Electronic Data Discovery:  
Integrating Due Process into CyberForensic Practice

“As a litigator, I will tell you documents are just the bane of our existence. Never write when you can speak. Never speak when you can wink.”

Introduction

Perhaps the quote above might be adapted to the emerging era of electronic data discovery (EDD) and cyberforensics as follows: proceeded with “Never type when you can write,” interleaved in the middle with “Never speak when you can whisper,” then completed with “Never wink when its understood.” While such communications practices might seem to avert damaging “smoking gun” revelations, they invite court sanctions as discussed in this article. The resulting culture is one of cover-up and risky behavior inconsistent with good public policy. This article reviews the emerging field of EDD under criminal, civil and regulatory process with implications for cyberforensics and sound electronic records management (ERM) practices.

Eventually every company, not-for-profit (NFP), non-governmental organization (NGO), self-regulatory organization (SRO) or government agency is engaged in litigation, many as plaintiff or enforcer, but most as defendant. Complaints are filed by customers, former employees, competitors, shareholders, criminal prosecutors, or by watchdog regulatory agencies such as the Security and Exchange Commission (SEC), Federal Trade Commission (FTC), Internal Revenue Service (IRS) or the U.S. Justice Department (DOJ). It is then nearly always certain that records are subpoenaed

---

demanding business records and correspondence, increasingly including emails related to the disputed issue.

Many people who use email for its efficiency, when compared with telephony or face-to-face (F2F) meetings, run a significant risk: phone call and personal F2F conservation content is evanescent unless wiretapped or recorded. By contrast, email is persistent, increasingly understood to be recorded and preserved by the sender, the recipient and various ISPs during transmission. Many high visibility cases now clearly signal that nearly any electronic record are subject to recovery of meta data and content during the pre-trial discovery phase of criminal and civil litigation as well as regulatory enforcement by government agencies and SROs. Anyone with a legally-enforceable interest, on either (any) side of the litigation, has the right to access and generally to use the content of traditional paper records, as well as electronic communications, to prove facts at issue in legal proceedings. The term, electronic data discovery (EDD) is generally applied to a wide range of electronic document acquisition from opposing or potentially adverse parties, in preparation for civil, criminal and regulatory legal proceedings.

Consider the famous case against Merrill Lynch when it’s star performing security analyst Henry Blodget referred in internal emails to stocks he recommended as “a piece of junk” and “a powder keg.” Such admissions in email reveal conflicts of interest between Merrill Lynch’s underwriting and its investment advisory divisions. Public disclosure by New York Attorney General Elliot Spitzer caused significant damage to Merrill Lynch’s reputation and was a pivotal fact in the $100,000,000 civil fine in the settlement with New York state and the SEC.2

Litigants on both sides may be required to disclose emails and archived internal and external communications (e.g., IM chat, file metadata, network activity logs). Many persons may still incorrectly believe that such communications are “private” or evanescent. The result of EDD can be a roadmap of “who knew what and when,” which is so pivotal in litigation. The costs of electronic records management (ERM) and of responding to mandatory EDD are very significant, including search of email, document files residing on (potentially) every employee’s desktop and laptop hard drives and restoring backup repositories in various locations. Such costs can easily exceed a quarter

of a million dollars in routine litigation. The threat of discovery costs, even before EDD became a predominant focus, was an available mechanism to pressure opposing parties into pre-trial settlements. The penalties for an insufficient response to a discovery request or for document destruction can be severe, such as a spoliation in civil and regulatory investigations and obstruction of justice in criminal cases. Consider that Martha Stewart was sentenced to prison for obstruction of justice and not for insider trading.³

