



Email as Evidence

12 steps to ensuring good evidential quality of email

Today's litigious and regulatory environments mean that organizations are obligated to store information electronically to support discovery and disclosure requests. Organizations that archive email in a "fractured" environment risk losing control and may struggle to produce evidential-quality email.

Table of Contents

Audience and Remit	2
Executive Summary	4
The Legal Obligation to Give Discovery of ESI	5
Fragmented Email Environments	8
Authenticity in a Fractured Environment	11
Repairing the Fractured Environment– Justifications Beyond Litigation	13
12 Steps to Ensuring Good Evidential Quality of Email	14

AUDIENCE AND REMIT

The intended audience for this white paper includes corporate counsel, IT management, compliance managers and others concerned with the management of email, although legal experience and knowledge is not assumed.

The remit is the writer’s experiences as a litigator and advocate and how those experiences may correspond to comparable situations in the United States.

THE AUTHOR

Stewart Room is a partner at the European law firm Field Fisher Waterhouse LLP, where he specializes in the contentious aspects of privacy, information and technology law. He is dual-qualified as an attorney, with over 16 years' experience as a litigator and advocate.



He is the President of the National Association of Data Protection Officers, author of “Data Protection and Compliance in Context” (2006) and “Email: Law, Practice and Compliance” (2008) and is rated as a leader in the field of data protection and privacy by the legal directory Chambers UK. His clients include BP, BBC, Marks & Spencer, Nestle, RSA, Symantec and Unicef.

Executive Summary

Litigants in the United States are required by law to give discovery of electronically stored information (ESI). The obligations are found in the 2006 modification to the Federal Rules of Civil Procedure (FRCP). The Rules impose rigid timeframes with sanctions for defaulting parties.

The law takes discovery seriously because it is one of the cornerstones of civil justice systems. The law generally prefers a “cards-up” approach to the resolution of disputes, albeit with exceptions. However, while the spirit and intention of the Rules cannot be derided, the fact remains that the process of discovery of ESI can be an onerous obligation, particularly where the litigant and the lawyer are working in a fractured environment and particularly where emails are involved.

The nature of a fractured environment is one in which ESI is not properly managed, resulting in a loss of control. A fractured environment causes ESI to be used and stored erratically; the provenance of ESI might be unclear; rules on retention and deletion might be user-defined rather than organization-defined; and there might be problems of considerable duplication.

A fractured environment is detrimental to ESI. If litigation touches such an environment, the discovery process is inevitably more complex, more time-consuming and more expensive than in cases affecting organizations with properly managed data systems. Moreover, the litigation may be less efficient in the sense that important documents can be overlooked, which can weaken cases and, ultimately, lead to failure when success might otherwise have been more likely and the more just result.

This white paper summarizes the author’s experiences of litigating in fractured environments, particularly as they pertain to email. In light of these experiences, it is the author’s opinion that potential litigants are always best advised to gain control of their email systems and, because email is a technological issue, this requires technological solutions.

THE LEGAL OBLIGATION TO GIVE DISCOVERY OF ESI: SHARED U.S.-UK EXPERIENCES

The primary obligation to give discovery of ESI is contained in Rule 26 of the FRCP and it mirrors closely the corresponding obligation in the United Kingdom, which can be found in Part 31 of the Civil Procedure Rules (CPR). When the FRCP and CPR are compared and contrasted, it will be found that the similarities greatly outweigh the differences. This should not be surprising, bearing in mind the shared ancestry of these legal regimes, the common law and adversarial approaches of each jurisdiction, the shared language, the very close social, political, economic relationships and ties, and the increasingly international flavor of litigation. Consequently, a litigator's experiences on the author's side of the Atlantic should be of practical help in the United States. Likewise, a litigator's experience in the United States will be of practical help in the UK.

Indeed, the close connections and cross-pollination of ideas on ESI between the U.S. and the UK is evidenced by the fact that work on ESI by the Sedona Conference¹ provided the seed to the amendment of the CPR's rules on eDiscovery in 2005.



¹ The Sedona Conference is a U.S. think tank whose mission is to advance the development of the law. Its "Sedona Principles" categorize types of ESI for litigation purposes. In 2005, the Commercial Court for England and Wales endorsed the Sedona Principles and incorporated their essence within amendments of the CPR so as to clarify the scope and ambit of eDiscovery.

