DEALING WITH DATA

No, you can't call them documents anymore

By George L. Paul and Robert F. Copple

We are awash in electronic information. It is smeared across our technology systems. Managing this morass is one of the most serious problems facing business today. Companies, large and small, often don't appreciate the ramifications until it is too late, and they are at risk of serious legal liability. At that point, trying to fix the problem can be very expensive. It is often unsuccessful.

During the ancient days before computers and networks became the predominant business paradigm, most information was kept in the form of laboriously typed paper documents that were neatly filed and, at the end of their life cycle, either thrown in the trash or filed away in document storage facilities. We have, ourselves, searched for old documents in places such as an abandoned Colorado mineshaft (hazardous waste suits required); a forgotten storage building in the Puerto Rican jungle (mosquito netting required); and the garages of long-retired engineers (great patience required).

Because paper document preparation and storage were both burdensome and expensive, there was a natural limitation on the volume of documents produced and subsequently preserved. But computers and electronic data storage have changed all that. Electronic document generation and storage is simple and cheap. The digital equivalent of a warehouse full

of paper can now be stored on a server no bigger than the average computer. Encyclopedias can exist on a thin piece of plastic. As a result, rather than cull old files before storage, it is much easier just to save *everything*.

So, this is a good thing, right? Not really. Proper data life-cycle management requires thoughtful procedures governing what data to keep, what data to discard, when to discard it, and, very important, how to control what is left.

First, there is a growing collection of federal and state laws, as well as international rules, that require companies to preserve specific data for prescribed periods of time. For example, Sarbanes-Oxley, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Internal Revenue Code and certain SEC rules all establish data retention and reporting requirements. The federal courts, of course, are now imposing strict penalties of their own for spoliation of electronically stored information.

The European Union Privacy Directives establish stringent policies governing the collection, storage and use of personal information that apply to forays into international commerce, particularly if European workers are involved. Such rules vary by industry and jurisdiction. But failure to abide by the regulations can subject companies to fines, penalties, and the forfeiture of the privilege of doing business.

So the answer is simple: Just save everything? Wrong. If a business saves all of its electronic data, whether required to or not, the company will literally drown in its digital waste. The data that is important becomes less

accessible because it is lumped in with useless data. And if litigation occurs, electronic discovery is guaranteed to be debilitatingly expensive as there will be huge and unnecessary quantities of useless data to search, and to review for privilege.

We have seen many examples where the failure to properly save or properly dispose of electronic data either saved the ship, or sank it. Arthur Andersen and Enron went down, at least in part, because they illegally attempted to destroy documents after litigation was on the horizon.

But with thought and planning, businesses can create data life-cycle policies that will minimize the exposure associated with either saving too much or too little of the company's data; or more important, of losing control of what is there. An electronic data life-cycle policy can be built around several basic principles:

Identify the objectives of the enterprise — First, it is critical that each company self-consciously devise "objectives" in maintaining its electronic records. This function has become more important now than ever, since it is easier to treat all records the same — just save everything, and let everything go unprotected on the "network."

But depending on the business, different types of records have vastly different degrees of importance. Universities treat their academic records as sacrosanct, whereas payments for lawn care might be much lower on the scale. Companies hired to keep track of individuals crossing national borders might have strict record-keeping priorities for certain databases, but not others.

Information categories are simply

Paul is a partner and Copple is of counsel at Lewis and Roca, LLP, in Phoenix. Paul's e-mail is gpaul@lrlaw.com. Copple's is rcopple@lrlaw.com.

Tom Gianni

not the same. Importance and function vary by orders of magnitude in any enterprise. Accordingly, the first job is to prioritize. What is critical for the business? Devise data life-cycle management with such critical records in mind.

Practice minimalism — Data should be discarded unless there is a good business or legal reason to retain it. Implementation of this principle requires that a company, once again, take a hard look both at the types of data it collects and the regulatory constraints relating to that data. Under what is now known as the *Zubulake* standard of the federal courts, data should be preserved if it is potentially relevant to any foreseeable litigation.

