

CHAPTER 1
E-Discovery
Begins With a
Retention Policy

CHAPTER 2
In Search of ...
E-records Man-
agement Tools

CHAPTER 3
Don't Forget
Facebook

CHAPTER 4
Making Email
Retention Work



Email Retention: Standards and Practices

Electronic records are as real as paper documents. Learn how to manage the data for e-discovery and recovery.

E-Discovery Begins With A Retention Policy

With a few simple steps, you can help prevent electronic discovery surprises and costly fines.

BY JOHN WEATHINGTON

What's happening in today's court system when it comes to compliance violations is a transposition of guilt and innocence. I constantly tell my clients that it's not good enough anymore to just do the right thing; you must be able to *prove* that you're doing the right thing. Once you establish your intent is pure, you're literally 80% out of compliance harm's way.

EMAIL RETENTION IS low-hanging fruit for IT, so it's surprising how often I see it done wrong. When done properly, e-mail retention as part of a comprehensive records retention policy can prevent potential compliance problems. When done wrong, however, it can cost your company millions of dollars.

Email retention is a very simple task both for you in IT and the rest of your organization. I recently wrote an article for SearchCompliance.com wherein I mentioned a company that was fined \$2.75 million for improper email handling (see "[E-Discovery Critical to Corporate Health](#)," page 4). This had nothing to do with its archiving strategy or reproduction of email records. The company simply did not handle its email processing properly.

START WITH A RECORDS RETENTION POLICY

Your company absolutely must have a records retention policy. Note that I didn't say *email retention policy*, because an email is just one of many ways a record can be created. This is important to understand: It's not email, per se, that drives retention consideration—it's about what's in the email.

If your company does not have a record retention policy, then I recommend you have an off-site with all the stakeholders and figure it out immediately. If you get caught with a legal problem and you have no records retention policy in place, you're as good as guilty.

With policy in hand, your next step is to create a policy database to man-

CHAPTER 1
[E-Discovery Begins With a Retention Policy](#)

CHAPTER 2
[In Search of ... E-records Management Tools](#)

CHAPTER 3
[Don't Forget Facebook](#)

CHAPTER 4
[Making Email Retention Work](#)

age and record things. In your policy database, you'll need to capture the following attributes:

- **Policy version and date:** Anytime the policy changes for any reason, a new record needs to go into your database so you can review what the policy was at any point in time.
- **Document type:** The document type will drive the retention and destruction properties. This is a general term, and may end up being two or three fields.
- **Retention period:** How long documents of this type should be retained. Once again, it's up to your company to decide how many phases of retention (i.e., on-site, off-site, etc.) records need to go through.
- **The policy:** You should have a scanned image of the policy available in your database in case there's any confusion.

BUILDING THE EMAIL RETENTION SYSTEM

How you handle your non-email records (instant messages, typed documents, etc.) is beyond the scope of this chapter; however, be aware that it's just as important as your email retention system. Let's focus for now on building your system for email retention.

A good email retention system does four things:

- **Captures every email** and stores it in an immutable state.
- **Indexes the contents** of every email so it can be researched effectively.
- **Retains every email** for exactly the period of time required (as dictated by its document type), then obliterates it and every trace that it existed.
- **Has an "in case of emergency" switch** that completely disables the obliteration functionality mentioned above.

Sounds easy enough, right? Good—don't overcomplicate things. Start with a write-once, read-only database (similar to the old-style CDs). Centralize your email traffic and send everything to this database. The database needs to store every email in two forms. First, scan the email into an image for permanency, then hyper-index the contents as any Internet search engine would. This handles the first two bullets.

Metadata in the email should convey what document type we're dealing with, which will tell us what the retention period should be. With this information, stamp every single email with a "destroy on" date. On this date, blast this email to pieces unless the "in case

CHAPTER 1
[E-Discovery Begins With a Retention Policy](#)

CHAPTER 2
[In Search of ... E-records Management Tools](#)

CHAPTER 3
[Don't Forget Facebook](#)

CHAPTER 4
[Making Email Retention Work](#)

of emergency” switch has been activated. Ensure your email system is airtight and that there are no copies of this email floating around anywhere (i.e., in personal folders). Be very serious about destruction. Having incriminating email available can get you into more trouble than not having it available.

The “in case of emergency” switch is mandatory in case of a litigation hold. This is the trump card of email retention. If your legal department issues a litigation hold, all email traffic must be retained, no matter what, until the litigation hold is lifted. That

\$2.7 million fine I referenced earlier was imposed because a litigation hold was issued and the company continued to delete emails. In the court’s eyes, it was an admission of guilt.

It’s not hard to build a good email retention system—it starts with a policy and finishes with good IT architecture. Start today by creating or revisiting your existing email retention policy. The benefits will far outweigh the few days it will take to get things going. ■

John Weathington is president and CEO of Excellent Management Systems Inc., a San Francisco-based management consultancy. For more information, visit www.excellentmanagementsystems.com.

