The Paralegal's Guide to Electronic Evidence

LORMAN®

Published on www.lorman.com - October 2017

INTRODUCING

Lorman's New Approach to Continuing Education

ALL-ACCESS PASS

The All-Access Pass grants you UNLIMITED access to Lorman's ever-growing library of training resources:

- ☑ **Unlimited Live Webinars** - 120 live webinars added every month
- ☑ **Unlimited OnDemand and MP3 Downloads** - Over 1,500 courses available
- ☑ **Videos -** More than 700 available
- ☑ **Slide Decks -** More than 1700 available
- ☑ White Papers
- ☑ Reports
- ☑ Articles
- ☑ ... and much more!

Join the thousands of other pass-holders that have already trusted us for their professional development by choosing the All-Access Pass.

Get Your All-Access Pass Today!

SAVE 20%

Learn more: www.lorman.com/pass/?s=special20

Use Discount Code Q7014393 and Priority Code 18536 to receive the 20% AAP discount.

*Discount cannot be combined with any other discounts.

The Importance of Preserving Electronic Evidence

In the age of E-Discovery and electronically-stored evidence, paralegals now face a new genre of rules under the Federal Rules of Civil Procedure, Federal Rules of Evidence, local court rules, case law and custom within the legal profession. It is important that paralegals fully understand how to preserve, collect and process electronic evidence. Electronic evidence can make or break the case of an attorney.

At its heart, electronic evidence is information that is stored in a digital form and that has a probative effect on the outcome of the case. This means that the evidence tends to make it more likely or not that a fact in dispute occurred. The court has a duty to determine whether electronic evidence is authentic before it may proceed to determine if the evidence is relevant. The court will also assess whether the evidence is considered hearsay or is in violation of the Best Evidence Rule. This means that the court must determine whether a copy of the electronic evidence may be admitted into court or whether the original piece of evidence is required.

There are numerous pieces of information that can be considered "electronic evidence." Here is a list of the common sources of electronic evidence that are often used at a trial:

- Text messages
- Facebook status updates
- Date of access into social media accounts
- Emails
- Digital photos
- Bank and ATM transactions
- Word documents
- Excel spreadsheets
- History from an Internet browser
- Access dates into other computer systems
- Accounting information
- Backups of information stored on a computer
- Computer memory
- Logging dates
- Video files
- Audio files
- Cache
- Activity logs
- Telephone logs
- Voice mail
- Any other information that may be stored in a computer or electronic system

In 2006, a new rule under the Federal Rules of Civil Procedure was promulgated to require the preservation of electronic evidence. Because computer files can be easily accessed, destroyed or modified, the new rules are intended to preserve the electronic evidence in its original form. New state laws have also been created to deal with the preservation of electronic evidence. It is important that paralegals be familiar with the steps and guidelines required by the new amendments to the Rules of Civil Procedure and any rules promulgated under state law. Basically, the rules require that a paralegal or attorney identify, preserve, collect, process and review electronically-stored evidence.

The New Amendments to the Federal Rules of Civil Procedure

In 2006, there were six Federal Rules impacted by the amendments to the FRCP, and they were Rules 16, 26, 33, 34, 37 and 45. E-Discovery is formally referred to as "electronically stored information" (ESI) under the FRCP.

At the outset of litigation, the parties must meet to discuss the preservation of ESI under Rule 26(f). Parties have an obligation to create a written memorialization of their agreement regarding the management of ESI. Form 35 must be used for the written agreement.

The FRCP now also requires that attorneys and their teams work with clients to understand how information is stored in computer systems. Paralegals should be forewarned that they may need to deal with difficult issues and questions relating to IT storage of information on computer systems. They may also be in a position of having to probe opposing counsel about his or her storage methods for information.

For the management of ESI, ESI is now information that is discoverable in interrogatories and subpoenas. Parties have an obligation to disclose this information during the discovery phase if requested. The FRCP now provide parties with an important caveat that also should be understood by paralegals. If one's side is not clear in requesting the format that the ESI should be produced in, then the other party has the right to choose a "reasonably usable" format. Paralegals should clearly state the format of production for ESI to avoid receipt of the information in cumbersome forms, such as PDF or Word files that may be difficult to download.

Sanctions Under the Federal Rules of Civil Procedure

Paralegals can learn about sanctions imposed under the FRCP for a failure to preserve ESI, release of ESI or failure to provide ESI to opposing counsel after ordered by the court. This is known as the "safe harbor" provision. If the ESI was lost as a result of the good-faith operation of a computer system, a party will not face any sanctions from the court. However, this may not provide an excuse for an attorney or paralegal who fails to upload a necessary update for a computer program. If the attorney or paralegal was negligent in failing to download anti-virus software or other necessary updates, then he or she may not be protected under the Rule. Courts are still in the midst of interpreting Rule 37(j) through case law, so paralegals should stay aware of any new updates and how a future court may impact a particular rule in light of the case law.