**Defining Electronic Data Discovery (EDD)**

After litigation has commenced with the filing of a complaint and before the trial takes place, there is a (sometimes lengthy) period of trial preparation during which facts are investigated information is requested from all parties and opposing parties must make requested but unprivileged information available to the opposition. Discovery rules in the U.S. require production of the requested information even if this would weaken or compromise the producing party’s (target’s) interests. All litigants, both plaintiffs and defendants, may demand production of documents and “data compilations” relevant to the prosecution, complaint or defense of an issue from nearly any party in possession, custody or control of that information. This document production duty is required in the U.S. federal courts in civil cases under the Federal Civil Rules of Procedure (Fed.R.Civ.P.) or in criminal cases under the Federal Rules of Criminal Procedure (Fed.R.Crim.P.) as well as under similar discovery rules in all the U.S. states.⁴

Fed.R.Civ.P.Rule 34(a) broadly defines the potential sources of discoverable data as “writings, drawings, graphs, charts, photographs, phonorecords,⁵ and other data compilations from which information can be obtained, translated, if necessary, by the respondent through detection devices into reasonably usable form.” Therefore, data compilations may include reports, correspondence, memos, text files, spreadsheets, PowerPoint presentations, digital photos, graphics and art, email including all attachments, instant messages (IM) and any other data created on or stored on a computer, computer network or any other electronic storage media (i.e., detection

---

⁴ FED. R. CIV. P. 26(a) (1).
⁵ Under U.S. copyright law the term “phonorecord” is broadly defined to include analog vinyl and streaming tape recordings as well as digital recordings “fixed” in magnetic and optical media.
 devices).

Pretrial discovery in the U.S. differs from that required in many other industrialized nations because in the U.S. parties may not hide, destroy nor deny the opposing party access to most forms of incriminating evidence by claiming proprietary control. Often one party in litigation is not in possession of the facts or evidence needed to prove the other party’s fault. The formulation of “justice” in the U.S. gives all litigants the right to request and examine records, files, or other evidence from the opposing party if the latter holds exclusive control over such information. With great frequency, pre-trial discovery unearths evidence critical to the requester’s success. Consider the high visibility $253 million jury verdict against Merck, maker of the prescription painkiller Vioxx - a Cox-2 inhibitor.\(^6\) Merck defended by claiming that arrhythmia or irregular heartbeat caused the death and not as the plaintiff alleged, by a blood clot produced by Vioxx. However, the jury was likely influenced greatly when a 1997 email was produced, authored by Merck’s own research scientist Alise Reicin, admitting “the possibility of increased CV (cardio vascular) events is of great concern” sent two years before the FDA approved Vioxx for sale to the public. Vioxx was subsequently withdrawn from the market in September, 2004.

Until the 1990s, discovery requests for the production of documents largely involved paper records. Much of the traditional communication, F2F conversation and phone call content, was evanescent, effectively unavailable unless there were contemporaneous written notes, tape recordings or the conversation was recalled in a witness’ testimony under oath or in a deposition. The probative value of witness recall depends on witness’ credibility as tested by cross-examination and on the strength of rebutting evidence. Today, most business records are electronic and a growing amount of communication among individuals is transmitted through networks in digital form. Therefore, EDD has increasingly become the most important source of evidence in criminal and civil litigation as well as in government regulatory investigations.

According to one recent study on the proliferation of electronic repositories, over

90% of business documents are created and stored electronically.\textsuperscript{7} While the percentage growth of the 1990s is abating now, the quantity will likely continue to grow. Most intra-corporate and intra-governmental communication is conducted via email with a growing use of emerging electronic communications technologies including IM and Blogs. Each email leaves electronic traces that include content, file attachments, metadata, revealing the sender, recipient(s), sequence and timing data. Such information is often highly probative of motive, intent and even culpability of individuals and institutional actions. Persistent electronic records of telephone logs are also often available and will likely increase as voice-over Internet protocol (VoIP) proliferates. Consider the persuasiveness to triers of fact (jury or judge if no jury) such as Martha Stewart’s electronic office diary recording of data such as date, time, sender and subject matter of the messages that were received from her Merrill Lynch broker addressing the “cover story” for her sudden Imclone stock sale the day before announcement of the Food and Drug Administration’s (FDA) rejection of the drug application.

