

The Impact of the New FRCP Amendments on Your Business

An Osterman Research White Paper

Published January 2007

SPONSORED BY

FaceTime®

<http://www.facetime.com>



Executive Summary

Here's a guide to choosing an eDiscovery compliance solution for the enterprise:

- *Are messages captured from both endpoints and servers?*
- *Are messages protected against tampering?*
- *What coverage exists for IM networks beyond AOL, MSN and Yahoo!?*
- *Are entire conversations/chat threads recorded, including files transferred, as well as sender and recipient names and time and date tracking?*
- *Can messages be easily searched by individual user, time period, case number and other criteria and the relevant records extracted?*
- *Does the solution interface with existing IT infrastructure for minimal disruption and maximum flexibility?*

The newly adopted amendments to the Federal Rules of Civil Procedure (FRCP) will have a major impact on the way that organizations manage electronic data. These new eDiscovery rules have broadened the definition of electronically-stored information (ESI) to include chat and file transfers from applications such as:

- Public instant messaging networks such as MSN, Yahoo, GoogleTalk and AOL
- Enterprise instant messaging networks such as Jabber, as well as the communications aspects of infrastructure products like Microsoft Live Communications Server (LCS) and IBM Lotus Sametime
- Professional community networks such as Bloomberg and Reuters
- Peer-to-peer networks including Skype
- Web conferencing chat threads such as those produced by Webex

An Osterman Research survey conducted in December 2006 revealed that more than one-half of organizations do not understand the new rules well enough to understand the impact that they will have on their data retention practices, while only one in five organizations does not anticipate any sort of change in their corporate behavior in response to the changes. Further, another survey found that only seven percent of corporate counsel attorneys rated their companies as prepared for the new amendments, while more than one-half were not even aware that the new amendments were to go into effect on December 1, 2006¹

Truly, the consequences of non-compliance is severe. In May 2006, Morgan Stanley was forced to pay \$15M to settle a civil lawsuit with the SEC, over failure to produce tens of thousands of electronic messages.

Thus the new eDiscovery rules have required that companies involved in litigation must:

- Be prepared to discuss how and where their ESI is stored, early in the pre-trial proceedings.

¹ Survey conducted by LexisNexis Applied Discovery during the Association of Corporate Counsel 2006 Annual Meeting in October 2006.

- Preserve their ESI in a compliant manner and produce it with specified metadata intact.
- Produce their ESI data in a timely and complete manner according to the time line of the proceedings.
- Organizations must explore beyond any existing email compliance solutions they possibly have, and adopt an instant messaging solution that stores, archives, and retrieves promptly and efficiently all communications traffic, from the standpoint of a non-doctorable platform.

The next several months will present significant challenges to organizations of all sizes on several levels: corporate legal counsel will need to learn what impact the FRCP changes will have on their organizations, IT managers will wrestle with the potentially significant investments in technology that will be required to adequately preserve electronic data, and senior managers will need to evaluate and improve their corporate governance policies and procedures to meet the new requirements.

This document was authored by:

- **John A. Heer**
An attorney that focuses on e-discovery in complex civil litigation and environmental matters. Mr. Heer is a respected speaker and author on topics such as electronic discovery and evidence, litigation tactics and environmental law.
- **Michael D. Osterman**
Founder and principal of Osterman Research, Inc.

What are the Federal Rules of Civil Procedure?

The FRCP are a body of rules focused on governing court procedures for managing civil suits in the United States district courts. While the United States Supreme Court is responsible for promulgating the FRCP, the United States Congress must approve these rules and any changes made to them.

A number of important and substantive revisions to the FRCP went into effect on December 1, 2006. These changes represented several years of debate at various levels.

A number of important and substantive revisions to the FRCP went into effect on December 1, 2006. These changes represented several years of debate at various levels and will have a significant impact on electronic discovery and the management of electronic data within organizations that operate in the United States. In a nutshell, the changes to the FRCP require organizations to manage their data in such a way that this data can be produced in a timely and complete manner when necessary, such as during legal discovery proceedings.

New Amendments to the FRCP

The amendments to Rules 16, 26, 33, 34, 37, 45 and revisions to Form 35 are aimed at electronically stored information (ESI). The amendments attempt to deal with the important issues presented by ESI:

- ESI is normally stored in much greater volume than are hard copy documents.
- ESI is dynamic, in many cases modified simply by turning a computer on and off.
- ESI can be incomprehensible when separated from the systems that created it.
- ESI contains non-apparent information, or metadata, that describes the context of the information and provides other useful and important information.