The overall goal is to achieve business objectives and comply with the law, and to discard data that is not required by law, or not required for business purposes. Given the fact that digital files can be copied *ad infinitum* onto different media, unless one controls access to data during the time it is stored by a business, one loses control over the ability to discard information. Maintaining such control is no easy task. Achieving it puts one on the forefront of the business process.

Demand information security — Perhaps no practice can enhance data life-cycle management better than appropriate "information security" procedures. A primer on information security is beyond the scope of this article. But how else can one ensure that shared records are not improperly accessed or edited? How else can a company keep its valuable information from being stolen, for example, or sold to spammers?

Given that such a theft incident may now trigger notice obligations, and perhaps liability — not to mention theft of valuable IP — information security reigns supreme. It is fundamental to protecting the assets of the enterprise.

Develop a records authenticity system — Give thought to how one might prove the authenticity of one's own records if they are ever challenged in court, an administrative proceeding,

or an audit. This suggests the need for proactive procedures. Authenticity, which has been stretched to the breaking point by the new information paradigm, should no longer be taken for granted.

Again, devising authenticity protocols is not amenable to shortcuts or quick fixes. One way to accomplish the task is to rely on the "logging" of network events and file access far more stringently than is currently the norm.

Another solution is to make robust use of "digital signatures," a form of encryption technology that allows an easy test of whether a digital file has been changed through time. Thus, when using a digital signature, a corporation would be able to prove that

PRACTICE MINIMALISM.

a file had not been changed since the event in question, whether it be the entry into a financial journal or worksheet, or the entry of grades for a student onto an academic records database. The bottom line is to design business processes that allow one, ultimately, to come into court to prove that business records are what they purport to be.

Require distribution controls — The interactive ease of networks, including that network of networks the Internet, means that once access to specific data is acquired, the data can be transmitted to countless destinations in a matter of seconds. Every day there are new examples of this phenomenon.

It can involve the public release of valuable intellectual property, such as

the case of the Swedish man who released highly confidential DVD source code to the Internet. Or, it can involve the dissemination of personal and private matters, such as the apparently unauthorized released of Paris Hilton's "homemade movie." Or, it can be just a silly and destructive e-mail that gets read by many in a few seconds.

At least when it comes to business data, unauthorized access can largely be eliminated by appropriate information security. Within an enterprise, in addition, different users or classes of users can have differing levels of access to defined classes of data.

A different problem, however, arises regarding the distribution of data by persons who have legitimate access. Whether the situation involves complex project files shared by a team of engineers or a simple e-mail communication, uncontrolled electronic replication can be a disaster. One solution is to use available software that encrypts the data and allows the sender to specify the degree of republication rights granted to the recipient. Sophisticated companies are beginning to use these types of solutions as part of their overall data management strategy.

The technology is somewhat similar to that restricting the republication of copyrighted works. An Apple iPod, for example, can have music "downloaded" onto it from a computer, but can not "upload" music, because the designers of the product wanted to build in asymmetrical "distribution controls." Companies similarly can control the distribution of data — if they think about the issue.

Prepare for retrievability — One of the major problems with electronic record keeping is that when a request for information does come — for example in discovery in litigation — it can be a six- to seven-figure chore just finding the data that formerly could easily be retrieved from a set of file cabinets.

Accordingly, advance planning is now required to facilitate future retrievability of data. Law firms,

strange to say, are somewhat in the vanguard of businesses in this respect. Their handling of huge numbers of different types of electronic files for many different customers has led to database management tools that facilitate filing by subject matter, with indexing, and methodical retrievability. This "subject matter centered" database control of data has yet to permeate the mainstream of business data storage, which is currently mostly haphazard.

Businesses, therefore, must attack a mounting data retrievability issue. Consider various vendors who sell an enterprise-wide database that allows one to mark a record by subject matter; to control access by identity or class of user; to flag documents as attorney/client privileged; or to control the distribution of data. This issue is so new, however, that off-the-shelf solutions are not readily available in great quantity. Businesses will need to put innovation to work to design solutions that perform database management functions.

