

Preserving electronic information: avoiding pitfalls

Dulce Foster and Oliver Fuchsberger

Special to Minnesota Lawyer

E-discovery is an integral part of any litigation, but— for those of us who didn't go to law school to capitalize on our technical prowess — it can be a little daunting. Many fail to recognize that good E-discovery practices begin with document preservation even before a complaint is filed.

Taking steps to preserve electronically stored information (ESI) is not only good strategy for gathering evidence — it is usually required. A company investigating criminal conduct may be accused of obstruction if a prosecutor believes it destroyed ESI intentionally. In federal civil cases, E-discovery is governed by Rule 26 of the Rules of Civil Procedure. Rule 26 requires litigants to automatically disclose ESI they intend to use in litigation, and also imposes on the parties an affirmative duty to meet and devise a plan for ESI discovery. Whether a written discovery plan exists or not, litigants who intentionally destroy relevant ESI risk being sanctioned, or at a minimum, becoming embroiled in costly discovery disputes.

Since the ultimate scope of the claims is typically unknown when preservation efforts begin, deciding how much effort to spend on ESI preservation may be difficult. Unfortunately, there are no second chances when it comes to preserving electronic information, so initial steps



Dulce Foster



Oliver Fuchsberger

should err on the side of being over-inclusive.

Key considerations

Before a company takes any steps it might later regret, it would be well-advised to keep in mind these principles:

1. **The act of deleting a file on a computer does not actually destroy it.** The information still exists on the computer; it is just inaccessible without special tools and expertise. Over time and usage, all or portions of the deleted information will be overwritten by new information, but it does not disappear immediately.

2. **The activity that occurs on a computer or server is always recorded.** Logs are generated on networks and computers tracking activity. Each file contains “metadata” fields that record file information and activity. IT experts can utilize this information to reconstruct a history of the actions that took place on a computer.

3. **Even the simple act of booting up a computer results in a loss of in-**

formation. Each process that a computer runs — whether user requested or automated — will modify and overwrite information on the computer.

First steps

The first step a company should take when the threat of litigation arises is to hold a meeting with representatives from its legal team and IT and record management departments. The goals of this meeting should be: to identify where, within the company's IT infrastructure, relevant information exists (including the identity of key employees or “document custodians” likely to possess relevant information); to determine the steps needed to preserve that information; and to evaluate the business impact on the company of preserving, collecting and reviewing that information. The meeting should result in the development of an ESI preservation plan.

Another important step is to issue a “litigation hold” notice to employees likely to possess relevant information to prevent the inadvertent destruction of evidence. The notice should describe the claims and instruct employees not to destroy any documents related to them. The company should also instruct its IT and records management departments to suspend email deletion “robots” and other routine document destruction policies that could overwrite information related to possible claims.

Computers and hand-held devices

The computers used by employees suspected of wrongdoing and other information custodians should be located and secured immediately to prevent the intentional destruction of evidence and refute possible spoliation claims. There are several different ways to accomplish this:

Remove the hard-drives from the employees' computers and replace them with new ones, retaining the old drives in a secure location for future analysis as needed;

Have outside counsel retain and direct a computer forensic expert to image and analyze the computers, under an agreement that protects the expert's work from discovery under the attorney work product privilege. While this is the most costly alternative, it is the best way to analyze the computers while ensuring the data is complete and forensically sound;

Create images of the employees' computers using basic computer imaging software. While less expensive than conducting full forensic analysis on the computers, such images may not capture all the activity logs or deleted files residing on the computers and would not be appropriate in all situations.

Companies should not ignore the data that might be stored in other locations, including portable flash-drives, CDs, external hard-drives, cell phones, and other hand-held devices. Identifying such information and consulting with IT experts on how to preserve it should be part of the company's ESI plan.


Email, network file servers and server back-ups

The ESI plan should take steps to preserve relevant email residing in key employees' email accounts, as well as email that employees may have archived in paper form, on their hard-drives, or elsewhere on the company server. Locating and preserving such information may require copying all emails and attachments in key employees' mailboxes, interviews with employees to determine where they store archived materials, and conducting targeted searches of email accounts using specified terms.

Other information contained on the company's computer network should be preserved as well. Many companies assign "home shares" to each employee that can only be accessed by that employee. The preservation of electronic data may require copying and securing

everything contained in an employee's home share. Alternatively, a company may hire a computer forensics expert to create and analyze images of all network servers to which key employees had access.

Finally, most companies keep backup tapes of their servers. Typically these tapes are created and then overwritten by future backups on a scheduled rotation. Companies should consider pulling tapes from the rotation if they relate to time periods at issue in litigation, and retain them in a secure location.

These are just a few of the steps companies can take to preserve their ESI. While creating an ESI preservation policy may seem daunting, the alternatives — either losing exculpatory evidence or being forced to defend against spoliation charges — are considerably worse. 

Dulce Foster is a shareholder in Fredrikson & Byron's White Collar & Regulatory Defense and Litigation Groups and Chairs the Internal Investigations Group. She can be reached at dfoster@fredlaw.com.

Oliver Fuchsberger, Fredrikson & Byron's Litigation Support Consultant, has over 20 years of litigation support experience. He can be reached at ofuchsberger.com.