The changes reflect the reality that discovery of email and other ESI is now a routine, yet critical, aspect of every litigated case.

The changes reflect the reality that discovery of email and other ESI is now a routine, yet critical, aspect of every litigated case. First, the amendments treat ESI differently. Second, they require early discussion of and attention to electronic discovery. Third, they address inadvertent production of privileged or protected materials. Fourth, they encourage a two-tiered approach to discovery – deal with reasonably accessible information and then later with inaccessible data. Finally, they provide a safe harbor from sanctions by imposing a good faith requirement.

Who is Most Impacted by the Changes to the FRCP?

Unlike many data retention requirements in specific industries, such as those imposed upon broker-dealers by the Securities and Exchange Commission (SEC) and the National Association of Securities Dealers (NASD), the FRCP apply to virtually all organizations in all industries. If an organization can have a civil lawsuit filed against it, then the FRCP should figure prominently in that organization's data management strategy.

Obviously, all cases brought after December 1, 2006 will be subject to the new FRCP amendments. However, the Supreme Court has determined that cases filed prior to this date could be subject to the FRCP if a court determines that undue delay or burden to the parties involved² will not be imposed by adherence to the new rules.

The Supreme Court has determined that cases filed prior to this date could be subject to the FRCP if a court determines that undue delay or burden to the parties involved will not be imposed by adherence to the new rules.

Key Rules Within the FRCP

Civil Rule 16

Pretrial Conferences; Scheduling; Management

The amendments establish a process for the parties and court to address early issues pertaining to the disclosure and discovery of electronic information. They are designed to alert the court and litigants to the possible need to address handling of ESI early in litigation if such discovery is expected to occur. Rule 16(b) is amended to invite the court to address disclosure or discovery of ESI in the Rule 16 scheduling order and gives the court discretion to enter an order adopting any agreements the parties reach for asserting claims of privilege or protection after inadvertent production in discovery.

Civil Rule 26

General Provisions Governing Discovery; Duty of Disclosure

- **Rule 26(a)(1)**
The amendment clarifies a party's duty to include ESI in its initial disclosures by substituting the word "ESI" for "data compilations."
- **Rule 26(b)(2)**
The amendment clarifies the obligations of a responding party to provide discovery of ESI that is not reasonably accessible (deleted information, information kept on

² <http://www.supremecourtus.gov/orders/courtorders/frcv06p.pdf>

Any organization should first obtain and examine the information that can be provided from easily accessed sources and then determine whether it is necessary to search difficult-to-access sources. A party might be obligated to preserve information stored on sources it has identified as not reasonably accessible.

some backup tape systems, and legacy data from systems no longer in use). The amendment requires the responding party to identify the sources of potentially responsive information that it has not searched or produced because of the costs and burdens of accessing the information. If the requesting party moves for production of such information, the responding party has the burden of showing the information is not reasonably accessible. If the responding party makes this showing, a court may order discovery for good cause and may impose conditions. Any organization should first obtain and examine the information that can be provided from easily accessed sources and then determine whether it is necessary to search difficult-to-access sources (a court can order a sampling technique to determine the usefulness of searching the difficult-to-access sources). A party might be obligated to preserve information stored on sources it has identified as not reasonably accessible.

- **Rule 26(b)(5)**
The amendment provides a procedure for asserting privilege after production that is parallel to similar changes in Rules 16 and 26(f). Upon notification to the recipient of the producing party's post-production privilege claim, the recipient must return, sequester or destroy the information until the claim is resolved.
- **Rule 26(f)**
The amendment requires the parties' conference to include discussion of any issues relating to disclosure or discovery of ESI, including form of production, preservation, and privilege/protection issues. The amendments encourage parties to enter into voluntary agreements under which the inadvertent production of privileged or protected materials would not result in a waiver. Any such agreement should probably include an "attorney's eyes only" provision, no waiver of trade secret protection, penalties for distribution of the material, including by e-discovery providers, and provision for certified and validated destruction of privileged data or data not used.

Civil Rule 33 ***Interrogatories to Parties***

The amendment expressly provides that an answer to an interrogatory involving review of business records should involve a search of ESI.

