



## MessageWatcher® – E-mail Archiving and Surveillance

E-mail • Instant Messages • Tweets • Facebook Postings • LinkedIn Updates

Solutions for regulatory compliance, eDiscovery or simply reducing the risk inherent in employees' electronic communication.



## Don't Get Bitten By the eDiscovery Related Amendments to the FRCP

As you may be aware, on April 12, 2006 the U.S. Supreme Court approved a set of amendments to the Federal Rules of Civil Procedure (FRCP). These amendments pertain to how litigants must respond to electronic discovery (eDiscovery) requests in federal court cases, effective December 1, 2006. These amendments have placed vitally important demands on all companies, and even in some cases individuals, to look at how they store their electronic data, for how long, and in what forms.

### The Discovery and eDiscovery Process

To understand the ramifications of the amendments to the FRCP, it is important to understand the role of discovery and eDiscovery in litigation. At the start of litigation a conference between all parties involved in the case takes place. At this conference both sides will ask the other, under oath, about any information they may have which pertains to the case at hand.

The FRCP, with regard to discovery, for years has mandated that each side of a court case is obligated to produce the reasonable information asked for by the other side. A simple example of this would be in the case of an ex-employee suing for wrongful termination. The attorney for the ex-employee would ask for copies of their employment files, performance reviews, etc... This is considered discovery in the most classic sense.

eDiscovery is further defined as electronically stored information. FRCP 26(a) was amended to say that all parties are obligated, early in their case proceedings, to share with the other party the existence of all electronically stored information relevant to the case. With FRCP 16(b) both sides are obligated to hold a discovery conference early in their case, talk about eDiscovery, and the electronic information pertinent to the case.

In the case of electronically stored information, such as e-mail and other electronic information, companies are now required to produce anything relevant to the case or be able to explain why they no longer have the relevant information available. In the example above this means that the attorney for the ex-employee could ask the previous



## MessageWatcher® – E-mail Archiving and Surveillance

E-mail • Instant Messages • Tweets • Facebook Postings • LinkedIn Updates

---

**Solutions for regulatory compliance, eDiscovery or simply reducing the risk inherent in employees' electronic communication.**

employer for all e-mail from their managers and supervisors that related to the employee, for the last five years. The company then must respond by producing the information or with an explanation as to why they are unable to produce such information. A simple "it was destroyed" or "it was not backed up by our technology staff" are no longer acceptable answers under the amendments.

If the party of a case asked to produce the electronic information is unable to do so, they may have very stiff sanctions placed on them by the court. They may also face the reality of a judge telling a jury to assume they purposefully destroyed the evidence and that it is considered to have been of harmful to their case!

### **What is considered "Electronically Stored Information?"**

Electronically stored information (ESI) is not clearly defined by the amendments to the FRCP. However, in recent case law where these amendments have come into play, it has been shown that just about any electronic information is fair game. This means that the courts can expect you to produce computer files, intact e-mail messages with metadata attached (creator/sender, creation date, receivers, routing details, and subject line of the message), instant messenger logs, data contained on handheld devices and cell phones, and even stored voice-mail messages.

Think about this for a moment and understand the ramifications for any person or businesses who may end up in a federal court. What if you, or your business, were to be asked to produce electronic information in a court of law today? Could you produce all reasonable electronic information in an eDiscovery situation if asked to?

### **What is Reasonable and What Isn't?**

Thankfully the amendments to the FRCP allow for the reality that not all electronic information ever created can be stored indefinitely. FRCP 26(b)(2) says that all relevant and readily accessible electronically stored information is discoverable and that which is not readily accessible is not discoverable. This does not mean that if you have a million e-mail messages stored, with no index, that you cannot be expected to find all messages from "John Smith" in that archive. However, it does mean that if you have a policy of deleting e-mail archives every three years, then any files before that time are not discoverable and you would likely not be sanctioned by the court for not being able to produce them.

### **Information Technology Impact and Suggestions**

It is clear by the amendments to the FRCP that businesses need to find a new ways of dealing with their electronically stored information. Simply allowing things to be deleted



## MessageWatcher® – E-mail Archiving and Surveillance

E-mail • Instant Messages • Tweets • Facebook Postings • LinkedIn Updates

---

**Solutions for regulatory compliance, eDiscovery or simply reducing the risk inherent in employees' electronic communication.**

at the will of their IT staff, or because a backup tape is needed for another use, is no longer acceptable practice and has the potential to cost a company millions of dollars.

At the beginning of litigation, at the eDiscovery conference, each side will need to be able to explain their corporate policies on electronic information and what data is available, what isn't, what form is it in, and why things may not be available at all. They will also be tasked with explaining how ominous it would be to retrieve such information. Case law to date has proven that while it may be an ominous task to retrieve the information, the company may have to do it anyway.

It is in every companies best interest to address the issues of the amendments to the FRCP sooner rather than later. This is one of those situations where a business can hope they are never in this position, but must be prepared for a day when they might be. Just as one would prepare for a natural disaster, one should also prepare preemptively for possible future litigation as much as reasonably possible.

To prepare for possible future litigation, a company should have its Information Technology Department and its Legal Department on the same page as to exactly what the corporate policy on electronically stored information will be. A solid plan needs to be put into writing, and into action, as to how data will be stored, indexed, retrieved, and for how long.

In the amendment 37(f) the rule clearly states that if litigation is happening, or will likely be in the near future, all routine destruction of electronic data must cease. The minute a suit becomes even a remote possibility it is then time for a company to stop deleting anything from its computers, servers and backup tapes.

### Conclusions

While the amendments to the FRCP appear daunting, if they are not taken into account before any litigation could arise, they would surely be insurmountable and potentially very costly. This really is a case where an ounce of prevention is worth a pound of cure. It is vital to make a plan, ensure it is legal and conforms to the amendments to the FRCP and current case law, and then require technology and legal teams to sign off.