Build in "auditability" — The idea behind the Public Company Accounting Oversight Board's new Auditing Standard No. 2 is "internal control" over information. Public companies, obviously, will need to pass audits of their financial statements. Their management of information will need to pass the tests auditors devise to gauge financial data as represented in electronic records, from the transaction level on up to the income statement and balance sheet.

Unless the data life-cycle management system can pass an audit, a company is put in an unfortunate situation indeed. Accordingly, a sound data life-cycle management plan is at the same time a Sarbanes-Oxley compliance program.

This concept of "auditability" is yet another reason that companies should seriously consider both the use of "digital signatures" and the robust logging of network and file access events to provide a test for the information flowing throughout their data system. How else can the auditors know that

the information they are reviewing was not edited — the night before the audit?

Implement training and simple procedures — Of course, for everyone, a data life-cycle policy must be simple and easy to implement. As with all things corporate, there is a strong tendency for policy initiatives to become increasingly intricate to the point of dysfunction (only interpretable by those with graduate degrees in operations research). Once the policy becomes too complex, it is likely that employees will ignore it.

For example, during the beginning of the Internet boom, the National Security Agency created complex internal rules for the transfer of sensitive data from one NSA employee to another. Rather than comply with the rules governing NSA's secured systems, employees discovered it was easier to simply send data to each other through the Internet as e-mail, thus defeating the policy.

Therefore, any policy should strive for simplicity by establishing a limited number of broad subject matter categories and functions. While simplicity might result in some over-inclusion of data retained, it nevertheless increases the chances that employees will actually comply with the policy.

Require consistency and internal enforcement — Data retention practices must be consistent. Inconsistent document retention actions will create a taint of intentional spoliation and wrongdoing. It is hard to explain why you discarded data following your three-year-old policy for the first time, just three days before being served with that antitrust complaint. Therefore, if you have a data-retention policy, make sure it is implemented consistently. If there are dates or milestones for data review and disposal, they must be followed.

Also, enforcement must be simple and consistent. The policy should use both automated systems to dispose of unnecessary data and procedures to motivate employees to appropriately deal with the rest of the data that

cannot be picked up through automated systems. So, for example, unnecessary e-mail accumulation can be limited either by strictly controlling the size of employee mailboxes, thus forcing employees to delete old e-mails in order to receive new ones, or by automated systems that automatically dispose of old e-mails after a set period of time (such as 30 days), unless there is conscious action to override the deletion default.

The term "document retention" is now a profound misnomer. Businesses now deal with ever-flowing electronic records — shared by users on multi-layered networks. Such records are accessed, edited and transmitted with applications that defy a full understanding by their users. The data is then saved in a myriad of media that challenge accountability. As a result of such dynamics, a new complexity in the business world has emerged.

The sudden evolution of such an "information ecosystem" poses fundamental questions: Can we still control information, so as to comply with law and business strategies? How do we know who is changing which records? What is authentic? How is an electronic record "private?" How can we "audit" the information in our enterprise if we can't find out when it was created?

Clearly, a new approach must evolve. Businesses should remember that:

● Electronic information exhibits complex behavior that was absent in the age of documents. We now deal with something akin to an ecosystem.

● Data management is *not* just the domain of the IS department. It is the combined concern of the CEO, general counsel, CFO, outside counsel and auditors with expertise in the field. Strategy requires teamwork.

● There can be severe penalties for destruction of the wrong kind or class of information. Yet, with appropriate data management, electronic discovery in litigation is facilitated, as well as reduced in cost.

● With appropriate data management, proof of the authenticity of one's own records is easier.

● There are rapidly emerging rules that deal not only with *retention* of data, but with its *access* and required *destruction*. Such rules co-exist with retention, thus necessitating a "life cycle" concept for data.

Data life-cycle management is a dynamic concept that has and will continue to evolve with, and probably somewhat behind, technical and computing developments. Therefore, establishing data life-cycle management policies is not a one-time process. Implementing and maintaining a system is a small, but necessary, price to pay for continuing to be a player in the marketplace. **blt**