Civil Rule 34

Production of Documents and Things and Entry Upon Land for Inspection and Other Purposes

ESI is explicitly recognized as a category that is distinct from "documents" and "things." Rule 34 also authorizes the requesting party to specify the form of production. Absent court order, party agreement or a request for a specific form of production, a party may produce responsive ESI in the form ordinarily maintained or in a reasonably usable form.

Rule 34 also includes the notion of sampling data from an entire data set to determine if additional discovery is warranted. A key provision of Rule 34 is the production of data in "a form or forms in which it is ordinarily maintained or in a form or forms that are reasonably usable."

The amendment creates a "safe harbor" that protects a party from sanctions for failing to provide electronically stored information lost because of the routine, good-faith operation of the party's computer system. The problem with this rule, however, is that it is subject to a wide variety of interpretations.

Civil Rule 37

Failure to Make Disclosure or Cooperate in Discovery; Sanctions

The amendment creates a "safe harbor" that protects a party from sanctions for failing to provide electronically stored information lost because of the routine, good-faith operation of the party's computer system. Rule 37(f) provides limited protection against sanctions for a party's failure to provide ESI in discovery if the ESI sought in discovery is lost as a result of routine operation of an electronic storage system, as long as the operation is in good faith. Good faith likely requires that a party intervene to modify or suspend certain features of the routine operation of computer systems to prevent loss of information if the information is subject to a preservation obligation (i.e., the party must initiate a "litigation hold").

The problem with this rule, however, is that it is subject to a wide variety of interpretations. For example, if a defendant considers a failure to produce ESI in a particular case the result of a "good faith" operation of an electronic information system, such as erasing backup tapes on a routine basis, a court may not agree and may find the defendant liable for spoliation of data.

Civil Rule 45

Subpoena

These are technical amendments that conform to other proposed amendments regarding discovery of electronically stored information by adding ESI to the scope of information that a person receiving the subpoena must search.

Subpoena may specify the form in which ESI is to be produced.

Form 35

Report of Parties' Planning Meeting

This is a technical revision reflecting the amendment to Civil Rule 26, amended to add the parties' proposals regarding disclosure or discovery of ESI to the list of topics to be included in the report to the court.

Most backups are retained typically for no more than 60 to 90 days as subsequent backups on tape or disk are recycled or overwritten. While backups can be preserved indefinitely in order to preserve business records, there are three fundamental problems with using backups as an archive.

Important Considerations Moving Forward

Almost all organizations perform regular backups of their email system, file servers and other data repositories. While many organizations believe that these backups constitute an "archive" of their business information, this is not the case. A traditional backup takes periodic "snapshots" of active data so that deleted or destroyed records can be recovered, such as after the failure of a server's hard disk or an application upgrade gone awry. Most backups are retained typically for no more than 60 to 90 days as subsequent backups on tape or disk are recycled or overwritten. While backups can be preserved indefinitely in order to preserve business records, there are three fundamental problems with using backups as an archive:

- Backups constitute "raw" content and lack any sort of indexing. If information, such as in response to a discovery order, must be produced from a set of backup tapes, the process is typically time-consuming, highly disruptive to IT staff and expensive, particularly if third-party forensics firms must be used.
- The integrity of backup tapes is not guaranteed. There have been many cases in which older tapes were not readable due to data corruption or physical corruption of the media itself.
- Because backups capture a snapshot of data, information generated and deleted between backups will not be captured. For example, if an organization is required to preserve communications between senior management and external auditors, an email sent from the CEO to the external firm at 10:00am and then deleted from the "Sent" folder at 2:00pm on the same day will never be captured in the nightly backup.

While backups are a critical and necessary component of an organization's data management strategy, they are not a substitute for an archive. In short, a backup is designed to preserve data for short periods in support of the physical infrastructure that an organization maintains, while an archive is designed to preserve information on a long term basis in support of more strategic corporate objectives.

The Benefits of Archiving

As noted above, an archive that is populated based on a pre-determined set of corporate policies offers important benefits:

A properly configured and managed archiving system makes production of data in response to an e-discovery order far simpler than if backup tapes must be searched for the same information.

