

Manage Your Electronic Data or Risk Litigation Disaster

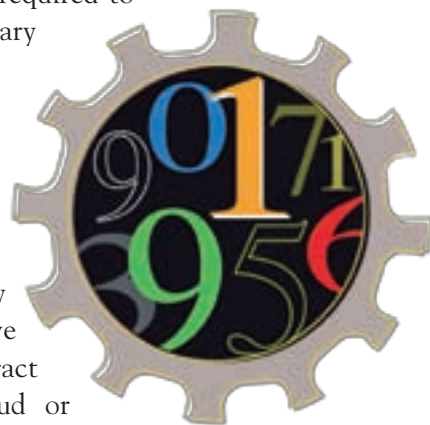
In the “old” days, evidence in a lawsuit primarily took two forms: paper documents and witnesses’ testimony. Anything that had not been put down on paper (and kept) was subject to the competing recollections of those involved—if no one remembered it, for all practical purposes, a statement had not been made. Today, the various types of electronic data have become so commonplace as to render paper documents and witnesses’ memories considerably less important. Consequently, the existence of electronic data has transformed civil litigation.

The notion that one shouldn’t put in an e-mail or instant message something one wouldn’t commit to paper is not news—no matter how frequently it continues to happen. If a communication occurred electronically, by whatever means, it can be uncovered in discovery and can often then be used at trial. In fact, the mere existence of electronic data (regardless of its content) presents problems for a party to a lawsuit, problems that can only be avoided by steps taken long before the lawsuit begins.

A party who enters litigation without having a fairly clear understanding of the potentially relevant electronic data in its possession faces two very real dangers: the party will either (1) have to spend substantial time and money to determine what exists and how it can be processed to ensure that all potentially relevant data has been identified or (2) risk the very real possibility of court-imposed sanctions

for failure to produce relevant evidence. Such sanctions could include a so-called “adverse inference”—in which the jury is permitted to conclude that evidence that no longer exists would have been harmful to the party who no longer possesses it—or substantial monetary payments that may be imposed independent of the outcome of the lawsuit. Parties have been required to pay onerous monetary sanctions for having failed to produce relevant electronic data during a lawsuit, regardless of whether the party was found to have breached the contract or committed fraud or what have you, in the underlying dispute.

What can you do to avoid either of these circumstances? You could try to get the rules governing electronic discovery changed, but despite a recognition that electronic discovery has increased the costs of litigation beyond reason, that is not likely to occur soon. What you can do instead is get a handle on what electronic data you and your employees generate, how it is maintained, and how (and when) it is destroyed. You can do it internally, using your own resources, or you can hire someone to conduct such an inventory for you. > [Continued](#)





What is an “electronic” document?

In a lawsuit, each party asks the opposing side to produce potentially relevant “electronically stored information,” which can include anything that exists and is reasonably accessible (and sometimes even information that is not reasonably accessible), such as word processing documents, e-mail, databases, spreadsheets, images (photographs, PDFs, PowerPoints, etc.), instant messages, records of chat room conversations, audio recordings, and video recordings, whether stored on a server, a desktop computer, a notebook computer, a netbook, a smartphone, a not-so-smart cellphone, a DVD, a CD, an external hard drive, a flash drive, an SD card used in a camera or telephone or MP3 player or audio recorder, a backup tape, or on the internet (whether in the form of a backup or in a web-based repository such as Google Docs or Zoho), and whether stored on equipment owned by the party or equipment that is in some manner accessible to the party, whether through its employees, a vendor relationship, or otherwise. And that listing is merely illustrative and by no means exhaustive.

Those who operate under regulatory compliance regimes of one sort or another (whether Sarbanes-Oxley or industry-specific regulation) should already have a clear understanding of what electronic documents they generate as well as where those documents are stored and when they are destroyed. But for the rest of us, the prospect of having to respond to a discovery request that requires production of electronic documents should be enough incentive to prompt an electronic document inventory. Such an inventory would include not only storage on company resources but would also include storage of any company “documents” on employees’ personal computers, cell phones and in the so-called “cloud” of web-based repositories.

If such an inventory reveals a somewhat haphazard approach to the storage and destruction of electronic documents, the company should seriously consider adoption and enforcement of policies to regulate the storage and destruction of those documents. The policies with respect to storage of electronic documents will, if followed (a big if), give a litigant a significant head start in dealing with discovery obligations in a lawsuit. Also, when a document has been destroyed pursuant to a longstanding document retention policy (rather than in a one-time act committed days after the lawsuit was filed), the party who destroyed the document will usually not face any sanctions related to the document’s destruction.

As with much preventive maintenance, the cost of such an inventory may cause one to put it off. However, if the day arrives when one is faced with the tremendous cost of collecting and producing a hodgepodge of electronic data (or the equally unattractive risk of being sanctioned for failure to produce such data), then the cost of such an inventory and implementation of retention policies will pay for itself many times over.

By Mike McCarthy |



Mike McCarthy represents business entities and individuals in appellate and complex business litigation (principally class actions) in areas such as consumer and securities fraud, fiduciary breach, antitrust, and environmental contamination. mike.mccarthy@maslon.com