125 CASE STUDY

In 2006, Morgan Stanley agreed to pay a \$15 million fine to the Securities and Exchange Commission for repeatedly failing to produce emails during the course of investigations concerning share allocations in IPOs. The SEC's complaint said:

"From December 11, 2000, through at least July 2005, Morgan Stanley failed to produce tens of thousands of emails sought by Commission subpoenas and other requests issued in the course of two Commission investigations: an investigation into Morgan Stanley's practices in allocating shares of stock in initial public offerings ('the IPO Investigation') and an investigation into conflicts of interest between the firm's research and investment banking practices ('the Research Analyst Investigation'). As a result, Morgan Stanley violated the provisions of the federal securities laws requiring Morgan Stanley, a regulated broker-dealer, to timely produce its records and documents to the Commission."

The Morgan Stanley case provides a salutary warning to organizations about the need to take emails seriously for the purposes of recordkeeping and for the purposes of regulatory investigations. Among other things, the Morgan Stanley experience teaches organizations the following priorities for email:

- During the course of regulatory investigations, they should ensure diligent searching of archives.
- Any statements to regulators about the availability of email should be wholly accurate.
- Emails should be delivered in a timely fashion.
- The introduction and implementation of an email archive is a high priority.
- Emails should be properly preserved to avoid deliberate or accidental overwriting and deletion.

eDiscovery Under the FRCP

If the FRCP and CPR are stripped down to their fundamentals, the same core obligation is discovered; litigants are entitled to give disclosure of ESI that assists their cases, and they can be compelled to give disclosure of ESI that undermines their cases or which assists their opponents' cases. This right/obligation approach is the hallmark of an adversarial legal system. Of course, in order to be effective on a day-to-day basis, the right/obligation approach within the FRCP is supported by considerable detail.

In summary, the core components for discovery of ESI are:

- The scope of the obligation to give discovery is non-privileged material relevant to claims and defenses and extends to disclosing “the existence, description, nature, custody, condition, and location of any documents or other tangible things and the identity and location of persons who know of any discoverable matter.”
- The obligation to make initial disclosures arises after the parties have conducted their pre-scheduling conference (the pre-scheduling conference is known as a Rule 26(f) conference); discovery must be given within 14 days of the Rule 26(f) conference, unless an exemption applies.
- The initial disclosures extend to providing the other side with information about individuals holding “discoverable information” and copies of documents, ESI and tangible things, if the disclosing party will rely upon these in its claim or defense, plus documents and evidence that support the computation of damages. Discovery must be given of information “reasonably available.”
- The obligation to make initial disclosures arises without the need for a request from the other side.
- Parties must also give pretrial disclosures at least 30 days before the trial, which extends to the identification of witnesses and documents and exhibits.
- The court can compel discovery.

The obligation to give discovery of ESI is subject to important caveats, in the sense that it is subject to a reasonableness component. The Rules say:

“A party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost. On motion to compel discovery, or for a protective order, the party from whom discovery is sought must show that the information is not reasonably accessible because of undue burden or cost.”

Although these caveats can provide an organization with a fractured environment some comfort, there is a sting in the tail. The burden is on the party disputing the reasonableness of eDiscovery to prove this is so.

FRAGMENTED EMAIL ENVIRONMENTS

Email forms one of a company’s greatest assets – it is both a critical communications tool and a repository of historical business intelligence. Today it provides supporting evidence during disputes with external parties and internal employees.

For a whole host of reasons, ancillary services have been built around email servers to provide risk mitigation from threats such as spam, malware and data loss. In addition, other requirements for effective enforcement of email Acceptable User Policy and legislative compliance have arisen. Over the past decade vendors have reacted by providing dozens of technologies to solve the issues around email, such as email firewalls, email routing, denial of service protection, intrusion prevention systems, anti-spam, anti-virus, anti-phishing, attachment management, disclaimer management, email marketing, email storage management, high availability, archiving and managing discovery.

Almost all of the ancillary services deployed in an email infrastructure are designed to provide functionality in three broad areas: to increase internal governance; to mitigate risk; and to improve legislative compliance.

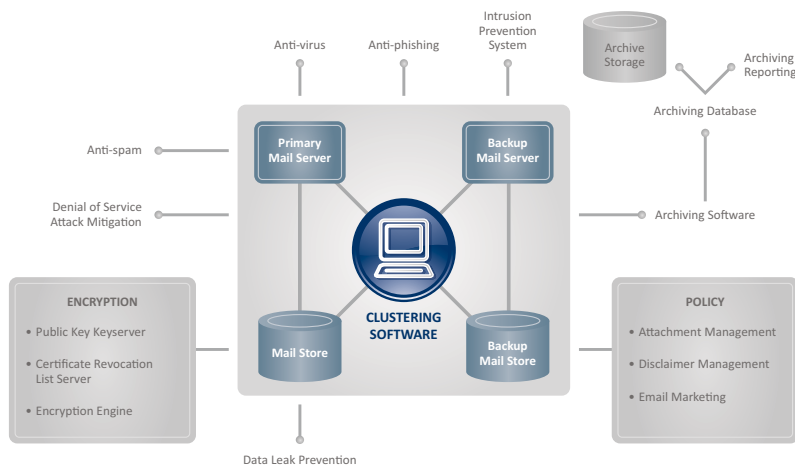
These solutions are typically deployed as they become necessary to adapt to new threats or regulatory requirements and build up organically over time around the mail server.