CHAPTER 1
[E-Discovery Begins With a Retention Policy](#)

CHAPTER 2
[In Search of ... E-records Management Tools](#)

CHAPTER 3
[Don't Forget Facebook](#)

CHAPTER 4
[Making Email Retention Work](#)

E-Discovery Critical to Corporate Health

NOT RESPONDING TO an electronic discovery request is just as good as an admission of guilt, and this downfall lies squarely on the shoulders of the IT organization. In the well-known case of Zubulake v. UBS Warburg LLC, UBS could not produce potentially incriminating emails critical to the case, and the courts actually ruled that it was more likely than not these emails existed. This had damaging effects on UBS's case. Likewise, in United States v. Philip Morris USA Inc., Philip Morris was fined \$2.75 million for continuing to delete emails after a notice of litigation was issued.

Cases like this have instantiated a tidal wave of fear in organizations, and just as they did in response to the Sarbanes-Oxley Act, organizations have seemed to overreact, overcorrect and overspend. And, as with Sarbanes-Oxley, I'm now hearing electronic discovery used as a blanket excuse to justify IT processes and spending that serve no business purpose. Continue down this road, and you won't need to worry about a lawsuit because there will be no company left to sue.

So how do you put these e-discovery concerns to rest for good?

- Get your IT organization under control. Know where your data is at all times.
- Coordinate with finance, legal and other departments to clearly understand your document retention and destruction policies.
- Hope for the best, but plan for the litigation hold. —J.W.

Restoring all those
back up tapes (again)
to search for emails
made me go Google.

www.google.com/postini/gogoogle

 postini services

© Copyright 2009 Google. All rights reserved. Google and the Google logo are registered trademarks of Google Inc.

In Search of ... Electronic Records Management Tools

CHAPTER 1
[E-Discovery
Begins With a
Retention Policy](#)

CHAPTER 2
[In Search of ...
E-records Man-
agement Tools](#)

CHAPTER 3
[Don't Forget
Facebook](#)

CHAPTER 4
[Making Email
Retention Work](#)

E-records are equivalent to paper records in regulatory compliance or legal cases, so find the right strategy and tools for retention and recovery.

BY STAN GIBSON

IT'S A NIGHTMARE waiting to happen at many enterprises: the arrival of an order to produce documents—and the clock is ticking.

An organization that's prepared could vindicate itself before a court of law or regulatory body with only modest expense; an organization that's not ready could find itself consumed by a costly and ultimately unsuccessful scramble to produce materials from a welter of systems with search tools that are unequal to the task.

Although companies that are wont to be on the receiving end of lawsuits,

such as tobacco and pharmaceutical firms, are no strangers to the rigors of the discovery process, the advent of regulations such as the Sarbanes-Oxley and Health Insurance Portability and Accountability acts is causing a wave of concern through companies of all sizes in practically all industries. Further, amendments to the Federal Rules of Civil Procedure governing e-discovery that took effect in December 2006 mandate that electronic records be considered equivalent to paper records in the discovery process.

If that weren't enough, the tough economy is exacerbating matters. Increased regulation following the financial markets' meltdown of 2008, coupled with lawsuits to redress grievances due to job losses and broken contracts, are fueling an unwelcome e-discovery boom.

RETURN ON INVESTMENT LACKING
A CIO at a financial industry company, who asked to remain anonymous, saw the handwriting on the wall and built a document management system to

accommodate audits by the Securities and Exchange Commission, which regulates his industry.

"We have a cost-effective system that helps us fulfill our obligation of compliance. We have the ability to produce documents," he says. Still, the executive has no illusions as to the nature of the e-discovery burden. "None of this generates a single iota of revenue. There is no return on investment. The only way I can justify it is that the cost is less than the fines we might get if we don't do it," he says.

Although the civil procedure rule changes of 2006 included measures to discourage the use of e-discovery as a weapon with which to harass defendants, more significantly they took away from defendants the excuse that, "The computer ate my homework," according to John Bace, an analyst at Stamford, Conn.-based Gartner Inc.

"We saw this in the case of Enron and MCI Worldcom. They said their systems were too complicated for them to produce [relevant documents]," Bace says. But, he explained, the new rules regarding electronic records management have teeth. "If you can't produce ESI [electronically stored information], you are subject to the same sanctions and penalties if you had destroyed the evidence on purpose. It can be as little as a fine, a negative instruction to the jury, or being held in contempt of court."

The new rules have made them-

selves felt in court, according to Florinda Baldrige, director of practice support at Fulbright & Jaworski LLP, a large law firm in Dallas. "There's a lot of case law evolving around e-discovery, including how technology is used in the search for evidence," Baldrige says. No less significant, she points out, is the impact of the rules on enterprise IT. "The inclusion of electronic documents has increased the universe of potentially discoverable documents exponentially, while the deadlines for discovery have remained the same, creating both time and cost constraints. You have to find it and produce it in a defensible manner. You have to make a diligent effort."

