

# Kroll Ontrack®

## E-PITFALLS<sup>i</sup>

Linda G. Sharp and Michele C.S. Lange<sup>ii</sup>

The phrases “electronic evidence”, “e-discovery”, and “computer forensics” do not appear in the latest edition of *Black’s Law Dictionary*. Yet, now more than ever before, attorneys are finding that a basic understanding of technology (and in some cases thorough computer proficiency) is essential to effectively litigate a matter. No longer can parties or their counsel claim to be unaware of digital data. Instead, judges are expecting e-savvy litigators in their halls of justice. Since it is easiest to learn from others’ oversights, this article analyzes some of the most common mistakes litigators and parties have made while dealing with electronic evidence.

1. Having no electronic discovery plan or pursuing discovery of electronic evidence in a haphazard manner.

With a majority of all written data now stored in electronic form, gone is the day when an attorney is likely to find the “smoking gun” document in a box located in a remote storage facility. Litigators who take the time to learn what e-evidence is, how to find it, how to use it, and how to avoid problems when dealing with it increase their chances of prevailing in a case and avoiding judicial sanction. Today, almost every case strategy should include an electronic evidence component, which details a comprehensive plan for collecting, analyzing, and producing digital data.

2. Not understanding that delete does not mean delete.

Far too many educated and sophisticated business professionals have learned this lesson the hard way. State and Federal case law is full of civil and criminal decisions where the individual did not understand that the “delete” key on the keyboard is not the equivalent of the paper shredder. Each and every electronic document leaves an electronic fingerprint. This fingerprint is then stored or captured on the hard drive, even if all that you do is open a document from a floppy drive and send it to the printer. The fingerprint remains magnetically embedded on the drive (and ripe for the picking by computer forensic experts) regardless of the fact that you direct the computer to “delete” the data. Only until you resave over the fingerprint, which typically occurs when the all hard drive space has been utilized, might the fingerprint disappear for good.

3. No backup policy or document retention policy.

A document retention policy, or more appropriately called a “document destruction policy”, involves the systematic review, retention, and destruction of documents received or created in the course of business. In most cases, the existence of a document retention policy may be a mitigating factor when documents are destroyed according thereto. On the same token, a company’s failure to have a document retention policy may raise red flags. The bulk of the retention policy should include a method for determining retention periods, the retention schedule, the retention procedures, and a records custodian. Close consideration must be given to specific state and federal statutes/rules that govern document retention time periods for certain classes of records and certain industries. The policy should also create an index of active and inactive records and implement “log books” in which all destroyed documents are recorded. Lastly, the policy should be revisited regularly to assess whether discovery obligations raised by litigation or changes in the way the business operates or uses information warrant modifications.

# **Kroll Ontrack®**

## 4. Failure to fully discontinue document destruction practices.

A corporation cannot blindly destroy documents and expect protection from a document retention policy. In the wake of pending or impending suit, your clients must immediately halt all electronic document-handling policies that result in intentional and negligent destruction of potentially relevant evidence. It is critical to reach the individuals that actually carry out the document destruction to ensure that preservation is properly and completely enacted. Too many situations arise where the individuals tasked with the destruction state, "I didn't realize you meant me." It is also important to discontinue any automated document destruction programs.

## 5. Ignoring certain "hard to deal with" sources of evidence.

It is easy to ignore "hard to deal with" media types, such as out of date backup tapes or hot off the market personal digital assistants or electronic tablets. However, many times these media sources are where the smoking gun documents are located. No longer is it appropriate to hide behind the technology, claiming that the systems are too antiquated, damaged, or burdensome to be searched for responsive documents and email. There are a vast number of experts that are well-equipped and professionally trained to assist you. The important thing to do is get them involved early. Do not wait until the court issues an order demanding production of electronic information. Additionally, far too often opposing counsel is quick to say, "I want it all." The electronic evidence expert can work with you to define and refine the universe of potentially relevant information and determine the most cost effective way to retrieve that data.

## 6. Underestimating email use.

Employees create more electronic evidence than you think. Many parties have found themselves in the middle of a landmine for not producing electronic evidence from custodians that seemingly "do not use their computers much." You might be surprised to learn that sometimes seemingly "e-phobic" individuals have their assistants retrieve and respond to email on their behalf. Thus, it is imperative that those individuals' email boxes be reviewed if potentially relevant data might be found. Keep in mind, if the Court issues an order directing retrieval, or worse yet, the opposing party happens to have email from that individual and those records were not produced, it could give the appearance of impropriety and may lead to sanctions.