Many other persistent electronic records are useful in proving facts, impeaching witnesses or casting doubt on an opponent’s depiction. These records can include website visits, content downloaded dating back several years, identity and dates of voice mail callers and employee security code use (access cards to physical locations, log data of network access, parking facility access), many of which are corroborated by video surveillance tapes. E-ZPass and many other automated toll collection authorities frequently must respond to subpoenas for toll use records identifying customer, registered vehicle, time, date and location for various evidentiary purposes in legal and regulatory matters. Such advances over the past decade in electronic recordkeeping has transformed litigation in the U.S.

\textbf{Electronic Records Subject to Discovery}

Electronic data is subject to discovery or subpoena from targets, that is, anyone possessing information potentially relevant to issues, subject matter and participants in an investigation or litigation. Innovation in technology continues to expand the types of

electronic data discoverable. Consider how voicemail is shifting from individual desktop
recorders to networked digital storage. Unless effectively purged, voicemail may become
as permanent and accessible as is email today resulting in much more revealing voicemail
discovery. This architecture holds the promise for unpleasant surprise because currently
voicemail is most often preserved only by the recipient, not the sender. Indeed, it is
unlikely senders can produce voicemails if sought in discovery making employers of
most senders ignorant of the precise voicemail content and ignorant of the general
content of renegade employees. It is costly to identify all potential voicemail recipients
and request recipient recordings. Voicemail search technologies are still developing and
are neither as sophisticated nor as ubiquitous as are text search methods for email search
of keywords in key fields such as sender, recipient(s), time, date, routing, attachments
and subject matter.

Many potentially-discoverable messages are archived on internal backup media,
by third party service providers, at ISPs (e.g., Hotmail, Yahoo, AOL), on personal digital
assistants (PDA) and Blackberry devices, on cell phones, on personal laptop and home
computers and in various personal storage media (e.g., floppies, portable hard drives,
thumb/jump/USB flash drives). External archives and caches of Internet content are often
useful to retrieve the content of web sites and web pages previously posted but later
“taken down” and such Internet archives are often admissible evidence in the proof of
infringement, internet domain name misuse, defamation, trade libel, harassment,
misrepresentation, fraud.⁸ Litigators now refer to “doing a Wayback,” to inform pre-trial
strategy, essentially a search of archive(s) of (most) all websites for a potential
adversary’s prior Internet postings.

It is important to note that pre-trial discovery rules permit that requests may be
made from targets in possession of potentially relevant records even if they are not (yet)
parties to the litigation. Discovery is mandatory from opposing parties and from most
employees. With some limited exceptions for privileged communications, such as the
attorney-client privilege and the attorney work product privilege, documents are
discoverable from almost any opposing party or third party source. Depending on the

⁸ The Internet Archive claims that its Wayback Machine contains “approximately 1 petabyte of data and is
currently growing at a rate of 20 terabytes per month.” See http://www.archive.org/
situation, there are other important, but typically narrowly construed privileges, such as the spousal privilege, the doctor-patient privilege, the priest-penitent privilege, and in much more limited situations the accountant-client privilege and the self-evaluation privilege. Even when unprivileged information is obtained in discovery, its use and publicity may be restricted by various types of confidentiality, such as court records held under seal by a judge’s order for trade secrets or national security matters. Increasingly, confidentiality requirements or secrecy orders may suppress disclosure of divorce records and information about juveniles and minors. Unless specific public policies like the privileges discussed above are applicable, there is no general right to privacy in the U.S. that prevents discovery of incriminating information or other evidence damaging to a party’s interest.9

