



Amended FRCP Rocks the Data Center

Index

The New Rules	2
Impacting the business.....	2
Remember the Metadata.....	3
Preserve the Safe Harbor.....	3
Conclusion.....	4
Get the Help You Need	4
About C2C	4

Overview

On December 1, 2006, the Federal Rules of Civil Procedure was amended to provide expanded definition and structure to the newest class of legally discoverable business data: electronically stored information (ESI). Data management will never be the same. In a nation where litigation is a continuing threat, companies cannot afford to ignore the new rules. Neglecting the rules will send litigation costs soaring in the form of ad-hoc electronic discovery procedures and meaningful court sanctions.

With this in mind, having a rapid Discovery system in place is colossally important. The dangers of litigation in Federal and State courts are not confined to multi-million dollar corporations. The smallest company can face financial and market devastation from litigation, legal fees, court costs and settlements. It makes no sense to assume the risks of additional court sanctions dependent on rules violations.

The New Rules

The new rules are evolutionary, rather than revolutionary. In simplest terms, they are designed to clarify that e-discovery is now a part of traditional discovery. The amendments provide for roughly equivalent treatment of electronic documents and paper documents. It is the implementation of these rules that potential litigants need to consider. Organizations that fail to comply with these rules face a variety of sanctions, including adverse instructions, default judgments and even monetary fines. Even worse, they risk losing cases that otherwise would have been won or favorably settled.

It is important to note that there are not substantive requirements, guidelines or directives under these new rules that you can pull out and implement. Much like the existing discovery rules, the new amendments are directed to the ways lawyers and courts handle and conduct cases in the federal court system (and in many, if not all, states). They deal with the ways electronic information will be gathered and produced in the litigation context. They do not mandate records management requirements. As a result, organizations have not found the clarity and certainty they might have expected from the new amendments. A look at some of the impacts is in order.

Impacting the business

Rules 16 and 20 are amended to provide the court early notice of e-discovery matters. Specifically, 16b states that the scheduling order must include "provisions for disclosure or discovery of electronically stored information." Rule 26f requires that parties discuss any issues relating to preserving discoverable information and develop a proposed discovery plan.

These rules accelerate matters. A party to litigation literally needs to have ESI available for assessment and analysis earlier in litigation than ever before...even before the decision is made to fight the case or settle it. It is also clear that the number of cases subject to rapid case assessment, "litigation holds" on information otherwise scheduled for retirement, evidence preservation and collection will increase.

To a business, all of this means that a full dress management program is necessary to preserve, protect and track data throughout its lifecycle. Management, financial management, IT and legal counsel will have to interoperate to install a data management and security infrastructure.

While every kind of data object is covered by the new e-discovery rules, email is significant. Emails are now business records within the meaning of the statutes, and their preservation and retirement are important considerations in considering a data management strategy. It will come as no surprise to those who read the New York Times or the Wall Street Journal on a regular basis that email often forms the basis for civil and criminal investigations of the country's largest corporations. Astute attorneys and their investigators will infallibly request the laptops and email servers hosting information relating to a particular individual or project, understanding that email prove or disprove the elements of the matter or investigation. Dealing with server data, such as Microsoft Exchange or Lotus Notes email, or some other type of data, requires specialized software and handling. Some large corporations have legacy, proprietary e-mail systems that may need data conversion to a more common format in the interests of ease of restoration.

Without a reliable and tested program in place, a business could spend so much time locating emails, text files, graphic elements, and spreadsheet data that time to analyze what is essential and what is not is severely limited. Without reliable data security, a business will have problems with establishing that the information is reliable and that evidentiary data is genuine. Massive disruption to productive work could result without a program in place. The program's solutions should be formed to fit the needs rather than imposing solutions that are cumbersome or impose unwanted overhead/costs.

The program will require a cross-discipline approach to data protection and security. It should include data classification software, archiving software for emails, databases and such unstructured data as text files and graphics files. Some companies sell archiving as the only solution to discovery, so "buyer

beware” is the rule when selecting supporting software. Security should include access control, authentication, and other protections in hardware or software to assure data authenticity.