Each of these support services is typically provided by a separate point solution, each requiring maintenance, and comes with its own provisioning and reporting interface.

Each of these solutions will typically operate in isolation, independent of the actions that the other components are taking. Because each platform will log its actions into its own reporting environment, seeing the sum total of actions taken on a particular email may involve extensive aggregation and normalization of the logs from dozens of different servers. With a fragmented reporting infrastructure, it is difficult to detect changing trends in email usage, to identify anomalies, or even to get a high-level snapshot of whether the level of risk involved with email is increasing or decreasing.

This fragmented environment results in islands of protection against specific threats but makes it very difficult to apply and enforce organization-wide policy. The fragmented environment also inhibits eDiscovery – each email may have several different variants in existence within the receiving organizations due to multiple independent point solutions applying parts of the overall policy. Often the email recorded in an archive will be just one variant which may differ from the original email received.

TRADITIONAL FRAGMENTED EMAIL ENVIRONMENT ARCHIVE



Meeting the Timetables for eDiscovery in a Fractured Environment

Perhaps the greatest problem for attorneys and organizations working in a fractured environment is how to comply with legal timetables. It should not be underestimated that if ESI is improperly managed it can be extremely difficult, if not impossible, to comply.

When a litigant requires the court's indulgence, it usually creates a bad impression and can cause the other side to scent blood. Being on the back foot in litigation should always be avoided.

Good litigators always seek to be in control, because it is from a platform of control that cases are won.

As far as emails are concerned, the problems associated with a fractured environment increase by a large order of magnitude. Part of the essence of email is its ability to reproduce, replicate and spread. Should litigants find themselves in a position of having to chase after and track down emails, they will be deflected from much more profitable endeavors within the litigation, such as putting pressure on the other side!

CASE STUDY

In 2005, UBS Securities was fined \$2.1 million by the Securities and Exchange Commission for failing to preserve emails for a three-year period between 1999 and 2002, which the SEC required access to for purposes of its investigation into UBS's researching and investment banking activities. The complaint filed by the SEC said:

"During all or part of the relevant period, UBS failed to preserve for three years, the first two of which in an easily accessible place, all electronic mail communications (including interoffice memoranda and communications) received and sent by its employees that related to its business as a member of an exchange, broker or dealer. UBS lacked adequate systems or procedures to ensure the preservation of electronic mail communications. The Commission, NYSE, and NASD (collectively, 'the regulators') discovered these deficiencies during inquiries into the supervision of UBS's research and investment banking activities."

The UBS case teaches organizations the following priorities for email:

- Archives containing email should be identified and preserved in a manner that they can be located and delivered quickly during regulatory investigations.
- Archives should provide protection against corruption of email data.
- Internal policies for the handling of archives should be adhered to and properly managed.
- Where the handling of email is subcontracted or outsourced to a third party, the organization must be able to exercise control over the third party in order to guarantee successful eDiscovery.

Assessing the Relevance of ESI in a Fractured Environment

One of the most critical parts of the discovery process is assessing the relevancy of materials. This task is rendered much more difficult in a fractured environment because the assessment of relevancy is just as much about context as content. If ESI is poorly managed, the risk of misunderstanding the proper context is significant, which can lead to a substantial risk of failure of discovery. Relevant materials might be improperly withheld, and privileged materials might be improperly disclosed.

Again, the problems are magnified where email is concerned, and there are many reasons for this. For example, senders of emails might use the blind copy field. Where this context is overlooked, the organization could also overlook the existence of potential witnesses. Like a domino effect, this leads to a cascade of breaches of the FRCP. Similarly, senders and recipients of email might print hard copies, a fact which might not be appreciated; again, the litigant is put at risk of breach of the rules. Furthermore, the body text of email can be easily manipulated after the fact, which might not be apparent in the fractured environment. Finally, emails are connected to computers, not people; in a fractured environment it might not be appreciated that the sender of an email, or indeed the recipient, was the person to whom the email account was assigned.