- **Ease of capture**
Information can be captured from a variety of data sources, indexed and placed into an archive without any intervention by IT staff or end users. Further, if a discovery hold order is imposed for a particular set of users, for example, a new policy can be created instead that will address this order automatically, minimizing the potential for spoliation of evidence.
- **Ease of production**
A properly configured and managed archiving system makes production of data in response to an e-discovery order far simpler than if backup tapes must be searched for the same information. For example, in the case of *Bank of America Corporation vs. SR International Business Insurance Company* [2006 WL 3093174 (N.C. Super. Nov. 1, 2006)], the defendants requested that a non-party to the case, Marsh, Inc., produce deleted emails from 400 backup tapes. Kroll Ontrack estimated that the cost to produce these emails could have been up to \$1.4 million, or an average of \$3,500 per tape. While Marsh was not required to produce the deleted emails in this case, the example illustrates the potentially enormous cost of retrieving discoverable content from backups.

Other Benefits of Archiving

While archiving offers very clear benefits to organizations that must address their data governance practices in the context of FRCP compliance, archiving also provides a number of other benefits:

- **Regulatory compliance**
As noted above, there are a wide variety of regulations that impose data retention and management requirements on organizations operating in the United

States. These requirements, which literally number in the thousands, are quite diverse, ranging from the Americans with Disabilities Act to the Toxic Substances Control Act. While most of these regulations' data retention provisions do not specifically call out ESI, email, instant messages or other specific forms of data, the growing quantity of ESI dictates that business records and other information should be preserved in their native format as a best practice. In the case of instant message, this should include attachments sent as file transfers thru IM networks. The ability to archive both instant message text and the content of IM-borne attachments is important for e-discovery purposes.

This increased use of email, coupled with growing use of attachments, larger attachments and multimedia files means that email storage is becoming a critical issue. Osterman Research has found that the growth in email storage is the leading problem for email managers and constitutes more of a problem than spam.

- **Storage management and storage optimization**

Email use is growing dramatically – Osterman Research has found that email use by employees is growing at about 20% annually. This increased use of email, coupled with growing use of attachments, larger attachments and multimedia files means that email storage is becoming a critical issue. Osterman Research has found that the growth in email storage is the leading problem for email managers and constitutes more of a problem than spam.

Archives consist of largely static data – if that data is included as part of regular backup and restore, then organizations are constantly backing up the same static data over and over, which represents a significant cost. This approach necessitates continually buying larger servers and more storage over time.

An appropriately configured archiving system can automatically offload data from email servers, resulting in better email server performance and shorter restoration periods after a server crash. Further, IT can continue to impose mailbox-size quotas on their users (which about 60% of organizations do today). However, because data is automatically transferred from users' mailboxes to an archive in many archiving systems, users experience what seems to be a mailbox of infinite size, eliminating the need to manually move data from the inbox to other repositories in order to stay within the quota limitation.

It is also important to consider instant messaging in the context of storage management, since use of instant messaging systems will increase rapidly, growing from

one-third of all email users at present to near ubiquity by 2009.

- **Knowledge management and data mining**

Three out of four email users in the workplace in a December 2006 Osterman Research survey reported that email is “extremely important” in helping them to do their work. This is due primarily to the fact that most of the information that employees produce is somehow tied up in email in the form of documents, contacts, email threads and other content. An archiving system allows an organization to preserve this information for long periods so that employees have access to it when necessary.

- **Other benefits**

An archiving system can also assist an organization with recovering from a disaster by providing an off-site copy of current data, it can help in resolving disputes prior to legal action by preserving all necessary ESI and the context of this data, and it can help an organization to assess the viability of its legal position at the commencement of a legal action, among other benefits.

Most of the information that employees produce is somehow tied up in email in the form of documents, contacts, email threads and other content. An archiving system allows an organization to preserve this information for long periods so that employees have access to it when necessary.

Understanding Media Choices

Another key consideration for satisfying FRCP, compliance, and other data retention issues for on-premise data management is the choice of hardware, software, and media on which to archive data on a long term basis. Considerations should include random access to data, long term media longevity, data permanence and authenticity, recoverability and cost.