SEARCHING A 'TOXIC WASTELAND'

Diligent effort or no, many organizations aren't ready, Bace says. "Most corporations have not had very good document hygiene. There is a toxic data dump of information. When they need to produce it, it's near impossible to do," he says.

One of the reasons many companies aren't ready is that data is stored in different places: in corporate databases, email and instant message archives, as well as voicemails—all of which are governed by different retention policies and searchable by different tools.

"E-discovery is large and fast-growing, but it's at an early stage, with many immature components. Technology fragmentation within enter-

CHAPTER 1
[E-Discovery Begins With a Retention Policy](#)

CHAPTER 2
[In Search of ... E-records Management Tools](#)

CHAPTER 3
[Don't Forget Facebook](#)

CHAPTER 4
[Making Email Retention Work](#)

prises is remarkable," says Brian Hill, an analyst at Cambridge, Mass.-based Forrester Research Inc. The quandary is paralyzing many organizations. According to Forrester, only 17% of companies in a recent survey said they were confident that their electronically stored information would be accurate, accessible and trustworthy in the event of an e-discovery proceeding.

The stakes of inaction are high. According to a report issued in 2007 by The Sedona Conference, an organization that creates standards for e-discovery, it costs approximately \$1 to store a gigabyte of data and \$30,000 to review it.

BEST PRACTICES FOR E-DISCOVERY

Savvy organizations are waking up to the inevitable and taking action, usually forming a task group as the first step. Baldrige and others recommended the committee include leaders from legal, IT, human resources, finance and operations. "It's critical to bring those stakeholders together—it's not just a technology issue or just a legal issue," Baldrige says. Such a group can help overcome an endemic problem identified by Hill: "Key stakeholders in IT and legal don't communicate and collaborate as they should," he says.

Despite differences, group members must identify electronic documents that may be encompassed in a discovery proceeding in order to establish a

document retention policy. Tax records must be kept for seven years; other data, such as email traffic, should be deleted after a matter of months according to a regular electronic records management schedule. The group must also consider technology tools for document management and archiving, of which choices range from on-premises applications to Software as a Service offerings.

Task groups should pay attention to a growing body of best practices information compiled by different organizations, such as The Sedona Conference. In an effort to help enterprises get a handle on e-discovery search, the Text Retrieval Conference initiative of the National Institute of Standards and Technology has conducted annual studies to bring best practices to light. The Electronic Discovery Reference Model group is also crafting practical guidelines and standards for e-discovery.

THE SEARCH FOR BETTER SEARCH

Sooner or later, the question of search technology must be addressed. Some corporate task groups start with the assumption that the capabilities of Microsoft's Exchange 2007, Google Desktop or enterprise search tools such as the Google Search Appliance are good enough. Lawyers and judges often have a similar impression. "A lot of the courts think that if you can Google the entire Internet, then why can't you just Google the enterprise,"

CHAPTER 1
E-Discovery Begins With a Retention Policy

CHAPTER 2
In Search of ... E-records Management Tools

CHAPTER 3
Don't Forget Facebook

CHAPTER 4
Making Email Retention Work

Bace says.

Experience is showing, however, that a different kind of search is needed for e-discovery. While enterprise search tools are intended to make knowledge workers more productive, e-discovery search tools are geared to support a legally mandated discovery

initiative by applying clear search criteria, tracking searches meticulously and keeping costs low (see “Industry Standards Aid Archiving, Electronic Discovery Process,” below).

While enterprise search tools typically discover a plethora of documents, ranking them from most to

CHAPTER 1
[E-Discovery Begins With a Retention Policy](#)

CHAPTER 2
[In Search of ... E-records Management Tools](#)

CHAPTER 3
[Don't Forget Facebook](#)

CHAPTER 4
[Making Email Retention Work](#)

Industry Standards Aid Archiving, Electronic Discovery Process

THE PERFECT STORM of new regulation, increased litigation and proliferation of electronic data has led to widespread concern over the problems of archiving, discovering and producing electronic records in answer to court cases and regulatory enforcement. In response, several organizations have launched initiatives to help businesses understand the requirements of e-discovery and how to execute a sound discovery process.

The Sedona Conference's Electronic Document Retention and Production group, known as WG1, has issued a number of publications, including a paper published in May covering best practices in implementing a sound e-discovery strategy. In addition, the Sedona Conference Collaboration Project brings together judges, trial lawyers, corporate and government counsel, technical experts and academics to develop tools to reduce adversarial tension, cost and delay during pretrial discovery.