Arguing Reasonableness in a Fractured Environment

The FRCP contains the caveat for reasonableness for obvious reasons. Unlike paper documents, electronic ones can soon multiply out of control; they can be subject to many different storage environments and locations; and they can be under the control of a much larger number of persons. Consequently, eDiscovery can often be an onerous, time-consuming and expensive task, quite out of kilter with the importance of the case and the issues. Thus, the rules contain the caveat set out above.

In a fractured environment, eDiscovery becomes an even more onerous, time-consuming and expensive task, but it is a fundamental principle of most systems of civil justice that litigants should not be rewarded for their own failures or want of diligence. For this reason, the rules place the burden of proof on the party trying to resist discovery.

When addressing the reasonableness of discovery, the inevitable problem for the poorly managed company is not the obligation to give discovery, but rather their poor systems creating an obstacle to doing so. However, the well-organized opponent will be bound to advance an argument to the court to that effect. It is the writer's experience that this argument very often meets with success; after all, why should a poorly managed organization be in a better position to avoid discovery than the well-managed one?

eDiscovery can often be an onerous, time-consuming and expensive task, quite out of kilter with the importance of the case and the issues.

AUTHENTICITY IN A FRACTURED ENVIRONMENT

As indicated earlier, ESI, particularly emails, is much more vulnerable to amendment, alteration, loss and destruction in a poorly managed environment than in a properly managed one. Indeed, it is the writer's experience that the "ephemeral" nature of email often attracts arguments about authenticity.

There is no doubt that ESI is admissible in evidence; that is why it is subject to the discovery process. However, admissibility is only one component of proof. Evidence needs to be of sufficient probative value, or "evidential weight," to discharge the burden of proof. If the evidence is not of sufficient probative value, the court will discount it or accord it less weight.

Astute litigants will regularly consider the extent to which the probative value of ESI can be challenged. If the ESI results from a fractured environment, the prospects of a successful challenge are significantly increased. If the provenance of an email cannot be proved to the satisfaction of the court because it has not been kept in a safe and tamper-proof environment, the outcome of the case might be affected. Thus, attacking the authenticity of email is often a highly productive tactic.



CASE STUDY

In a recent case, the writer was defending a group of businessmen who were accused of stealing a company database. The evidence against them was compelling; there were emails passing between some of them which referred to the possibility of their setting up in direct competition with their employer. Due to poor quarterly sales and failed business development projects, some of them had motive to set up in competition. Importantly, they had opportunity, and they had legitimate rights of access to the company database. Finally, there was evidence that the database had been downloaded from a PC that was used by one of the group. Not surprisingly, the company thought that it had a “killer” case.

However, the company was forced to withdraw. Although the “visible” evidence seemed to point only one way, there was a huge amount of “invisible” evidence that fatally undermined the company’s case. This invisible evidence was found in the fact that the company had a fractured environment for data processing and ESI. Whereas computers were password protected, passwords were weak, often shared, and never changed. Although hard copies of emails were available, the electronic versions had been irrevocably deleted and there were no archive copies. Even though the group had motive, so did other company personnel. Where the emails seemed to have passed among the group, they had actually passed between computers.

The failure of the case was 100% attributable to the fractured environment. If the use of email had been properly managed – with proper access control mechanisms and a proper email archive – the company would have won the case. Yet they managed to snatch defeat from the jaws of victory.

REPAIRING THE FRACTURED ENVIRONMENT – JUSTIFICATIONS BEYOND LITIGATION

Although the eDiscovery rules in the FRCP justify new approaches to the handling of ESI and email, many organizations will delay acting because they might have been successful in avoiding litigation. Why “fix” something for an eventuality that has so far not materialized? It is understandable to think that way, but such thinking might be a mistake. No organization is immune from litigation – litigation can strike at any time, and when it strikes at an organization with a fractured environment, the results can be devastating. The company referred to in the case study lost not only the litigation, but also much business, because once the word got around their industry that they were not managing their information assets properly, many clients decided the risk of continuing to work with them was too great and they took their business elsewhere.

However, there is more than just the fear of litigation to justify investment in tools and technologies for the proper handling of email. eDiscovery obligations also exist in many regulatory frameworks for business: under Sarbanes-Oxley (SOX), the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), and the Federal Trade Commission Act (FTC), for example.

Discovery is a primary tool of regulatory bodies, along with licensing regimes and fines. Regulations contain discovery obligations in order to ensure a level playing field between the organization, the regulator, and the person whom the regulator is trying to protect, usually a consumer. In regulatory terms, discovery and transparency go hand in hand and, indeed, transparency components are being built into regulations with ever-increasing enthusiasm.

