

The Brave New World of Document Retention

Delete, delete, delete....This key on a computer keyboard is used to eliminate a word or sentence from written text and connotes a sense of finality. It is important to note; however, the simple delete stroke of the key does not permanently erase the data from the computer. The delete key has the potential to change the address or reference point for the data. **IT DOES NOT ACTUALLY DELETE THE DATA FROM THE HARD DRIVE!**

Deleted data on a computer becomes hidden data that exists and is accessible with the proper tools. Data may be destroyed through the use of certain software programs; however, the use of this software is not a fail safe method and may be dangerous. Permanently destroying data requires physically destroying the hard drive of the computer and is not a recommended act.

The destruction of electronic data and documents may have severe implications for all businesses. In several high profile cases the successful destruction of data resulted in unintended consequences. It is imperative for businesses to effectively communicate to its employees

that "deleted" data does not actually disappear, and in fact may be recovered. This fact is extremely important to the well being of the business and the employee.

A second concern for business with respect to data retention is the retention of relevant electronic evidence. In today's business context a comprehensive and frequently updated data control policy is essential. An effective document retention policy will include back-up procedures, archiving, and other systematic fail safe mechanisms for retention of data.

Understanding the issues related to the retention and destruction of documents is critical and should be based upon industry standards and specific circumstances. The same factors apply to email, voicemail, and instant message logs.

The Federal Rules of Civil Procedure and several high profile cases have highlighted the need for effective data control.

The Federal Rules of Civil Procedure have recently been modified to address the discovery

of electronic documents and information and have heightened the applicable standards and penalties. In order to comply with the modifications to the procedural rules, businesses are required to develop and implement retention policies regarding electronic data. It is equally important for companies to develop and implement programmatic changes that are designed to efficiently access and search for data. Deleted data, meta data, voicemail, temporary files, all forms of e-mail, backup tapes and other forms of electronic information have been found admissible and discoverable under the new discovery rules.

It is also important to note that that storage media found in PDAs, Blackberries and laptops have been found discoverable. In addition, "deleted" data is actually evidence of intent to destroy. The importance of developing retention policies and procedures for electronic data is evidenced by the significant fines and sanctions that have been imposed upon corporations found to be in violation of discovery rules. Examples of the costs associated with non-compliance are:

§ \$10 million fine by the SEC against Bank of America;

§ \$ 8.25 million fine imposed by the SEC upon 5 different financial firms;

§ \$ 2.75 million fine imposed by US District Court on Altria; and

§ \$ 1 billion judgment against Morgan Stanley for electronic discovery related issues.

The case of Zubulake v. UBS Warburg, LLC demonstrates the importance of implementing effective policies relating to electronic data. Zubulake was an employment discrimination case in which the court found that UBS employees attempted to destroy relevant evidence by deleting emails and other data from their computers.

Even though corporate counsel and outside counsel informed all employees to halt any data destruction prior to the destruction taking place, the company was found to have willfully destroyed relevant evidence, a finding that eventually lead to a punitive damages judgment in excess of \$20 million dollars.

It is fair to say that courts will not stand for the "accidental delete" excuse and hitting the delete key on your computer may have financial legal and financial implications that are disastrous.

This outline is not a complete analysis and may not be relied upon as legal advice. Please contact Gary R. Pannone, Esquire for further consultation at 401-824-5115 or send an email to him at gpannone@pldw.com