The case of Zubulake v. UBS Warburg is relevant for understanding the obligations a court may impose on a party for production of ESI. In that case, Laura Zubulake was an equities trader for UBS and filed an EEOC claim against the company for discrimination. The company instructed its employees to retain any information related to Ms. Zubulake and her case. During the discovery phase of trial, she requested access to any relevant documents, including electronic information. UBS provided a 300-page response that included emails from leaders within the organization. UBS also stated that it would not produce other emails due to the high cost. The court disagreed and ordered the UBS provide the tapes containing the emails. Prior to this order, UBS had been in a routine of deleting the emails due to the high cost of maintaining them. Because UBS had deleted these emails that were necessary for trial, the court ordered that UBS pay the attorney's fees of Ms. Zubulake. The court also instructed the jury that the destruction of the emails could be considered an adverse inference in regards to the behavior of UBS.

The case should serve as a source of instructive law for paralegals. In that case, the court determined that a party has the duty to preserve ESI as soon as a claim is filed. If a company anticipates litigation, then its duty to preserve ESI will began at that time. A company or legal team should make all efforts to preserve ESI that is relevant and reasonably calculated to lead to the discovery of admissible evidence.

Sources of Electronic Evidence

When considering the sources of ESI that must be preserved, a paralegal should consider those sources that are relevant to the facts of the case at hand. Some of the cases in which ESI is likely to be relevant include:

- Bankruptcy cases
- Antitrust litigation
- Fraud cases
- Employment discrimination cases
- Personal injury cases
- Contract disputes
- Real estate disputes
- Criminal law cases

The types of ESI that are relevant in a case will typically be derived from social media websites, email files, computer files, information stored on smartphone devices and any other information in electronic form. The paralegal should assess the claims and allegations made by the other party to determine whether it is necessary to preserve the evidence. If a person is alleging that he or she was defamed on Facebook, then the other legal team will likely have a duty to preserve any status updates created on the client's account that could be at issue in the case. Deleting any status update that relates to the character of the alleged victim could affect the outcome of the case, and a court could impose severe sanctions for this behavior.

Next, a paralegal should determine how the ESI was created and stored. They should consider the IT systems used to manage the information. A paralegal should take a broad approach in considering any information that could be relevant in the case. He or she may also need to make efforts to communicate with an IT professional to ensure that any relevant evidence is not destroyed under a schedule.

The Duty to Preserve Evidence

There are common sources of ESI that a paralegal may have a duty to preserve in litigation. Email is a common source of ESI that can be relevant in a case. An attorney may have to instruct a client that he or she may not delete any emails from a smartphone, laptop or other PDA. The paralegal may also need to assist the attorney in determining whether the client stored emails in Gmail or any other external websites.

Instant messaging is often a form of relevant communication that may need to be admitted into trial. Any messages or images sent on a phone should be preserved for trial. Deleting text messages that are relevant for trial could result in sanctions against one's party.

Paralegals may also need to work with a company to ensure that no documents are lost on a company database. Companies frequently use programs like Oracle to preserve information. Sometimes, these databases will automatically delete files to create extra space for storage. The paralegal should immediately speak with a company about any program that contains information that could be compromised or automatically deleted. If the evidence is relevant in any way to the trial, then it will be important to preserve it for discovery.

Backup information and network storage devices should also be preserved for trial. A company may place documents on external hard drives, and this information may also be admitted into trial. Throwing away an external hard drive could be considered the destruction of evidence reasonably calculated to lead to the admission of relevant evidence. A court could impose sanctions if a company throws away a hard drive that contains backup information. Paralegals may need to work with an IT department to freeze a retention period and prevent the deletion of files.

How to Preserve Electronic Evidence

Paralegals should have thorough knowledge of the storage forms of computer files. They should understand how to work with the following types of files:

- Word Documents (.doc, .docx, .wpd, and .rtf)
- OpenOffice Documents (.odt)
- Text Files (.txt or .asc)
- Database Files (.rpt or .csv)
- PowerPoint Files (.ppt)
- PDF Files (.pdf)
- Image Files (.tiff, .img, or .jpg)
- Corrupted Files
- Fragmented Files
- Any other common files transmitted over the Internet or stored on electronic devices

Basically, any evidence that could be relevant for a case must be preserved. It will be placed in "legal hold." Paralegals must take care to preserve the evidence and prevent its destruction. It is also important that paralegals do whatever they can to prevent spoliation of ESI. They should not attempt to tamper with files on a computer until they have had any questions or concerned addressed by IT professionals.

A computer forensic expert may be necessary to assist in the process of obtaining data from a computer. The computer forensic expert can also testify in a trial about the important of retrieving certain files from the opposing counsel and what this information could prove.