Metadata is another important source for EDD of which many business executives and government leaders are still unaware. Metadata is literally “data about data” it accompanies data file communications or is susceptible to association from various sources. A “metadata tag” may indicate various items of description including: file creation date, computer on which it was created, the IP address from which it was accessed, dates of editing or simply last viewed/opened and by whom and deletion. Email metadata may also include the sender’s address book information, dispatch and receipt date of messages, information about forwarding or replies, and the existence or content of attachments. Metadata can be very useful. For example, in the Martha Stewart obstruction of justice case, an erased and later restored electronic record of a phone call discovered on office computers was argued, when correlated with an electronic diary entry showing a meeting with her broker, to prove the development of a “cover story” for the motivation to sell the Imclone stock. Despite reports that Ms. Stewart had second thoughts almost immediately and allegedly reentered the erased phone call log herself, metadata supported the obstruction of justice charge by evidence of tampering. Additional forms of metadata are in use and are still developing as the architecture of communications methods evolve. The recording and association of IP address with

---

9 In the high visibility antitrust case against Microsoft, an email by Bill Gates sent to someone outside Microsoft concerning the competitive objective of bundling Internet Explorer within Windows was held not to be protected by Mr. Gates’ personal right to privacy and was proof admitted as relevant to Mr. Gates’ state of mind.
particular site visits and the potential for court orders to require disclosure of such metadata by ISPs substantially limits the anonymity of web communications and transactions. Such methods are in widening use by law enforcement to identify offerors and users of child pornography on the web or to identify both those serving and those downloading content using peer-to-peer (P2P) networks.

“Litigation Hold” Compliance

All persons, businesses, institutions and government agencies have a legal duty to preserve records relevant to both reasonably expected investigations and to litigation. When litigation becomes “reasonably expected” a “litigation hold” must be issued immediately throughout the organization that preserves all potentially-relevant evidence. Delays of only a few days in implementing the litigation hold might permit the overwriting and permanent loss of files archived on back-up media concerning email responsive to the discovery request. For example, organizations should have ERM programs including document retention and destruction policies depending on various factors such as time, date, subject matter of file, internal needs, etc. Consider the landmark EDD cases of Zubulake v. UBS-Warburg\(^\text{10}\) in which the employer was ordered to pay $29.3 million for sexual harassment. The female stock broker made civil discovery requests for internal emails sent by her alleged harasser that were expected to prove the alleged harassment. The judge described the litigation hold process for electronic evidence and email as follows:

> Once a party reasonably anticipates litigation, it must suspend its routine document retention/destruction policy and put in place a “litigation hold” to

ensure the preservation of relevant documents. As a general rule, that litigation hold does not apply to inaccessible backup tapes (e.g., those typically maintained solely for the purpose of disaster recovery), which may continue to be recycled on the schedule set forth in the company's policy. On the other hand, if backup tapes are accessible (i.e., actively used for information retrieval), then such tapes would likely be subject to the litigation hold.

However, it does make sense to create one exception to this general rule. If a company can identify where particular employee documents are stored on backup tapes, then the tapes storing the documents of “key players” to the existing or threatened litigation should be preserved if the information contained on those tapes is not otherwise available. This exception applies to all backup tapes.11

When about to initiate litigation, opposing party’s counsel may send a “preservation demand” demanding preservation of backup email files potentially relevant to a threatened lawsuit. Once pre-trial discovery begins, interrogatories are a useful tool to identify the existence and location of electronic records and potential witnesses. These are written questions demanding the opposing party’s answers under oath.

Once a litigation hold must be issued there are numerous and significant legal consequences. Legal counsel must immediately notify the information technology personnel to immediately discontinue document destruction. It is advisable to request the IT department to explicitly acknowledge the litigation hold. Document destruction must cease and initiate preservation efforts for relevant emails, electronic documents and records, and backups. A written preservation plan with procedures should be devised that designates specific electronic evidence and emails for preservation and then the plan should be distributed to all employees potentially in control or possession of relevant evidence. Outside or independent directors of corporations should also be instructed to preserve relevant documents and records.12 Reasons should be stated for the litigation hold such as potential future litigation or regulatory enforcement actions, filed lawsuits or complaints, preservation letter, or a court order requiring the preservations of records. The notice should also warn of serious sanctions for failure to comply.