## 7. Claiming to have produced everything or turning over electronic data late in the game.

Technological developments have not caused courts to waiver when admonishing or sanctioning parties for bad faith maneuvering or rule violations when it comes to electronic discovery. Caselaw has held that where a party breaches a discovery obligation by failing to produce e-evidence or excessively delaying in producing e-evidence, the trial court has broad discretion in fashioning an appropriate sanction. Such sanctions can include delaying the start of a trial, declaring a mistrial, issuing an adverse inference instruction, or ordering monetary penalties. Sanctions may be imposed where a party has not only acted in bad faith or grossly negligent, but also through ordinary negligence.

## 8. Failure to image hard drives of departing employees.

It is important to have a policy in place for handling the electronic business records of all departing employees. Often times a simple bit-by-bit hard drive image may be extremely useful in the event litigation ensues. There is nothing more frustrating to a litigator than to be in the midst of discovery and hear "that information is on John's laptop and we let him take that out-of-date machine with him when he left" or "Sue is now using John's computer." The costs

# Kroll Ontrack®

associated with imaging a hard drive are minuscule compared to the costs involved in later attempting to locate and, if possible, retrieve the data later on down the road.

## 9. Inexperienced people conducting well-intentioned computer forensic investigations.

When an incident occurs, there is a strong tendency to have the security or technical staff “take a quick look” at the suspect’s computer in an attempt to confirm or deny suspicions. Unfortunately, the act of “taking a quick look,” if not carried out using proper computer forensic protocols, most often results in unintended and unnoticed changes to the digital files. For example, simply booting a computer can destroy temporary files and change file dates/times. Problems may arise when that employee must be called to testify as to what happened and how the computer evidence may have become tainted.

## 10. Shouldering the electronic discovery burden alone.

Some companies choose to handle electronic discovery requests in-house on a case-by-case basis. However, as one author recently noted, “It is unrealistic to assume that I.T. professionals can pay attention to all the nuances of litigation, manage the lifecycle responsibilities associated with email, and enforce an overall email archive policy. Companies will be caught off guard by assuming that I.T. can shoulder this burden alone.” I.T. professionals are well-informed about their company’s systems, data locations, media types, software use, and data retention policies. Yet, this wealth of information does not give rise to an expertise in the area of e-discovery. Depending on the complexity of the technology involved, intricacy of the request, judicial deadlines, exposure to liability, and diversion of internal staff, you might want to consider consulting an electronic evidence expert (check their credentials) to help maneuver around any potential stumbling blocks.

All in all, keep in mind that whatever would have been discoverable in the paper world is discoverable in the electronic world, and then some. In the old days, counsel would spend weeks, if not months, in a dusty warehouse full of boxes, reviewing each document for responsiveness or privilege and then producing them “as they are maintained in the ordinary course of business.” This would necessitate the opposing party, accompanied by counsel to then sift through the same documents in the same dirty warehouse for months on end. Technology is creating solutions at breakneck speed that can help you find that needle in the haystack instead of spending months sifting through paper documents to never find it at all.

---

<sup>1</sup> This article appeared in the June 16, 2003 edition of the Daily Journal. Copyright 2003 Daily Journal Corp. Reprinted and/or posted with permission. This file cannot be downloaded from this page. The Daily Journal’s definition of reprint and posting permission does not include the downloading, copying by third parties or any other type of transmission of any posted articles.

<sup>ii</sup> Linda G. Sharp, Esq., MBA ([lsharp@krollontrack.com](mailto:lsharp@krollontrack.com)), a Legal Consultant, and Michele C.S. Lange, Esq. ([mlange@krollontrack.com](mailto:mlange@krollontrack.com)), a Staff Attorney based in Eden Prairie, Minnesota, work for Kroll Ontrack Inc., a company specializing in the collection and production of electronic evidence. Ms. Sharp and Ms. Lange have published numerous articles and speak regularly on the topics of electronic discovery, computer forensics, and technology’s role in the law. [www.krollontrack.com](http://www.krollontrack.com).