Beware of “compliance-only” products, be they software or appliances. They may not cover the relevant data required by e-discovery. Unlike well-known and much-discussed regulations, including Sarbanes-Oxley (SOX), SEC regulation 17, FDA 21 CFR part 11 and HIPAA that may only impact certain businesses and certain classes of data, the FRCP, while not a regulation, has a much broader impact on those who may be involved in future litigation.

Remember the Metadata

Data preservation cannot be confined to the data alone. Metadata needs to be reliably preserved as well. Metadata, among other things, routinely includes file name, location, the file’s originator, and the file’s date. Discovery questions often revolve around “who did what and when.” Therefore, metadata is probative and discoverable. A treasure trove of potentially damaging information hides in plain sight beneath the surface of today’s electronic documents. Although we see the occasional newspaper story announcing the embarrassing release of this hidden data, the issues raised by document “metadata” have only slowly made their way into litigation matters, court cases and law practices.

That’s all now changed – and drastically – with potentially disastrous consequences for the unprepared. The new rules have brought organizations to a crossroads in the way they deal with the issues raised by metadata in civil litigation. These new amendments update traditional discovery rules for the modern era of electronic documents, and will force organizations and their legal teams to consider the impact of electronic data, including hidden data associated with documents, in every case.

Organizations that attempt to deal with metadata on an ad-hoc basis rather than managing metadata from a document’s creation based on well considered policies now face risks and costs that are simply unjustifiable. Even companies already doing an adequate job of archiving email may experience disastrous complications. For example, many companies use email archiving solutions in which a fundamental requirement of the product is to offload and archive all email data, without regard to attributes or other policy, after a predetermined amount of time has elapsed – typically 90 or 180 days. The technology dictates the business practice rather than the other way around. There are precious few practical tools on the market that will search un-archived email or its metadata, and speed of access to archived email is severely impaired.

Likewise, if there is an immediate legal need to search email but there is not yet an archiving solution in place, the usual approach is to first archive the email and then search. This is a daunting task. Given that email may have taken seven years to accumulate, it is not going to be archived in seven days, let alone seven hours! Here again there is a dire need for technology that searches un-archived email.

Compliance and security technology often forces handcuffs on your business. It’s important to be aware of the impact of these “solutions” on potential litigation and discovery, and consider how data and metadata will be searched pre-archive, post-archive, or even if email should ever be archived at all.

Preserve the Safe Harbor

Of course, some believe that they can just hide or delete emails or other files. Quite apart from the moral aspects of such a decision, such an action would take a litigant out from under the only real “get out of jail free” provision of the new rules. Rule 37f is the so-called Safe Harbor Rule, which states that “absent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the routine, good faith operation.” This rule may offer companies protection should relevant ESI be lost, but only if a “routine, good faith” discovery process is fully defined, fully documented, and fully followed. Hiding or deleting emails would not be consistent with such a process, and demonstrates bad faith. Contempt is punished by fine and imprisonment.

Indeed, proof of non-tampering is essential. This proof is not confined to the data being stored, but security in such areas as mailbox access, system access, and procedures for access control, allowing only authorized custodians to emails and network files. Encryption and intelligent key management, regularly and reliably used, is also an element of proof that the files are genuine and reliable.

Conclusion

It is unlikely that lawmakers, lawyers or business executives anticipated the growth of digital communications and the substantial role such growth would come to play in litigation. That growth has brought unique issues to those involved in litigation.

These issues are moving targets, but can be made more manageable by adopting a framework and a consistent procedure for data management and data security. The initiation, implementation and adherence to business records policies are critical to the success and viability (both financial and market) of many large and midsize corporate entities.