Large organizations that are regularly engaged in litigation should have teams already organized to quickly and effectively implement a litigation hold including experienced members from IT, legal, human resources (HR), and other in-house and third party records management professionals. Litigation hold compliance should be actively monitored. Experienced electronic, computer and cyber-forensics experts are often needed to preserve evidence. Files found or recovered should be authenticated and preserved to establish the “chain of custody” and avoid inadvertent spoliation. For example, a review of files from desktop, laptop and handheld computers of the key employees likely involved should help determine whose emails, files or Internet activity is potentially relevant. Unopened copies are useful for later review by supervisors or internal investigators to preserve metadata preceding the litigation hold date. There is vulnerability to claims of subsequent electronic evidence alteration unless “snap shot” images are made to preserve a complete mirror-image record of the content and files when the litigation hold is implemented. Electronic forensics experts, often third party service providers, employ procedures and software that can authenticate the chain of custody and thereby refute charges of alteration or destruction post-litigation hold date. Backup media must be preserved to avoid charges of post-litigation hold date tampering.

**Allocating EDD Costs**

Many observers of U.S. litigation argue that pre-trial discovery is too costly and can be intentionally deployed to intimidate defendants into unjust settlements. Indeed, numerous proposed and achieved reforms of product liability, tort liability and securities litigation focus on halting discovery with a litigation “stay” to enable early dismissal of abusive litigation precisely because of the nuisance costs of discovery.13 Judges have long had the power to consider the oppressive costs of discovery. The basic discovery rule in federal civil litigation, Fed.R.Civ.P. 26(c)14 grants discovery targets a right to seek protective orders limiting the scope of discovery if the request is overly broad, seeks privileged information or would result in “annoyance, embarrassment, oppression, or undue burden or expense.”

---

Back when paper records were predominant, discovery targets were typically required to bare the costs of locating, screening for relevance, assembling and copying requested records. Today, the much larger volume of electronic records, when exacerbated by conversion costs from backup storage formats, increasingly prompt judges to shift some of these EDD costs to the requesting party. The Zubulake decisions delineate five categories of increasing recovery difficulty and expense that are currently relevant to determining EDD cost sharing:

1) **Active** online data on hard drives or active network servers;
2) **Near-line** data on removable media (e.g., CD-Roms, floppy disks, magnetic tapes);
3) **Off-line** storage or archived data of organized files on off-line removable media;
4) **Backup** tapes organized not for convenient retrieval but for disaster recovery, produced in time sequence (network throughput backups made daily, weekly, monthly) and therefore intended primarily for massive re-image restoration:
5) **Deleted**, fragmented data files recoverable only by forensic experts.

Active data files, generally found in categories one through three above are accessible with the least costly restoration so discovery targets would usually be expected to bear the costs of production. Archived, compressed and hidden data recovery is more expensive and in the extreme may require the specialized services of outside forensic experts to de-compress, restore, read and organize such files. In such cases, judges are becoming more sympathetic to cost sharing by the requester and target. Sometimes it may be appropriate to sample the requested data recovery to predict the effort and costs of the data recovery project before cost sharing is ordered. Such cost balancing is authorized by Fed.R.Civ.P. 26(b)\(^{15}\) authorizing judges to weigh the potential relevance of requested documents against the burden on the target. The likely benefit of discovery is evaluated against the litigation stakes, the parties’ resources and the likely relevance of the proposed discovery to resolving the issues.

The facts of the Zubulake case are illustrative. SEC rules require broker/dealers like UBS Warburg to preserve all external emails sent to customers for three years, which UBS stored on optical disks making them relatively easier to search. UBS was ordered to

