



The New Federal Rules of Civil Procedure

Are you in the 7% who are ready —
Or the **93%** who are not?

93% of US companies are not prepared

Pike & Fischer's report means that despite over 5 years of drafting, reviewing, debating and publishing - along with review and acceptance by the US Supreme Court - 93% of companies and organizations in the United States are not prepared to comply with the demands that electronic discovery now carries!

- 62% of IT personnel surveyed have nobody in charge, or do not know who is in charge, of implementing the company's processes for supporting the new federal rules (Computerworld)
- 81% of the time, corporate policies are put in place and managed by IT—NOT the business decision-maker or legal expert (IDC)
- Email data stores are growing 42% year over year with 51+ billion solicited email messages sent each day (Radicati Group)
- 35 – 45% of mission critical data lives in the mail store and is unchecked or unmanaged (IDC)

In their conclusion to the recommended changes to the FRCP, the Advisory Committee stated "Electronically Stored Information (ESI) has the potential to make discovery more efficient, less time consuming and less costly, if it is properly managed and effectively supervised." Looking at the statistics above, it is clear that the majority of companies currently cannot properly manage or effectively supervise their ESI.

In a recent study, legal analyst and publishing firm, Pike & Fischer, reported that only 7% of corporate counsels thought their companies were prepared for the changes in the new Federal Rules of Civil Procedure that went into effect on December 1, 2006.

What changed and why does it matter?

The new rules mandate that the parties to a lawsuit prepare for a scheduling conference to address plans for Electronic Discovery and document production after the filing of a lawsuit. The rules also state that parties must sit down prior to this conference to agree on forms of procedure or protocols for the ED portion of the lawsuit. At this "meet and confer", attorneys representing the parties to the suit must be prepared to discuss:

- "Any issues relating to preserving discoverable information"
- "Any issues relating to disclosure or discovery of ESI, including the form or forms in which it should be produced"
- "Any issues relating to claims of privilege or protection as trial preparation material"
- If a party is going to assert that specific data is not "reasonably accessible", they must be prepared to identify what the data is, where it resides and justify why it is not reasonably accessible

Unlike prior to December 1, 2006, where it could take a case a couple of years after filing to get to the discovery stage, the scheduling conference must occur within 120 days of the filing and the "meet and confer" must happen 21 days prior to that. That leaves only 99 days to prepare for this meeting after a suit is filed.

Ask Your General Counsel or Legal Department

- Do we have a complete inventory of all our email messages & attachments, preferably in a single site?
- Are all of our email messages & attachments full-text indexed to allow comprehensive searching of all data?
- Can we quickly sort and segregate email data based on privilege or responsiveness & tag it for future use?
- Can we quickly initiate or maintain a default "litigation hold" on email?

Ask Your CIO or IT Director

- Can you easily grant search access to all or part of your email data in a single archive?
- How expensive would it be for you to search every online email server and offline (backups and PSTs/NSFs) for messages for keywords and people?
- If you could meet the new FRCP requirements while reducing storage up to 70%, would you?

The Cost of Doing Nothing

Sanctions. Summary Judgment. Dismissal. All of these are possible costs of not meeting the new rules. Also, if you do not have all of your discoverable information in a single archive location for easy search, "looking" is the expensive part of discovery. In a recent case, *Murphy Oil USA, Inc. v. Flour Daniel, Inc.*, the cost estimates to simply search for responsive email, based on a narrow scope of discovery, was 6 months and \$6.2 million, excluding attorney time—prohibitively expensive and well past the deadline under the new rules.

Now, more than ever, a company will be expected to have and maintain an accurate and complete inventory of their ESI, be able to initiate litigation hold on a moment's notice, have a eDiscovery team and systems capable of responding to the drastically shorter production timelines for ESI, and be prepared to accurately find, review and produce all responsive electronic information. In order to do that, once the policies and teams are in place, companies will need tools to help meet these obligations.

MailMeter is a Solution that Can Help

MailMeter software offers the capability to meet the new, and existing, requirements for capture, retention, discovery and production of email. Given the fact that 60% of the ESI the new rules apply to is email, it makes sense for a company to begin their process for supporting the new rules with an email archive solution.

MailMeter will capture all existing information in an environment, including PST and NSF files, and, through the use of journaling, will ensure the capture of all future information sent or received. Using MailMeter, end users can access their archived mail to search or display message and attachments, but they are unable to alter or delete these files. Using this methodology, all email users in a MailMeter environment are, in effect, always on a "litigation hold" status. There is no danger that users will accidentally delete or destroy mail that should have been preserved in accordance with the new rules.

In addition, you can safely eliminate PST and NSF files or other "unmanaged archives" from the environment to further reduce your costs and risks. The inability to accurately identify and search the email within their organization was the primary driver behind the \$1.4 billion judgment against Morgan Stanley in 2004.

Trustworthiness Is Key

MailMeter offers an ability to verify the integrity of email messages and attachments through the use of a unique 40-character identifier created from the content of the message and attachment. For each and every message processed, MailMeter encrypts and compresses the component pieces of the message and attachment and assigns the 40-character identifier. On demand, this process can be run again and the resulting ID tag is compared with the original. Since the tag is created using the content of the message and attachment, the IDs can only match if there have been no changes to the file. Once the tags are compared and match, the integrity of the message is verified.

Evaluate Your Risk

To see an online demonstration of MailMeter or arrange a privileged assessment of your risk from a leading law firm specializing in eDiscovery, you can visit our website. Also available for download are product evaluations, white papers, case studies and additional information on how MailMeter can provide a positive Return on Investment in the first year of use.

For More Information

Waterford Technologies is a leader in Email Management solutions that provide structure, metrics and business insight for corporate email activity. By storing all incoming, outgoing and intra-company email headers, subject lines, domains sent to/from, attachments and body text, in a dedicated database and archive, our MailMeter solution allows organizations to dramatically improve corporate governance, regulatory compliance, and employee productivity. Our customers typically generate an ROI of 100% on their first search project.

Web: www.mailmeter.com
 Email: sales@mailmeter.com
 Phone: 949-428-9300

Offices and resellers in major cities worldwide.

WATERFORD
TECHNOLOGIES