A very good example of this approach is contained in the raft of state laws that have introduced breach-notification obligations for organizations suffering security breaches and loss of Personally Identifiable Information (PII); these laws are all about transparency.



THE REGULATIONS:

- HIPAA
- Data Protection Act
- Financial Services Act
- MiFID
- Sarbanes-Oxley
- The Companies Act Combined Code
- EuroSOX
- GLBA

12 Steps to Ensuring Good Evidential Quality of Email

As a litigation attorney who specializes in email law, I would suggest taking the following steps to maximize the evidential quality of your email. An organization that adopts these 12 steps will be well-equipped to cope with an eDiscovery exercise, whether for the purposes of litigation or for the purposes of a regulatory investigation. These steps will provide the best environment for meeting the tight timetables within the FRCP; they will enable the organization to properly assess the relevance of materials; they will provide very strong ammunition for arguments about the reasonableness of discovery; and they will provide the organization with an almost cast-iron position on the question of authenticity.

And, of course, most important of all, they will equip the organization and the attorney with the position they need to take control of litigation, which will always increase the prospects of success.

- 1 Ensure that the use of email is subject to agreed-upon procedures, which are supported and enforced by high-level management. Acceptable use policies must prescribe good usage and identify bad usage.
- 2 Train users of email in acceptable use and of their rights and the obligations expected of them.
- 3 Implement access control mechanisms to computer systems so that use can be attributed to a person, a terminal, a date and a time.
- 4 Ensure that computer systems are kept safe and secure so that the systems and the data within are protected from unauthorized access and accidental or deliberate loss and damage.
- 5 Retention and deletion of email should be organization-defined, not user-defined. Individual users should not have any discretion as to the categories of emails that should be retained or deleted.
- 6 Implement a solution that archives and stores emails centrally. The archive should support all of the main file formats and also retain metadata.
- 7 The archive should classify emails entering the archive at the point of entry. The archive should prevent the entry of duplicates.
- 8 Ensure that the archiving platform facilitates the exporting of evidence as files as part of the eDiscovery process.
- 9 Implement an archiving solution that allows full search and retrieval. Both metadata and content should be searchable.
- 10 Enable logging of all events acting on the archive. The logs should be retained as part of the archive for auditing and verification purposes.
- 11 Provide contingency for continuity of both archiving and discovery in the event of an outage.
- 12 Ensure the archiving platform supports the marking up of files so that privileged materials can be withheld and/or redacted during eDiscovery.

ABOUT MIMICAST

Mimecast delivers SaaS-based enterprise email management for archiving, discovery, continuity, security and policy. By unifying disparate and fragmented email environments into one holistic solution that is always available from the cloud, Mimecast minimizes risk and reduces cost and complexity, while providing total end-to-end control of email. Founded in the United Kingdom in 2003, Mimecast serves 2,500 customers worldwide and has offices in Europe, North America, Africa, the Middle East and the Channel Islands.

ABOUT IRON MOUNTAIN

Iron Mountain Incorporated (NYSE:IRM) helps organizations around the world reduce the costs and risks associated with information protection and storage. The Company offers comprehensive records management and data protection solutions, along with the expertise and experience to address complex information challenges such as rising storage costs, litigation, regulatory compliance and disaster recovery. Founded in 1951, Iron Mountain is a trusted partner to more than 90,000 corporate clients throughout North America, Europe, Latin America, and Asia Pacific.

For more information, visit the Company's Web site at www.ironmountain.com.

Portions © 2009 Iron Mountain Incorporated. All rights reserved. Iron Mountain, the design of the mountain and Iron Mountain Digital are registered trademarks of Iron Mountain Incorporated. The reproduction of this white paper is limited to distribution by Iron Mountain Digital only.

Additional copyright and other rights worldwide in this white paper are the property of Mimecast Limited and those may only be reproduced with Mimecast Ltd.'s permission. Mimecast is a registered trademark of Mimecast Limited. All other trademarks and registered trademarks are the property of their respective owners.



IRON MOUNTAIN®
120 Turnpike Road
Southborough, Massachusetts 01772
(800) 899-4766

Iron Mountain Digital is the world's leading provider of Storage-as-a-Service solutions for data protection and recovery, archiving, eDiscovery and intellectual property management. The technology arm of Iron Mountain Incorporated offers a comprehensive suite of solutions to thousands of companies around the world, directly and through a worldwide network of channel partners. Iron Mountain Digital is based in Southborough, MA.