The TREC Legal Track is an annual research project that studies the e-discovery process and evaluates search methods. The 2009 TREC Legal Track consists of an interactive task in which participants will strive to produce a set of documents from public Enron data. A separate batch task will consist of searching the Web database of 7 million documents in the Tobacco Master Settlement, using hypothetical requests to produce documents. TREC is co-sponsored by NIST and the Department of Defense.

EDRM is an organization consisting primarily of law firms, litigation support companies and technology vendors. The group crafts practical guidelines and standards in order to reduce the cost, time and work required by e-discovery. EDRM has developed an XML standard to help e-discovery products interoperate. —S.G.

CHAPTER 1
[E-Discovery Begins With a Retention Policy](#)

CHAPTER 2
[In Search of ... E-records Management Tools](#)

CHAPTER 3
[Don't Forget Facebook](#)

CHAPTER 4
[Making Email Retention Work](#)

least relevant and likely including some that are irrelevant, e-discovery search tools must find only the relevant documents—but they must find all of them. That's because documents unearthed in the e-discovery process must be read and analyzed by lawyers, a step that can add tremendous cost to the project if false positives are permitted among the documents retrieved. In addition, the e-discovery search process must be defensible—that is, clearly and convincingly explained to a nontechnical judge or regulatory body. That may not be possible to do if the search tool is not specifically designed for e-discovery tasks.

Advances in search technology are improving a company's chances of not being taken to the cleaners when a legal hold order or e-discovery request appears. Traditional search engines find documents containing keywords often linked with Boolean operators such as *and*, *or*, *not* or *near*. Several vendors have crafted products and services that implement conceptual search, which looks for groups of words, rather than single word matches. Others implement fuzzy search, which finds documents that are predicted to be relevant, even though they do not contain the specific word in question.

Baldrige uses a tool from Recommend Inc. called Axcelerate, which implements a conceptual search technology that Recommend calls predictive tagging to winnow documents to

a relative handful for lawyers to review. "Otherwise, you might not get to those documents until \$100,000 into the review process," Baldrige says. "Axcelerate gives you a seed set. You can assess whether you want to proceed with the case or not. In the old Boolean search approach, it may take months to find the same documents."

Another vendor, Clearwell Systems Inc., offers a search appliance called E-Discovery Platform, which uses conceptual search to cull a manageable quantity of files from email systems, databases and enterprise applications. The Clearwell appliance is pointed to a data store, such as an Exchange server, database or archive on which it performs a conceptual search. Alternatively, the data can be collected with a tool such as Microsoft's Robocopy and then searched with the appliance. Networking giant Cisco Systems Inc. has implemented the Clearwell E-Discovery Platform so its lawyers can search, analyze and review documents remotely via a secure virtual private network, Clearwell officials said.

Page One LLC, a litigation support company in Nashville, Tenn., uses the MetaLINCS E-Discovery search tool from i365, a subsidiary of Seagate Technology LLC, to boil down piles of data to a manageable level. Law firms in the Tennessee and Kentucky area call on Page One when a client receives a legal hold order. Page One then feeds the data to the i365 MetaLINCS E-Discovery server, which uses

a conceptual technology called pinpoint search.

Page One president Rip Clayton says his firm can save a company hundreds of thousands of dollars with the tool, compared with having lawyers pick through irrelevant material. "They don't have to bill at \$250 per hour over stuff that IT has turned up incorrectly," he says. Using the MetaLINGS server, Page One performs data deduplication, then creates a detailed chain of custody that includes page-level and Bates numbering, which numerically organizes files as evidence, Clayton says.

Fios Inc., a Portland, Ore.-based provider of hosted e-discovery services, uses a variety of technologies, including keyword and conceptual search, to cull through data. Law firms send Fios data either electronically or by shipping a hard drive. The company's Prevail service incorporates both desktop keyword search and conceptual search from such companies as Content Analyst Company LLC and Kroll Technologies LLC. Brad Harris, director of product management at Fios, says his firm is performing e-discovery services over voicemail records for many clients using technology from Nexidia Inc.

E-discovery search tools are critical in determining whether to defend a case or to settle. If e-discovery costs \$10 million and the suit will cost only \$5 million, then it makes sense to settle. "This helps you discover what you're in for before you spend the \$10

million," Fulbright & Jaworski's Baldrige says. "Attorneys say they have to look at every document, but Recommind helps you look at the most important documents first."

BOTTOM LINE: BE PREPARED

As courts and regulatory bodies have awakened to the electronic age, businesses of all kinds must prepare for the unwanted day they must produce documents upon demand. Organizations should form a corporate task group to implement document management policies and should decide whether handling e-discovery tasks in-house or relying on litigation support service providers makes the most sense. Whatever the path chosen, the goal is the same: to avert catastrophic e-discovery costs, unfavorable out-of-court settlements and stiff penalties.