RAID, tape, WORM optical, DVD and other technologies can all be used for long-term archival storage, but there are trade-offs to consider. For example, specially designed archival storage products using RAID magnetic disk offer excellent performance and high capacity. There are several disk-based archiving products available in the market today that provide functionality for the long-term preservation of business records with content-aware or content-addressed storage approaches. Special consideration should be given to how data is protected long term with these systems, since backup or disk-mirroring technologies may not be sufficient to protect ESI over its useful life. It is also important to note that these use rewritable media with software-enabled WORM. Plus, not all

of these solutions can be taken off-line for secure vaulting and the TCO of a RAID archive system is higher than for some other technologies.

By contrast, tape is removable – important for disaster recovery – has extremely high capacity and offers fast read/write streaming at an affordable price. However, tape struggles as an archive medium because it lacks random access performance for discovery. Like RAID, it is also rewritable and requires special environmental conditions and periodic refreshing if used for long-term data storage.

High-density optical media is a cost-effective approach that combines low cost per bit, media-based WORM capabilities, random access and very long media life. Optical also eliminates the need to migrate data over the useful life of the ESI via backward compatible support and a non-invasive roadmap to future generations.

Today's best practices often combine technologies such as RAID disk, optical technologies, and tape to capitalize on the strength of each and mitigate the risk of failure.

A key question that also must be addressed as part of any data governance strategy is just how much should be saved and what can safely be discarded.

Understanding Delivery Models

Another important consideration is the delivery model for managing data in support of FRCP and other requirements. While most organizations currently opt for on-premise solutions, using appliances or software installed on in-house servers, another viable option is to use a managed service that will provide archiving capabilities without any investments in hardware or software.

The advantages of an on-premise approach are complete control over the infrastructure used to deploy the data management solution, the ability to re-use existing hardware and lower costs than hosting in some cases. The advantages of using managed services include rapid deployment (particularly useful when hit with a discovery hold order), minimizing IT involvement in the data management process and lower costs than on-premise solution in some environments.

How Much Content Should You Save?

A key question that also must be addressed as part of any data governance strategy is just how much should be saved and what can safely be discarded.

One approach is to save as little as possible, preserving data only as long as necessary to ensure that servers can be restored after a failure. This approach is the least expensive from an infrastructure perspective, since it minimizes storage costs, eliminates the cost of an archiving capability and minimizes IT's involvement in managing information. Plus, because it minimizes the storage of live data, servers can perform well and be recovered more quickly after a server crash. However, this can be an expensive approach in the long run, since it runs the risk of deleting information that must be preserved because of FRCP requirements, regulatory obligations and the like. Also, because most users will keep information for long periods anyway, enforcement and litigation costs are higher, there is greater risk of running afoul of discovery hold orders and users will often oppose strict deletion requirements.

At the other extreme is a policy of saving virtually everything – some organizations will even save spam for the sake of completeness. The primary advantage of this approach is that organizations run the least risk of deleting data accidentally, allowing them to satisfy regulatory requirements and discovery orders. The disadvantages of this approach are much higher storage costs, greater difficulty in finding necessary data because of all the unnecessary data that is also saved and saving “smoking guns” that a regulator or court would not have required an organization to save.

The best approach to data retention is to implement a balanced strategy that leans toward saving more rather than less. This approach includes establishing specific policies around data governance that work best for an organization based on FRCP guidelines, regulatory obligations and advice from legal counsel; implementing backup, archiving and other technologies that will help to satisfy these policies; and using the right combination of nearline and secondary storage most effectively.

The best approach to data retention is to implement a balanced strategy that leans toward saving more rather than less. This approach includes establishing specific policies around data governance, regulatory obligations and advice from legal counsel; implementing technologies that will help to satisfy these policies; and using the right combination of nearline and secondary storage most effectively.

What Should Organizations Do?

So, based on these changes and existing case law, what should an organization do in response to the new FRCP amendments? Here is a summary of the key steps that any organization should undertake:

- Review and assess existing document retention policies and practices. It makes sense to evaluate these policies now rather than waiting for litigation.
- Pay close attention to e-discovery issues from the earliest stages of litigation.
- Learn what types of electronic data exist in the organization and that might be needed very early in the litigation process.
- Investigate the amount and cost of preserving, restoring, processing and reviewing relevant electronic data.
- Assess the format of production that is appropriate for the organization and each case.
- Determine an appropriate protocol for privilege and waiver claims.

For organizations that were already aware of e-discovery and electronic data retention issues before, the new FRCP amendments simply incorporate those issues into the civil rules for litigation. However, organizations that have not considered e-discovery and electronic data retention issues should start now.

