result in significant sanctions and a lost lawsuit. While inadvertent destruction of data can result in severe sanctions, the courts really frown on deliberate data destruction. If it can be determined that data destruction tools like Eraser, BCWipe or Evidence Eliminator have been used after the initiation of litigation, there will be severe penalties. Many organizations have implemented document retention policies that include guidelines for the routine destruction of specific materials. While a company can not be sanctioned for the destruction of data during the “normal course of business” according to Rule 37, the “Safe Harbor Provision” in the Federal Rules, they can be sanctioned for not suspending the destruction process for the duration of litigation. Implementing a data destruction policy upon notice of litigation does not constitute “normal course of business!” The question that is asked is whether or not a party acted in “good faith” and made a reasonable effort to preserve relevant materials. If the answer is “yes,” then no sanctions will be leveled.

Implementing a “Litigation Hold”

While the above sounds fairly straightforward, one only has to look at how dispersed our data has become to realize what a complex task faces anyone implementing a “litigation hold.” The first step in the process is identifying where relevant materials are located.

Locations may vary depending on the issues in dispute, but the starting point would probably be the office computers of the key parties named in the litigation. From here you would look to preserve the relevant mailboxes on your mail server, and probably the home directories on the network server of the key parties. Preserving this information can be as simple as burning relevant files and folders to a series of CDs or DVDs. This type of storage medium is ideal since the files stored on them are "read only."

Unfortunately for most business professionals, digital records are not stored in two or three locations. We have hand-held devices, home computers and multiple e-mail accounts. In many organizations, voice mail is digital and is forwarded to an e-mail account. There are now tools that convert voice mail to text and can be sent as either a regular e-mail or text message (see SpinVox — www.viewyourvoice-mail.com and PhoneTag — www.phonetag.com). For some organizations, such as police departments, there are laptop computers in employee's cars.

For security professionals, archiving security camera footage may also be necessary. And do not forget back-up tapes, which can be taken out of the rotation cycle for the duration of litigation. For some storage locations and media, one can successfully argue that the cost to preserve the materials is unduly burdensome; however, keep in mind that companies will run into problems if something is overlooked or improperly identified.

To be on the safe side, organizations should implement a preservation hold when litigation is reasonably anticipated at the earliest and when served notice of litigation at the latest. The steps should include identifying the custodians of relevant information and the creation of a data map identifying the systems most likely to contain this information.

A data map is not the same as a network topology diagram that most system administrators are familiar with. This map should include the name of the system, the types of material it contains and the date the system was put into service. If the system was put into service after the issues in dispute occurred, it may not need to be preserved.

While this is a complex task, there are some excellent materials that can guide you and your lawyers through the process. The Sedona Conference (www.sedonaconference.org) is arguably on the forefront of these issues and has published some great resources. The first is "The Sedona Principles, Second Edition, Best Practices Recommendations & Principles for Addressing Electronic Document Production" (http://www.thesedonaconference.org/content/miscFiles/TSC_PRINCP_2nd_ed_607.pdf) and the other is "The Sedona Conference Commentary on Preservation, Management and Identification of Sources of Information that are Not Reasonably Accessible" (<http://www.thesedonaconference.org/dltForm?did=NRA.pdf>). This last document includes a decision tree that can help identify items that need to be preserved.

Deciding What to Dump and What to Keep

This preservation concept is often counter to the concepts embraced by security professionals and privacy advocates. By deleting and destroying data, one can reduce the risk of inadvertent disclosure of proprietary and confidential information. More and more tools are becoming available to remove or destroy digital data. While on the surface this appears to be a good idea, the more data that is destroyed, the more difficult it can become to identify the inappropriate activities of employees.

Computers generate an enormous amount of data in the background during use. Because much of this information is not user-created, users do not know it exists and rarely take time to delete it. One of the best examples is the data that is cached when someone visits a Web page. For Internet Explorer users, this information can be found in the "Temporary Internet Files" folder. Whenever you visit a Web page, that page's contents are stored in this folder. This does not sound too interesting on the surface until you realize that the contents of Web-based e-mails such as Yahoo and Hotmail can be found in this folder. This is very important from an investigative perspective as people will often use Web-based e-mail accounts to bypass the monitoring of their corporate e-mail. From an investigative perspective, this Web-based e-mail is a great source of information and can help identify the true nature of a person's activity.

Unfortunately, many organizations routinely delete Temporary Internet Files and other residual data that could benefit an investigation. This is not necessarily done to "cover one's tracks," but more likely as a security and privacy mechanism. The utility "Disk Cleanup," which is installed as part of a normal Microsoft Windows application, provides the option to remove Temporary Internet Files. Some organizations have "Disk Cleanup" scheduled to run every time a computer starts up in order to remove any potentially malicious files that might have been downloaded in the Temporary Internet Files folder. This means that employees can now communicate via Web-based e-mail regarding any inappropriate activities they choose because their own employer is helping them cover their tracks!

Some businesses will take this a step further and install a third-party application to assist with the removal of residual data. One such tool is CCleaner (formerly Crap Cleaner) that not only removes the cached files for Internet Explorer, but does so for the other popular browsers Opera and Mozilla Firefox. It will also remove other “hotbeds” of evidence such as the files in the Recent Documents folder, prefetch directory information and user assist history.

We had a client who suspected a former employee of having stolen proprietary information when they left to go work for a competitor. When we examined the former employee’s computer, we could not find any material that could help us determine the employee’s activities. We then noticed that CCleaner was installed and had been used prior to the employee’s departure. This is often a “red flag” and is an indicator that someone is trying to cover their tracks. When we brought this information to the client, they told us that they had installed CCleaner on all of their employee’s computers and encouraged them to use it daily. It makes it easy to behave inappropriately when your employer encourages you to destroy evidence!

If you are not familiar with the types of residual data that can be found on a computer, you may wish to download my whitepaper, “Secure File Deletion: Fact or Fiction?” which describes numerous types of residual data and data destruction techniques. It can be found in the SANS Reading Room at http://www.sans.org/reading_room/whitepapers/incident/631.php.

Data preservation is a complex issue and can only be addressed at a very elementary level in a short article such as this. But if you are a working business professional, you will be involved in preserving data for litigation or investigative reasons — and it is important to understand some of these issues surrounding preservation.

Take a minute to evaluate the digital information you and your team generate or are responsible for maintaining. If you were asked to preserve specific data from a certain period in time, could you do it? What problems might you face? As with any security-related project, prior planning can significantly reduce the cost of the process. If any of the concepts discussed in this article were either frightening or alien to you, I suggest you review some of the references cited (and review some of the case summaries at www.ediscoverylaw.com). The time spent could save your company a significant amount of money or help you identify the misdeeds of an employee.



JOHN MALLERY—SECURITYINFOWATCH.COM UPDATED: 02-4-2009 4:41PM