Because many of the regulations enacted within the past several years are just now beginning to be applied, organizations must pay attention to enforcement patterns as well as evolving e-discovery case law. As e-discovery search becomes more mature, courts are likely to expect a certain level of competence and when it's not there will likely levy penalties. Says Forrester's Hill, "Organizations are not yet willfully negligent for not having search in place, but that is where we're ultimately going to head." ■

Stan Gibson is a Boston-area technology writer. Write to him at editor@searchcompliance.com.

CHAPTER 1
[E-Discovery Begins With a Retention Policy](#)

CHAPTER 2
[In Search of ... E-records Management Tools](#)

CHAPTER 3
[Don't Forget Facebook](#)

CHAPTER 4
[Making Email Retention Work](#)

Email Archiving

A key aspect of enterprise information governance



Document volume is growing, in no small part thanks to email. Compliance rules, regulations, and laws governing content are also expanding.

Your information governance solution must give you centralized control. While supporting distributed, disparate content – from email, to reports and statements, to customer records.

So far, archiving solutions have failed to break the concrete bond between policies and repositories.

The time has come for a change.

To learn more, please visit us at www.rsd.com.

Founded in 1973 in Geneva, with affiliates in New York and London, RSD helps companies meet the growing challenge of information governance by providing market-leading products for business information delivery, content and records management, and document archiving and retrieval.

RSD solutions are used by more than 1,200 organizations worldwide, including a majority of the Fortune 500. Today RSD supports over 2 million users, and offers its innovative products and services in more than 26 countries around the globe – both directly and through strategic business partners.

Don't Forget Facebook

Businesses seek retention strategies for social media, instant messaging and texts.

BY ALEXANDER B. HOWARD

EMAIL RETENTION STRATEGIES are an important element of compliance for organizations subject to the Sarbanes-Oxley Act or other regulations that require companies to retain client communications.

In recent years, the explosion of social media messaging has stimulated a wave of vendor interest and development of new versions of monitoring, filtering and logging software suites to capture sensitive data before it reaches the public Internet.

In many enterprise and business environments, however, security and compliance officers have simply chosen to eliminate security risks by blocking access. According to a recent study from ScanSafe Inc., 76% of the San Francisco-based company's customers are now blocking social networking sites in the workplace.

Michael Seese, an IT security manager at a large Midwestern bank and author of *Scrappy Information Security*, says his organization has followed precisely this path. "We use a third-party service that puts labels on websites, like 'social networking,' and then block access to that category," he says. "We do get instances, monitored by a mailbox, where a site is mislabeled. We also get requests from people in our collections group that want access to Facebook or MySpace. Those people that have a legitimate business need have an Active Directory group that allows them external access."

FINANCIAL INSTITUTIONS REQUIRE SPECIAL MEASURES

Such an approach can be a cultural issue, however, and is generally not mandated by regulations—at least not yet. "The reality is most organizations don't need to do this," says Rich Mogull, an IT security analyst at Securosis. "That's not true for the financial industry, perhaps, but for the average organization, there's no regulatory requirement. Organizations are going to have a balance as more employees use social media at work."

Daniel Kennedy, chief information

CHAPTER 1
E-Discovery Begins With a Retention Policy

CHAPTER 2
In Search of ... E-records Management Tools

CHAPTER 3
Don't Forget Facebook

CHAPTER 4
Making Email Retention Work

security officer (CISO) and partner at Praetorian Security Group LLC, was previously the IT liaison at a financial institution for requests made by the Securities and Exchange Commission (SEC). In that role, Kennedy had to comply with SEC rules 17a-3 and a-4.

“For an IT person, it is most relevant to note that emails and instant messages are considered books and records under the exchange acts,” he says. “17A-4 includes further requirements, including storage of three to six years depending on record type; a requirement for write-once, read-many storage; accuracy verifications; indexing requirements; auditing capability; and related requirements.”

In his experience, however, “compliance officers seem to have settled on seven years’ retention as the right number that captures both SEC and other regulatory requirements in place. The firms I have dealt with have simplified whether a communication is brokerage-related by storing all communications.”

Requirements for storing and managing such messages can quickly become relevant if the SEC comes calling. These “take the form of requests for all correspondence in a specified time period between certain parties, on certain topics, or any combination of the two,” Kennedy says. “Accuracy of preservation and the fact that you have captured all relevant communication is something you are asked about eight ways to Sunday. Inconsistencies here will kill you, as

the most senior resources in your firm are attesting that the information provided fully meets what is being requested.”

INSTANT MESSAGING ARCHIVING

Kennedy also had to address instant messaging archiving for the financial institution. “We used FaceTime to register all instant messaging IDs and store all instant messages sent by firm associates,” he says. “An MS SQL Server database was the back end for this application. We allowed a common variety of instant messaging programs, as the corporate culture was such that this level of flexibility was desired.” That meant that Yahoo Messenger, Google Talk, MSN Messenger and a number of aggregators were all archived.