assume 100% of those search and production costs. By contrast, proof for a gender
discrimination claim would likely require production of internal emails. These were
preserved by UBS only on network backup tapes and existed in various file formats.
UBS argued for cost shifting because there were potentially 94 different network backup
tapes needed to comply with the discovery request. Instead, the Zubulake court ordered
sampling of 5 of the 94 backup tapes selected by Ms. Zubulake as most likely to contain
relevant emails and UBS’s outside forensic expert billed nearly $12,000 for producing
600 potentially relevant emails. The judge found 68 of the 600 emails had potential
relevance. Generalizing from the sample, UBS was ordered to pay 75% of the total
$165,000 estimate for internal email restoration and 100% of the attorney’s fees for
reviewing and transmitting the relevant documents, estimated at over $100,000.16 The
scale of EDD restoration and recovery costs illustrated in Zubulake are not atypical.
Indeed, the $300,000 restoration and search cost in Zubulake is not unusual for a larger
organization raising legitimate concerns that threatened discovery continues to unfairly
force settlement. Some cases are limiting backup restoration for this reason. Consider the
“fishing expedition” concerns of Federal Magistrate John Facciola when he declined to
order a full backup in the case of McPeek v. Ashcroft:

If the likelihood of finding something was the only criterion, there is a risk
someone will have to spend hundreds of thousands of dollars to produce a single
email. This is an awfully expensive needle to justify searching a haystack. . . . .
Ordering the producing party to restore backup tapes upon a (automatic
assumption) likelihood that they will contain relevant information in every case
gives the plaintiff a gigantic club with which to beat his opponent into settlement.
No corporate president in her right mind would fail to settle a lawsuit for
$100,000 if the restoration of backup tapes would cost $300,000.17

The privately developed Sedona Principles advocate more equitable cost sharing and hold
some promise to influence judges’ allocation of these burdens.18

Avoiding Consequences of Evidence Destruction

http://www.thesedonaconference.org/dltForm?did=TSG9_05.pdf
Parties always have a disincentive to produce documents that are incriminating or reveal proprietary information or strategy. Litigation process rules have long penalized the intentional destruction of evidence. Spoliation is the improper destruction of documents, including email, of potential relevance to a pending or forthcoming legal proceeding. The potential sanctions for spoliation vary, depending on the spoliator’s degree of fault, that either punish the spoliator and/or give justice to the requesting party. This degree of fault varies with the spoliator’s “culpable state of mind” - that there was a knowing destruction of evidence relevant to the opposing party’s claim or defense. In spoliation cases the courts balance the degree of fault against the degree of prejudice caused to the requesting party. Sanctions may include:

1. Discovery sanctions (monetary fines);
2. Attorneys fees and costs payments to the requesting party for spoliation hearings;
3. Additional discovery with the costs charged to the culpable party;
4. Adverse inference instructions to the jury – permits the jury to infer that the spoliation destroyed evidence favorable to the opposition’s case and harmful to the spoliator’s case;
5. Default judgment on a defendant (liable) or dismissal of a plaintiff’s case (an extreme remedy);
6. Tort (civil) liability for injuries due to the spoliation.

**Role of Document Retention and Destruction Programs**

Document management and document retention components of ERM programs involve pragmatic procedures to periodically destroy documents and records. There are justifications beyond the obvious self-serving effort to eliminate “smoking guns.” For example, the costs of storage, management and discovery response are well-known. When information is no longer useful or necessary for business purposes and no federal or state law requires its retention, there is strong incentive to accept the business reasons for destruction. Courts accept the balancing of retention/management costs and the needs for justice if the policies are applied consistently and without a sole purpose to thwart opposing parties in litigation. The key standard is whether the potential discovery target could reasonably anticipate such documents could be relevant to a likely or pending
government investigation or litigation.

Furthermore there must be clear proof that the document destruction program or its execution is implemented with intent to destroy evidence. Consider the recent U.S. Supreme Court reversal of a conviction involving Enron-related document destruction. The 2002 Arthur Andersen criminal conviction was overturned because the trial judge’s instructions to the jury were flawed, leaving this intent element unclear. An in-house Arthur Andersen lawyer’s email reminded staff to faithfully execute “document-retention” policies on their Enron audit papers and this allegedly triggered a extraordinary shredding of Enron audit documents just when, DOJ argued, Andersen could “reasonably anticipate” the forthcoming SEC investigation. This Arthur Andersen criminal conviction was arguably the direct cause of Arthur Andersen’s collapse as clients defected. Thus, a simple reminder of document retention program procedures is not wrongful, in itself and without further proof of a conscious wrongdoing. Such wrongdoing would require contemplation of a particular official proceeding in which the destroyed documents might be material.