Attorneys and paralegals should not try to search around a computer for files that they may need for trial. Whether the computer files are from a client or from opposing counsel, it is important that the attorney and paralegal be extremely cautious in dealing with the information. Searching through files could inadvertently cause the destruction of evidence, and one's party could become liable. Even starting the computer or shutting it down could impact the ESI stored on the computer. A computer forensic expert may be able to analyze the data stored on a computer and figure out a way to retrieve files without destroying the ESI. These experts are trained in the methods of identifying, preserving, managing and extracting electronic files.

How to Collect Evidence

If a paralegal is assisting an attorney in gathering ESI, he or she should be aware of Rule 26 (b)(2). This rule entails a two-tier process that allows attorneys to secure access to ESI. A party has the right to retain information if it identifies its existence and that the burden of requesting production shifts to the other party. The other party must then proceed to file a motion to compel discovery or seek a protective order from the court. The party retaining the information must show that releasing the ESI would pose an undue burden and great cost. The judge still has discretion to compel the party retaining the ESI to produce it if the court finds "good cause."

Also, Rule 26(b)(5) may enable attorneys and their teams to retain access to inadvertently produced documents. If another side accidentally releases privileged information, it has a certain time frame in which to send notice to the opposing counsel. The opposing counsel may challenge the privilege in a written communication back to the other side. The court may rule upon the asserted privilege and determine that one side has the right to access the ESI.

Before a case starts, an attorney and paralegal should meet with the client. It is vital that the attorney discuss the importance of being completely honest about any information that could be relevant to the case. The attorney will need to obtain any evidence that could be relevant to the case and determine how to proceed in the treatment of that evidence. It is better that a client proffer any evidence that could be incriminating or that could make him or her liable. If the attorney has suspicions that a client may destroy files on a computer or smartphone, then the attorney should try to impound the device. It is better that the attorney retain control over the device and have the device analyzed by a forensic expert.

Creation of Documents

A paralegal or forensic expert will then need to gain access to files in the computer to create forensic images of the relevant documents. An examiner will need to take notes regarding the condition of the computer and its serial number. The expert may also take notes on the condition of the hard drive. If the hard drive contains dust on it, then this is evidence that the drive has remained within the computer. If the hard drive is totally clean, this could indicate that the client or other individual tried to swap the disk for a new one. The cleanliness of the hard drive could actually raise an inference of improper behavior.

The paralegal or expert should also make copies of the hard drive. The second copy may be admitted if there are any disputes about the original copy.

A paralegal or expert may also be in the position of recovering deleted information. Special computer programs may be required to try to retrieve deleted files that were emptied from a recycle bin or overwritten. Any files that have been overwritten may be an indication that a client was trying to hide certain information.

Paralegals should also be prepared to deal with copies information. Metadata is frequently relevant in cases involving stocks, trading and accounting. A paralegal or expert should track the date in which the information was copied. The dates of creation or copying may be relevant in one's case. A mass copy event could indicate that a client or other individual was trying to evade liability.

E-Discovery and Filing Documents with the Courts

Ultimately, paralegals will need to defer to the local court rules to determine how to proceed in filing ESI with the court. Each court maintains its own local rules in regards to electronic evidence. States have also created their own Rules of Civil Procedure and Rules of Evidence. While it can be helpful to consider the FRCP as an overview of the requirements for handling ESI, a paralegal will ultimately also need to consider local court rules and state law. State law may also put forth the time limits that one has to file certain electronic evidence. A failure to abide by the time periods could have serious consequences on one's case. One may lose the opportunity to request ESI from opposing counsel or to have relevant evidence admitted into one's case.

Paralegals should be sure to work closely with attorneys so that the attorney understands the nature of any evidence retrieved. Any piece of ESI could have a significant impact on the outcome of a case. Paralegals should take care to summarize their findings in a document that can be easily accessed by the attorney. Before deleting any information, a paralegal may also want to consult with the lawyer. The lawyer may understand how a seemingly irrelevant piece of ESI actually does have a relevant place in a case. If a paralegal does delete information, then he or she could be making an error that negatively impacts the attorney's case. It is better for a paralegal to err on the side of caution and seek to preserve the information.

Conclusion

There may be moments when a paralegal feels frustrated in dealing with massive amounts of electronic evidence. If a paralegal feels that he or she cannot handle the complexity of computer files involved in a case, then it may be time for an attorney to seek help from a computer forensic expert or IT professional. These individuals have a thorough knowledge of computer to systems and may assist a paralegal in sifting through a computer to retrieve files that must be preserved for trial. Also, a paralegal should remember to carefully consider the new amendments to the Federal Rules of Civil Procedure in regards to ESI. These rules can provide the information that a paralegal needs to decide whether to preserve electronic evidence. Also, paralegals should search online to find the latest case law updates to determine how courts are applying the Federal Rules of Civil Procedure in regards to electronic evidence. The information included in this document will provide a starting point to assist paralegals in analyzing the electronic evidence offered by clients of opposing counsel.