Kennedy also ran into a retention issue common to many financial institutions: Many of the brokers used Bloomberg terminals, which have their own email and instant messaging (IM) applications. Since Bloomberg provides the messages using an FTP solution, Kennedy was able to work with an intermediary to translate and archive these messages on the same storage system that the email and other IM data was stored on.

“We usually looked at the intrusion detection system to see if any chat messages were being sent out from machines that were not the FaceTime servers,” Kennedy says. “The few folks who had admin rights had separate

CHAPTER 1
E-Discovery Begins With a Retention Policy

CHAPTER 2
In Search of ... E-records Management Tools

CHAPTER 3
Don't Forget Facebook

CHAPTER 4
Making Email Retention Work

accounts with which to use them. Software inventory lists from BigFix were checked quarterly for all employees and monthly for high-privilege users to ensure no unauthorized installations were in place. Noncompliance with these policies was dealt with according to a corrective action policy.”

Mogull says he does see cause for concern “in terms of malware, as hackers use social media sites to go after enterprises,” adding that he believes the “risk is low now but growing as social engineering attacks step up.”

PROACTIVE SOCIAL MEDIA MONITORING

Beyond security risks, however, ensuring that sensitive data does not leave the enterprise is crucial—particularly when it comes to the personally identifiable information of customers, clients and employees. When security and compliance professionals focus on data protection, as opposed to simply monitoring all employee communications, the task becomes both more focused and justified for clear business purposes. The challenge is that the social networking platforms employees are likely to use are external to the enterprise.

Michael Murray, vice president of professional services and CISO at Foreground Security, who has implemented retention technology, says he has seen harassment and leakage of inappropriate content from business-

es. That’s led to concerns about brand protection through the use of social media. He says in his experience, the issue is that they’re all technologies the enterprise “ultimately doesn’t

“I think applying email retention policies to communication channels is a losing proposition. Documents aren’t atomic, and the atoms of these documents can switch between media faster than IT policy.”

—IAN GLAZER,
senior analyst, Burton Group Inc.

own,” whether it’s a third-party instant messaging system like AOL Instant Messenger or Google Talk, or social media platforms like Twitter, LinkedIn or Facebook.

In Murray’s experience, he says, the problem of social media monitoring is two-sided. “Due to the lack of control of the central server, retention either falls to the responsibility of the user, which is difficult if not impossible to enforce; relies on some version of kludge at the desktop level; or relies on some new and unproven service that hasn’t shown itself to have enterprise scalability, like some of the

CHAPTER 1
[E-Discovery Begins With a Retention Policy](#)

CHAPTER 2
[In Search of ... E-records Management Tools](#)

CHAPTER 3
[Don't Forget Facebook](#)

CHAPTER 4
[Making Email Retention Work](#)

recently developed Twitter ‘backup’ systems.”

Larger strategic challenges are at issue as well. “I think applying email retention policies to communication channels is a losing proposition,” says Ian Glazer, a senior analyst for Burton Group Inc.’s identity and privacy strategies service. He says he sees significant challenges to traditional perimeter-centric processes that seek to control social messaging.

“Documents aren’t atomic, and the atoms of these documents can switch between media faster than IT policy can keep up,” he says. “Let’s say you and I work for the same enterprise. We start a conversation at work in the halls. It leads to a few internal wikis getting updated. On the drive home, you text me with another thought. We connect that evening on Facebook chat.”

Tim Brown, vice president and chief architect for security management at CA Inc., says he has observed a convergence of employee private and working lives. “In the past, a private person could post or do anything and it wouldn’t be related to the enterprise,” he says. “Those days are really gone. You can suggest some things and mandate others—no defamation, as a corporate employee, for instance—but from an enterprise perspective this comes down to privacy policy and what’s expected. The issue is when employees go home and use personal devices. We also can’t control what other people are posting.”

Andrew Hay, an analyst in the information security office of the University of Lethbridge in Alberta, says his department is working on more ways to capture more of these streams, at least for email. According to Hay, his group is moving toward a “new email infrastructure, which will allow us to perform more e-discovery and data mining of information to use in incident response and forensic analysis exercises.” Hay adds he anticipates more effective analysis of where sensitive data left the organization and the ability to more easily audit messages.

DATA LOSS PREVENTION A SOLUTION?

The issue for social messaging, in Glazer’s assessment, lies in the document-centric focus of most data loss prevention (DLP) software, as opposed to identity-centric solutions. DLP software represents one potential method of addressing the issue, although he cautions that technology needs to focus on the individual, not the document.

“DLP and traditional perimeter-centric technologies fail mostly because technology isn’t at the center,” he says. “It is our interactions—humans engaged in social behavior. Here awareness, training and policy come into play, and this is the most difficult of situations as the enterprise has to attempt to shape our behavior in order to stay compliant.”