**Document Retention Constraints**

Legal requirements for document retention generally depend on three factors: (1) line of business, (2) type of records in question and (3) significance of archived information to the business model. Government regulations from various sources, federal, state, local even international regulations may require creation and maintenance of various business records. Some retention requirements apply to most businesses, such as tax records under IRS rules, wage and hour records under the Fair Labor Standards Act, cradle to grave toxic chemical handling under the Resource Conservation and Recovery Act (RCRA) or employee exposure records under regulations of the Occupational Safety and Health Administration (OSHA). Other requirements are specific to regulated-industries such as for railroads, airlines, public utilities, nuclear power plants, federally-chartered or insured banks, securities broker/dealers, commodities future commission merchants or registered investment advisers. The Code of Federal Regulations (CFR) contains over 2,800 sections requiring record creation and/or maintenance. Retention

---

periods range from 30 days up to 50 years. Few federal agencies have email retention rules yet, the SEC is at the forefront with rule SEC Exchange Act Rule 17a-4(f) requiring retention for three years of all correspondence with customers generally and specifically this includes emails.\(^{20}\) Retained copies must be in a “non-rewriteable and non-erasable” format that the SEC describes as follows:

Under the rule, the electronic storage media also must verify automatically the quality and accuracy of the storage media recording process; serialize the original and, if applicable, duplicate units of storage media, and time-date for the required period of retention the information placed on such electronic storage media; and have the capacity to readily download indexes and records preserved on the electronic storage media to any medium acceptable under paragraph (f) as required by the Commission or the self-regulatory organizations of which the member, broker, or dealer is a member.\(^{21}\)

Despite the SEC’s detailed email retention requirements, such regimes at other federal and state agencies remain generally less detailed and frequently are unclear. Most retention laws are adapted to electronic communications rather than stated in language that is clearly and unequivocally applicable to electronic communications. Indeed, Donald S. Skupsky, a leading author in document retention argues that existing federal records retention requirements may not clearly apply to emails.\(^{22}\)

### Perils of Aggressive Document Destruction

It is widely reported that many organizations deploy aggressive email document destruction policies – erasure after short time frames of 30 to 60 days, possibly under the tacit reasoning that smoking gun emails are eliminated by routinely-applied document management policies and that such policies greatly reduce the probability of damaging discovery. Some document retention experts argue that most email is intentionally private and informal conversation deserving of treatment similar to F2F or phone conversations. This obviates the need to memorialize all email in the same way that recording devices

---

\(^{20}\) 17 CFR 240.17a-4(f).
still do not generally apply to all phone calls or F2F “water cooler” chats. Such a position might justify the physical separation of email backups from more official, “permanent” records. However, giving senders or recipients an option to archive or to effectively eliminate conversations clearly showing criminal intent or conspiracy will likely seem unacceptable to many policy makers.

Official policies of aggressive email destruction could also risk spoliation or obstruction liabilities. Consider the SEC’s discipline and civil fines against Deutsche Bank, Morgan Stanley, Goldman Sachs, U.S. Bancorp and Salomon Smith Barney in 2002 for their alleged systematic destruction of network email backups and departed employees’ hard drives.23 Second, the Sarbanes-Oxley Act (SOX),24 the SEC rules issued thereunder and the attendant internal control accounting standards issued by the Public Company Accounting Oversight Board (PCAOB)25 can be arguably interpreted to prohibit aggressive email destruction, at least for publicly-traded companies. Aggressive destruction arguably violates the SOX duties to maintain adequate internal controls. Further, employee customs and institutional practices regarding email often preserve copies in multiple locations, on employee hard drives and in electronic and paper printouts. Therefore, aggressive destruction policies may effectively eliminate only the organization’s primary copy of potentially incriminating messages, leaving untouched the persistent, secondary archives preserved by employees, service providers, suppliers, customers, online and Internet service providers. All too frequently such copies are held in less-friendly hands. A generally concerted effort among organizations would be needed to moiré effectively destroy email or lobby for shorter mandatory document destruction deadlines. Given the anticipatory defensiveness of such email elimination program, it must be expected that evasion and circumvention will frequently occur as copies are surreptitiously retained for individual defense and whistleblowing or retention is inspired by retaliatory motives in support opposing parties or perceived victims.