In short, the new amendments will place a greater focus on electronic discovery early in the litigation process; they will require the location, identification and categorization of ESI; they will expand the scope of subpoenas in the context of accessing ESI; and interrogatories that are focused on a review of business records can now specifically identify a search of ESI.

For organizations that were already aware of e-discovery and electronic data retention issues before, the new FRCP amendments simply incorporate those issues into the civil rules for litigation. However, organizations that have not considered e-discovery and electronic data retention issues (which Osterman Research has found is a sizable proportion of organizations) should start now.

Focus on Data Governance

Regardless of an organization's size or the industry in which it operates, a comprehensive corporate governance plan should be established that includes specific and detailed policies focused on data retention and disposal, as well as on other aspects of email, instant messaging content and

electronic document management. Organizations must understand the types of data that constitute business records (and so must be preserved), how long and in what form these records must be preserved, and when they can safely be destroyed.

Although retention of email, instant messages and other types of electronic documents is a necessary component of normal backup and disaster recovery requirements, data governance goes well beyond these requirements. Data governance focuses on the entire set of demands for data retention that are driven by regulatory compliance, legal discovery considerations, log management, industry-specific requirements and other demands.

In order to satisfy the requirements of the FRCP, organizations must implement systems that can a) capture information that must be preserved, b) store this information in a such a way that its integrity can be maintained and c) produce this information on demand in a cost-effective and timely manner.

Although the FRCP changes apply primarily to e-discovery, data governance focuses on a much wider set of requirements for data retention, including regulations like Sarbanes-Oxley, the Gramm-Leach-Bliley Act, the Health Insurance Portability and Accountability Act (HIPAA), various SEC requirements, and various requirements from the NASD, to name just a few of the many requirements that must be satisfied depending on the industry in which an organization participates.

Implement Technologies That Can Help the Organization Meet Corporate Governance Requirements

In order to satisfy the requirements of the FRCP, organizations must implement systems that can a) capture information that must be preserved, b) store this information in a such a way that its integrity can be maintained and c) produce this information on demand in a cost-effective and timely manner.

The most logical method for storing email, instant messages and other types of ESI is an archiving system that can satisfy all of these requirements. An appropriately configured archiving system will capture business records and other important content based on a pre-defined set of business rules and policies, store this content in a secure repository and provide robust search tools that will permit production of the data on demand with as little disruption to IT staff and others as possible.

Develop a Unified System

As a best practice for compliance with the new FRCP amendments, organizations should develop a unified system that spans archiving, backups, policies and overall media

management. It is important to consider everything from simple backups to complex archiving requirements as part of a continuum of data governance practices that must be managed cohesively. In short, all of the data that an organization generates should be managed as part of unified data management strategy that can address not only FRCP requirements, but also regulatory obligations, employee productivity issues, IT efficiency issues and other requirements.

Summary

The new FRCP amendments are critically important for both IT managers and business decision-makers to understand and consider, since they raise the importance of data governance practices to a new level. Instead of proper data retention being simply a best practice for organizations to follow, data retention is now a legal obligation that can carry with it serious consequences if managed poorly. While backup, archiving and other data retention capabilities are an important component of a proper data management strategy, organizations must adopt a holistic approach to managing data, particularly the growing proportion of electronically stored information that they manage.

About the Authors

John A. Heer

John A. Heer has counseled clients for more than 15 years in a wide variety of complex civil litigation and environmental matters. John is also a respected speaker and author on topics such as electronic discovery and evidence, litigation tactics, and environmental law. John's recent presentations and speaking engagements include:

- "E-Discovery: Get Ready To Apply The New FRCP Changes" at NBI Seminar in Cleveland in December 2006
- "Discovery in Environmental Cases: Securing Documents By Public Record Act and Electronic Discovery" at the Ohio State Bar Association's Environmental Law Seminar in April 2005
- "Electronic Evidence and Discovery Issues" at the Florida Bar Association's 2005 Health Law Institute in Orlando,

Florida in February, 2005

- "Litigating in Cyberspace" in an American Health Lawyers Association teleconference seminar in September, 2003
- "Electronic Discovery Issues" at a Cleveland Bar Association seminar in June 2003
- "Capturing Key Evidence Through Electronic Discovery in Ohio" at a NBI seminar in Cleveland, Ohio in March, 2003.