CHAPTER 1
[E-Discovery Begins With a Retention Policy](#)

CHAPTER 2
[In Search of ... E-records Management Tools](#)

CHAPTER 3
[Don’t Forget Facebook](#)

CHAPTER 4
[Making Email Retention Work](#)

Murray says he has functionally applied this perspective to his work. In fact, he says, “the difficulties of implementation have led any client I’ve worked with on this to determine that the risk of potential failure in the execution of the retention strategy made it easier to write these technologies out of the retention policy altogether and declare that they’re not formally approved business artifacts.”

Kennedy says he simply focused on the ability of social networking sites to allow employees to send messages, thus creating an archiving need. If you remove that ability, the issue is partially addressed. “If we could accommodate it, for example on LinkedIn, we tried to make things easier for employees by allowing access to parts of the sites that would not cause us a message retention issue,” he says.

“Facebook was a nonstarter, as there was no way to explain to a senior manager how allowing access to the site was work-related, the usual minimum criteria for fine tuning policy rules.”

Twitter was also blocked at Kennedy’s financial institution, although “certain exceptions were made where a business case could be made.” In his view, he adds, Twitter is “a little different in that, like news services, it can be used for research, keeping up with industry resources.” The messaging requirements are still in effect.

“Direct messages are akin to email, or at the very least SMS-style messages,” Kennedy says. “We logged and

retained SMS messages sent from company devices [BlackBerrys] just like everything else. Theoretically, you

“Facebook was a nonstarter, as there was no way to explain to a senior manager how allowing access to the site was work-related, the usual minimum criteria for fine tuning policy rules.”

**—DANIEL KENNEDY, CISO,
Praetorian Security Group LLC**

can get Twitter alerts via SMS, but if you did it on a company device it would be logged.”

Not logging social messaging can expose an organization to a different sort of risk, if a judge finds that social messaging is pertinent to an e-discovery order. The bottom line is that compliance officers should be ready for e-discovery with a records retention policy. Mogull recommends that organizations “start with DLP and look at Web gateways that filter malware to protect against infection.” ■

Alexander B. Howard is the associate editor for SearchCompliance.com. Write to him at ahoward@techtarg.com.

CHAPTER 1
E-Discovery Begins With a Retention Policy

CHAPTER 2
In Search of ... E-records Management Tools

CHAPTER 3
Don't Forget Facebook

CHAPTER 4
Making Email Retention Work



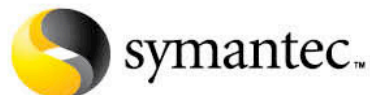
SYMANTEC IS

Up to 75% of your company's intellectual property exists within email. Using market-proven architecture, Enterprise Vault™ 8.0 provides an intelligent approach to improving email management, reducing costs, and controlling your information risk. It's a smart solution for archiving your most valuable data.

For an Email Health Check, visit enterprisevault.com today.

EMAIL ARCHIVING.

Confidence in a connected world.



symantec™

Making Email Retention Work

CHAPTER 1
[E-Discovery Begins With a Retention Policy](#)

CHAPTER 2
[In Search of ... E-records Management Tools](#)

CHAPTER 3
[Don't Forget Facebook](#)

CHAPTER 4
[Making Email Retention Work](#)

State Farm wanted control over its e-discovery process. The answer? Keeping 25 years' worth of documents in production systems fronted by a master management system.

BY LINDA TUCCI

STATE FARM MUTUAL Automobile Insurance Co. takes what many would argue is a counterintuitive approach to electronic discovery. The U.S.'s largest insurer of homes and automobiles keeps anything that might matter: emails, 100% of the email attachments of its claims officers, paper and electronic documents dating back 25 years, even the latest iterations of its human resources Web pages. The voluminous cache, meticulously imaged and coded, is stored centrally in an active system that is searched regularly as

litigation arises.

"For us it is not about cost but more about lowering risk. We have a lot of litigation all over the country," says Tim Crouthamel, section head of litigation support for State Farm's corporate law offices.

But saving basically everything in a centralized platform has also saved millions of dollars for the Bloomington, Ill.-based insurer, as evidenced in the wake of Hurricane Katrina. Crouthamel says the company was midway through the implementation of its centralized live repository when the hurricane hit. To recover data related to the Katrina litigation from just 1% of the hard drives cost State Farm \$30 million. The long-term cost of archiving email for all 30,000 or so claims officers? Something around \$1 million.

"Who knows what it would have been if we had searched everything we preserved, which, knock on wood, we haven't had to do," says Crouthamel, who spoke at this year's LegalTech event in New York.