Document destruction practices now increasingly include deletion of electronic file metadata; “wiping” programs may erase automatically-generated metadata on files,

communications and Internet browsing history. Consider how commercially available applications such as *Metadata Assistant* by Payne Consulting\(^{26}\) a tool that removes metadata such as a document’s author(s), various dates of file creation, printing or access and edits. Such tools are also useful to examine files submitted by opposing parties. Metadata wiping is prohibited following a litigation hold. Care must be taken because metadata can be falsified or surreptitiously supplied after wiping.

**Discovery Negotiations**

Courts are sensitive to limiting overly-broad and costly discovery requests. However, litigation to narrow the requester’s scope or the target’s responsiveness to pre-trial discovery can be costly. For example, much of the *Zubulake* litigation involved extensive motion practice, frequent court appearances, significant fees for lawyers and forensic experts and can risk adverse publicity. It is often advisable, at the outset of litigation or regulatory investigations to negotiate scope limitations on discovery - the subject matter, time window, electronic formats and production timetables. Many seasoned litigators can be willing to negotiate discovery with experienced and reputable counsel and forthright clients. Another area for negotiation can be the search criteria, keywords, search strings, concept searching and other screening criteria relevant to the litigation. Non-responsive production is all too frequently met with subsequent demands or court sanctions for failure to respond.

**Some Concluding EDD Observations**

Despite incremental litigation reforms, there is no clear signal that aggressive EDD will abate anytime soon. Instead, the public receives a steady stream of revelations of wrongdoing exposed increasingly through EDD. The strength of an organizations’ “ethical culture” is a fundamental issue in EDD and significantly impacts employee morale and the organization’s long-term survival and prosperity. Organizations resistant to electronic evidence accessibility might favor more frequent email destruction under a presumption that there are things to actively hide. Such a position risks a culture that communicates to employees a tolerance for unethical, irresponsible and illegal acts. By contrast, an organization that is able to make evidence accessibile, projects an opposite

\(^{26}\) [http://www.payneconsulting.com/](http://www.payneconsulting.com/)
culture of intolerance towards illegal and unethical activity. The proven ability to take corrective action both disciplines employees and impresses regulators and judges. This approach might be implemented with routine preservation of all emails and general backup in readily-accessible, well-organized and well-indexed central archives. While Zubulake shifts the cost burden to the target for deploying, maintaining and using ERM for discovery requests, there are clear advantages to ERM under SOX, SEC/NASD rules and in the eyes of prosecutors and judges.

Legacy paper systems imposed considerable document storage costs as well as discovery search and production costs. By contrast, the costs of electronic storage continue to drop precipitously. New archiving, recovery and search technologies from various respectable third party EDD firms simplify and reduce EDD costs after litigation starts. The lessons of recent EDD penalty cases discussed earlier is that reliance on emergency backup does not much reduce the probability of a costly smoking gun emerging, but instead adds significant expense to EDD targets while also increasing spoliation and obstruction risks.

In summary, EDD uncovers formerly private electronic communications of nearly all types frequently relevant to civil, criminal, regulatory or non-judicial (internal) investigations. EDD appears as a gold mine to opposing parties while a trap for secretive obstructionists. The law is keeping pace with many technological developments and EDD is transforming modern litigation practice. Landmark cases such as Zubulake and closely regulated business sectors such as financial services are setting the models for EDD that are likely to become pervasive in other industries and perhaps even in some other nations.