COLLINS COLLINS MUIR + STEWART LLP
ATTORNEYS AT LAW

When is it Safe to Delete Electronically Stored Information?

Computers have made communicating with clients, sharing documents, drafting details, accessing information and hundreds of other tasks quicker and easier, increasing efficiency in the work place. Advancements in software and data storage have made the retention and dissemination of large amounts of information the norm. Storage rooms that were once lined with box after box of paper files have been replaced with comparatively compact servers and back-up drives.

Then, over a dozen years ago when we were hit with the realities of preparing for "Y2K," individuals and organizations around the world were frantically backing up their electronic files and systems in an effort to save the computer data that was becoming so critically important to everyday life. Now, over a decade later, companies and individuals are doing everything they can to delete and destroy electronically stored information they fear could hurt them in a lawsuit or arbitration or just because storing it has become too costly. In this information age where engineers are bombarded with seemingly endless e-mails and electronic data, a new spin on an old problem has come to the forefront: when is it safe to delete electronically stored information?

ESI and the Courts

Electronically Stored Information ("ESI") is becoming an increasingly important part of the litigation discovery process throughout the country. Plaintiffs and defendants alike are seeking recovery of electronic files, emails, system server information, even text messages and "Tweets" or Facebook messages, and the courts are increasingly willing to allow this discovery to proceed. This signals an alarming trend for businesses potentially faced with not only having to save ESI, but to also assist the opposition in recovery efforts to produce ESI stored on computers, networks, onsite and offsite servers, and even cell phones and tablets.

At least initially, the courts were reluctant to impose sanctions or to delve too far into the electronic landscape, but this is changing. Perhaps it was simply a function of the law lagging behind the hard disk or an older judiciary being replaced by tech savvy judges, but over the past couple of years there have been a series of decisions, many of them coming out of the 9th Circuit Federal Court (the Federal Circuit for California and several other Western states) and the rulings are predominantly in favor of saving and producing electronically stored data.

9th Circuit's Message is Save That Data!

The first question anyone should ask is: "What kind of data do I have to preserve when a claim or lawsuit has been made again me or my company?" In California, the answer may well be anything that is potentially relevant evidence in your possession or control. This may include information and ESI on computers, laptops, and even portable electronic devices, and the duty to protect this information extends to what one court has

called the “key players” of an organization. A “key player” is someone in the organization that has access to relevant information that is associated with the claims or disputes at issue in the case.

So what happens when a “key player” decides to delete or destroy ESI they know to be relevant to the dispute at hand? If the court determines the loss of data (called spoliation of evidence) substantially denies the opposing party’s ability to support or defend a claim, the answer may be expensive sanctions and even dispositive rulings against the party destroying the ESI.

The determination of whether or not it was reasonable for ESI to be destroyed is becoming a careful balancing act, and some California courts have already ruled that a showing of bad faith is not required. This means the party seeking the ESI may not even have to prove the deleting party acted improperly; instead, all that must be shown is the deletion or destruction of the ESI was negligent or that it was somehow disobedient conduct that resulted in the loss of data that could have been relevant. Additionally, some judges (outside the 9th Circuit) have even recently handed down decisions where sanctions were granted over deletion of ESI that included jail time for flagrant attempts to delete ESI during an ongoing proceeding.

Standards and Safeguards for Engineers to Comply with ESI Requirements

With the threat of sanctions, dispositive rulings, and even jail time in some states all looming over our heads, the real issue today regarding ESI is how companies and individuals can protect themselves and what safeguards need to be considered.

At the very least, sound document retention (and destruction) policies must be in place in every organization and must be strictly followed. Any deviation from these policies is cause for alarm. For most companies, document retention policies are already in effect. What these companies need to do now is make sure their retention policies extend to ESI and that the information is being properly handled in compliance with the stated policy. Putting this safeguard in place protects the data and also helps to avoid the appearance of impropriety if and when disputes arise.

Beyond standard data retention, all businesses need to recognize that once a dispute has ripened into litigation, there is a very real possibility that a court is going to place strict requirements on the parties to ensure data is not lost or deleted. In many situations, a “litigation hold” is sent out by the opposing party demanding retention of ESI. Often, these “litigation holds” demand that a party must not erase, destroy, alter, or otherwise dispose of any document or ESI. It is generally a sound practice for a company to self-impose a litigation hold on all materials and ESI related to a specific project or issue once there is an existing claim or the potential for one.

As our business world continues into the 21st Century, electronic data will only continue to grow in importance, and every indication is that courts will continue to recognize ESI

as an integral part of the discovery process. It is important that you protect yourself and your business by creating and implementing document retention and destruction

policies. You never know—saving that email may someday, in a lawsuit, save your business!

Please contact us at the Oakland, South Pasadena, Orange, or San Diego offices to discuss further.

Samuel J. Muir, Esq.
1999 Harrison Street
Suite 1700
Oakland, CA 94612
Ph: (510) 844-5100
Fax: (510) 844-5101
smuir@ccmslaw.com
www.ccmslaw.com

Christian E. Bredeson, Esq.
750 The City Drive
Suite 400
Orange, CA 92868
Ph: (714) 823-4100
Fax: (714) 823-4111
cbredeson@ccmslaw.com
www.ccmslaw.com

Robert R. Walker, Esq.
1100 El Centro Street
South Pasadena, CA
91030
Ph: (626) 243-1100
Fax: (626) 243-1111
rwalker@ccmslaw.com
www.ccmslaw.com