State Farm is not in the legal business. But litigation sure is a big part of its business. The insurer has approximately 150,000 pending lawsuits. It employs hundreds of law firms, all of

Chapter 4

CHAPTER 1
[E-Discovery Begins With a Retention Policy](#)

CHAPTER 2
[In Search of ... E-records Management Tools](#)

CHAPTER 3
[Don't Forget Facebook](#)

CHAPTER 4
[Making Email Retention Work](#)

which in the past answered litigation requests in their own way from their own collections of documents. After the explosion of bad faith cases in the 1980s and 1990s, State Farm wanted a workflow process that would allow it to respond to cases in a consistent and efficient manner, Crouthamel says. It did not want to have to school each one of its law firms in its data retention policies. With the advent of electronic data discovery laws, the need for a centralized platform became more urgent.

"We knew we have certain kinds of litigation across different departments. We asked what are the documents that we use over and over again," Crouthamel says. Why not "put them up in a platform where we can reuse the documents and the work products in an efficient manner?"

The company installed a dedicated staff at its corporate headquarters that does nothing but e-discovery. It brought the supervision of class action lawsuits in-house, ensuring State Farm speaks in a single voice on legal actions that affect the enterprise. It hauled in the many discrete document collections built up by its field law firms. And then it paired with e-discovery platform vendor CaseCentral Inc. in San Francisco to build a central repository, or master library, of carefully coded documents to populate its hundreds of thousands of lawsuits, minus the duplication and inconsistency common to the paper world.

This aggressively proactive process is not just about managing the past or materials requested in litigation. Any new document that could conceivably be requested in a legal hold is put into

"For us it is not about cost but more about lowering risk. We have a lot of litigation all over the country."

—TIM CROUTHAMEL, section head of litigation support, State Farm Mutual Automobile Insurance Co.

the repository by State Farm's cadre of "gatekeeper" paralegals, ready if necessary to populate the company's many lawsuits.

"We're trying to take the duty-to-preserve issue off the table," says Crouthamel, who refers to the company's re-engineering of its document management as "optimizing our e-discovery supply chain."

"It's kind of hard for the government to make a conspiracy argument against you when you have all the email and attachments of the people they are talking about as targets sitting there and ready to look at," Crouthamel says.

The insurer's disciplined process

elicits something approaching awe from other lawyers.

"I think State Farm, more than any other corporation I have seen, gets long-term enterprise evidence management better than any other firm I have talked to," says John Woods, a Washington-based partner at Hunton & Williams LLP, who advises companies on internal investigations, business crimes and complex civil litigation.

But Woods, who participated on the LegalTech panel with Crouthamel and does not do legal work for State Farm, says companies with more typical litigation exposure might well find this approach a tough sell in hard times.

"You have made a philosophical choice that you are basically going to save everything, but your volume of litigation is atypical and probably your risk is atypical," Woods told Crouthamel at the event.

The main message for companies, Woods says, is that whatever electronic data discovery process they implement should be easily explainable to outside counsel required to sign off on the process.

"I know a lot of companies very focused on saving only what needs to be saved," Woods says. "The tension point is that you can do whatever you want, but I [in the role of outside counsel] am going to ask some questions about how you got there." ■

Linda Tucci is senior news writer for SearchCompliance.com. Write to her at ltucci@techtarget.com.



SearchCompliance.com

**Email Retention:
Standards and Practices**
is produced by CIO Decisions/
IT Strategy Media Group,
© 2009 by TechTarget.

Scot Petersen
Executive Editor

Jacqueline Biscobing
Managing Editor

Linda Koury
Art Director

Alexander B. Howard
Associate Editor

Linda Tucci
Senior News Writer

**John Weathington
Stan Gibson**
Contributing Writers

FOR SALES INQUIRIES
Stephanie Corby
Senior Director of Product Management
scorby@techtarget.com
(781) 657-1589

BUSINESS STAFF
Andrew Briney
Senior Vice President/Group Publisher
Jillian Coffin
Publisher, Sales

CHAPTER 1
[E-Discovery
Begins With a
Retention Policy](#)

CHAPTER 2
[In Search of ...
E-records Man-
agement Tools](#)

CHAPTER 3
[Don't Forget
Facebook](#)

CHAPTER 4
[Making Email
Retention Work](#)

Google™ postini services

- ▶ Learn more about Google Message Discovery
- ▶ Learn how Prince Georges County Public Schools deployed Google Apps and Archiving and saved a million dollars.
- ▶ Watch Harb, Levy & Weiland describe how they use Postini Services to make their email more secure, compliant and productive.



- ▶ "The Information Governance Imperative"
- ▶ "Email Archiving, an Information Governance Imperative"
- ▶ Information Governance Initiatives (records management, paperless administration) Deliver 532% ROI



- ▶ Best Practices for Defining and Establishing Effective Archive Retention Policies
- ▶ Improving Results for the Legal Custody of Information
- ▶ Effective Strategies for Backup, Archiving, and Recovery