His article, "A Broad-Brush Look at Electronic Discovery Issues When Advising Your Clients," was featured in the February, 2004 *American Health Lawyers Association Health Lawyers News*; the May 15, 2004 issue of *The Lawyer's Brief* and the July 2004 issue of *Corporate Counsel's Quarterly*.

John received his B.A. from Indiana University and his J.D. cum laude from Case Western Reserve University School of Law. John is an Associate of the Environmental Law Institute and a member of the American, Ohio State and Cleveland Bar Associations.

Michael D. Osterman

Michael Osterman is the principal of Osterman Research, Inc., founded in 2001. Since that time, the company has become one of the leading analyst firms in the messaging and collaboration space, providing research, analysis, white papers and other services to companies like Microsoft, America Online, Sun Microsystems, Yahoo!, Network Appliance, Iron Mountain, Postini, Hewlett Packard and many others.

Michael is a frequent speaker at industry and vendor-sponsored events on the topics of archiving, instant messaging, presence and other messaging-focused issues. He is also the author of a twice weekly column on unified communications issues for *Network World Fusion*.



1159 Triton Drive
Foster City, CA 94404
(888) 349-FACE
www.facetime.com

White Paper Sponsor

FaceTime enables the safe and productive use of public and enterprise instant messaging, Skype, Web conferencing and P2P file sharing. Ranked number one in Enterprise IM Management by IDC for three consecutive years, FaceTime's award-winning solutions are used by more than 800 organizations, among them nine of the top 10 U.S. banks as well as household names like Allstate, General Electric, McDonalds, Phillips, and Turner Broadcasting among its customers. These organizations depend on FaceTime to easily monitor, audit and secure IM conversations as well as more than 100 other greynet applications traversing their networks.

FaceTime's IMAuditor secures and manages all public and enterprise instant messaging (eg Microsoft LCS and IBM Sametime) use over an organization's network to prevent inbound threats from worms, viruses and other malware, protect against information leakage and maintain regulatory and e-Discovery compliance across all communications applications. IMAuditor, which resides on the LAN, maintains an integrated trust relationship with FaceTime's perimeter product, Real-Time Guardian (RTGuardian). These two products form FaceTime Enterprise Edition to deliver complete end-to-end security, management and compliance coupled with a mechanism for detecting and preventing rogue or unauthorized IM usage. Key features include Regulatory Compliance Archiving and Workflow, Centralized Management and Control, Content Hygiene and Security, Enterprise Integration and Extensions and Extensive research capabilities.

The company also has strategic partnerships with all leading public and private IM network providers, including AOL, Google, Microsoft, Yahoo!, IBM, Reuters, Bloomberg, WebEx, and Jabber. In 2006, FaceTime received SC Magazine's Reader's Trust Award for IM Security, the Network World Clear Choice Award and the World Class Award from Network Test Labs.

FaceTime provides a real time, scalable solution that offers:

➤ *Centralized, tamper-proof recording and archiving of all IM conversations, file transfers, and associated metadata that:*

- *Includes time and date stamping & identification of all participants*
- *Reduces costs from having to piece together conversations from multiple sources*
- *Leverages existing e-mail archiving and storage infrastructure*
- *Supports the strictest interpretation of compliance regulations and e-discovery requirements through unique TrueCompliance™*

➤ *Reduced cost and complexity*

- *Ensures ability to meet e-Discovery deadlines and minimizes financial exposure*
- *Enables search by case number, employee, time period and more, to avoid high costs associated with piecing together conversations from PCs, backup tapes, servers, smartphones, USBs, and other devices*

➤ *Enforcement of corporate usage policies regarding real-time communications*

- *Prevents the inclusion of inadvertent IM and other chat records as part of e-Discovery*

© 2007 Osterman Research, Inc. All rights reserved.

No part of this document may be reproduced in any form by any means, nor may it be distributed without the permission of Osterman Research, Inc., nor may it be resold by any entity other than Osterman Research, Inc., without prior written authorization of Osterman Research, Inc.

THIS DOCUMENT IS PROVIDED "AS IS". ALL EXPRESS OR IMPLIED REPRESENTATIONS, CONDITIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OR FITNESS FOR A PARTICULAR PURPOSE, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE DETERMINED TO BE ILLEGAL.