Without a sophisticated ESI management and security program that addresses anticipated legal issues, an organization will have to play “catch-up” when faced with the time sensitive demands of discovery. An unprepared company puts itself at a strategic and financial disadvantage, and will be forced to draw crucial resources away from core business purposes. It’s not worth it. It is best to anticipate a broad range of document requests that will focus on their systems and electronic document storage and security policies.

Get the Help You Need

Under the newly revised Rule 26f mandated discovery conference, counsel must now address electronic discovery issues, and this initial preparation for discovery will be a factor both in cost forecasting and strategic decision making. This early work in defining the case strategy can contribute to long-term cost reduction while simultaneously helping to rebut any claims of inadequate discovery preparation that might be made by opposing counsel.

An expert is often required to sort out key ESI issues, especially the essential issues surrounding of email classification and recovery. Archive One solutions from C2C (www.c2c.com) help organizations with both tactical and strategic archiving solutions for email discovery, retention and also compliance with various regulatory requirements regarding the use and retention of email, such as Sarbanes-Oxley, Freedom of Information Act, HIPAA, Gramm-Leach-Bliley, SEC and NASD Directives, and the Federal Rules of Civil Procedure.

About C2C

C2C offers email archiving and management solutions, which reduce risk, optimizes performance and minimizes compliance issues for over three million users at more than 2,000 organizations world-wide. Based on their in depth understanding of message management, C2C developed its award-winning Archive One suite to help organizations comply with industry regulations and minimizes mailbox size. C2C also offers rapid-response tools for email performance, security and crisis control.

The Company, a Microsoft Gold Certified Partner, supports organizations in the government, manufacturing, finance, education and healthcare industries, including Fortune 1000 companies. Established in 1992, C2C is a privately held company with US offices in Springfield and Westborough, Mass; and Reading, Berkshire in the UK.

About Archive One

Archive One creates a secure, indexed email archive to assist organizations in meeting regulatory requirements. Its menu-driven admin, search and retrieval functions are intuitive for use by the Administrator or Compliance Officer, yet flexible to execute fast, multi-criteria searches.

- **Enforces critical email retention**
Archiving internal and external email to secure, indexed repositories, ensures administrators find critical message content rapidly.
- **Exceeds due diligence expectations**
Maintains full and demonstrable records of every email transaction suitable for all audit requirements.
- **Helps meet compliance demands**
Archive One stores email information for regulatory requirements such as SEC, NASD, NYSE, Sarbanes-Oxley, ISO, HIPAA, BSI, Basel II and others.
- **Manages legal risks**
Retention criteria are enforced automatically, deleting appropriate archived data in accordance with regulations therefore avoiding unnecessary disclosure.
- **Imposes legal Hold**
Archive One retains the items pertaining to legal matters to make sure evidence is not lost.
- **Search within live Exchange stores**
Archive One accesses information on an Exchange system while it is live ensuring all current information is searched.
- **Improves email search and retrieval**
Administrators use intuitive multiple search criteria, making it quick and easy to find lost email or specific correspondence and all related data.
- **Managed Samples with Scheduled Retrieval and Controlled Handover**
Scheduling retrievals enable regular, unsupervised samples to be taken by searching the archive and retrieving items a mailbox, public folder or a portable PST. The handover of these items to subject experts is controlled and their feedback can be logged. This helps organizations to ensure that email system audit processes are in place and helps to check that they are being followed.
- **Is easy to implement, maintain and manage**
All functions are controlled by the administrator and are enacted away from the end user. Email users need not be aware that Archive One has been installed. For administrators the quick wizard-guided install, simple admin controls and standard interfaces minimize the Total Cost of Ownership.
- **Reduces storage volumes**
To save on storage space, archived email can be compressed without losing message integrity.
- **Archives more than just email**
Instant Messages, SMTP mail, Bloomberg Messages and RSS feeds can all be placed into the archive.

Disclaimer of Liability and Trademarks

While every precaution has been taken in the preparation of this document, C2C assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained herein.

All trademarks, trade names, service marks and logos referenced herein belong to their respective companies. Copyright C2C Systems 2008.