

Records and Information Management Perspectives

Part I: Legislative and Legal Developments

by Lee S. Strickland

Lee S. Strickland, J.D., is visiting professor in the College of Information Studies at the University of Maryland. He can be reached by e-mail at LSTRICKL@deans.umd.edu

Almost two years have passed since homeland security joined our national lexicon and became an issue of primary importance to Americans in general and information professionals in particular as we searched for solutions to meet this new challenge. Meanwhile, business and personal requirements for information continue to expand at a dynamic rate. As information professionals, we are most familiar with the theories and technologies by which information is stored, retrieved, analyzed, disseminated and archived. Yet, legal and policy developments can have an equal impact on information availability. Consider, for example, how information science and technology has created dynamic peer-to-peer information sharing, while legal and policy decisions may substantially limit the ultimate levels of use and benefit. In sum, these concomitant drivers – technology and law – suggest that we take a broad view of the critical information-centric issues facing our society and participate fully in the associated policy debates. This two-part article and three subsequent ones will survey the essential legal and policy issues in the areas of records and information management (RIM), intellectual property, privacy and national security, and, lastly, cybersecurity. We include with each article relevant recommendations as to sources of news and information for additional research and future developments.

The Sarbanes-Oxley Act

If there was one positive development from the Enron debacle, it is the passage of the Sarbanes-Oxley Act that brought major changes to corporate governance and corporate records management rules for publicly traded companies and public

accounting firms. Here, in addition to creating the Public Company Accounting Oversight Board and requiring new levels of corporate responsibility through required accuracy, individualized certification and reporting, the act also establishes significant new records management (RM) law. It does this, in part, by creating a new law, 18 U.S.C. §1520, that requires any accountant who conducts an audit of a publicly traded company to maintain all audit or review working papers for five years from the end of the fiscal period in which the audit or review was concluded. Additional rules in this regard will come from the Securities and Exchange Commission.

The act further establishes new records management law by creating tough new obstruction of justice criminal statutes that apply to any company, agency or individual and that address any form of direct or indirect destruction of records. Specifically, it creates another new criminal provision, 18 U.S.C. §1519, which prohibits (with penalties up to 20 years) any act to knowingly destroy, alter or falsify any document with the intent to impede, obstruct or influence the investigation or proper administration of any matter within the jurisdiction of any department or agency of the United States. It also amends the current obstruction of justice statute, 18 U.S.C. §1512; where previously the focus was corruptly persuading or forcing others, a new subsection (c) was added that addresses those who directly alter, destroy, mutilate or conceal a record with the intent to impair the object's integrity or availability for use in an "official proceeding."

A Frequent Question Is How These Similar Sections Relate. The new §1519 is substantially broader than the original obstruction of justice law

(§1512) available during the Enron and Arthur Anderson prosecutions. First, the new section applies to any matter within the cognizance of the federal government and not simply to “official proceedings.” And second, the new section provides for the lesser intent requirement of “knowingly” – essentially that the activity was a conscious act – whereas the original section has a requirement of “corruptly” – meaning with a “bad or evil purpose.”

Other sections of note in Sarbanes-Oxley provide that attempts will be treated as harshly as actual crimes and that retaliation against informants can bring penalties of up to 10 years in prison. The bottom line, however, is that this new legislation is not the extent of new records management law. The law here will continue to be active and critical – actions that heretofore may have caused difficulties in court will now clearly be criminal and/or result in substantial fine. By way

of just one example, in December of 2002, five brokerage houses – Deutsche Bank, Goldman Sachs, Morgan Stanley, Salomon Smith Barney, and U.S. Bancorp – paid Securities and Exchange Commission (SEC) fines in excess of \$8 million for records management violations. Specifically, the companies had ignored an SEC mandate that all e-mails be retained for three years with the first two years in a system that preserves accessibility and prevents destruction.

What we see today – and tomorrow – is that the SEC and the range of other regulatory bodies are actively promulgating new (or now enforcing old) RM requirements that will demand our attention. What is required is nothing less than a *continuing effort* at mapping an organization’s records control schedule to current and emerging legal mandates.

Electronic Record Keeping Systems

Often referred to as ERKS or electronic records management (ERM) systems, such systems may conceptually be viewed as a composite system of hardware, software and management processes by which electronic records of a certain type (or all types) are created, filed, maintained and ultimately preserved or destroyed. Unfortunately, while simple in concept, many government agencies and many private businesses have failed to keep their records management processes in step with their development of electronic records. In practice, an ERKS system would consist of dedicated electronic storage, approved software for the creation of electronic documents, and necessary management processes that insure that e-documents, as they are created, are properly indexed, marked and filed. Additionally, such a system would also incorporate a series of future-looking rules and practices to insure that

the e-documents created could be accessed over time, notwithstanding the natural degradation of physical media or the antiquation of hardware and software.

What Are the Essential Keys to ERKS Implementation? One essential key is the adoption of a comprehensive taxonomy for organizational records – the rules by which the records of an entity are organized in a logical, functional, predictable manner. The second key is organizational discipline in the creation and storage of records in accordance with the adopted taxonomy – a matter today that can be facilitated by a user interface with existing document creation software. The essence of this key is that any form of document creation includes the identification of necessary records management metadata and the independent, protected storage in accordance with the requisite records management schedule. A final

key is the agreement on media and software standards for preservation – although this issue should never delay the implementation of an ERKS since preservation is not an option but rather a legal mandate. In sum, an effective ERKS does not alter the required flow of information within a business – it serves only, and largely behind the scenes, to preserve records for future use and archival preservation as required by law.

What Are the Difficulties in Implementing ERKS in Government and Private Industry? One is that some organizations have lacked the internal drive to impose the needed organizational discipline – often until disaster strikes. The Federal Bureau of

Investigation (FBI) learned in this regard and has made substantial improvements since the McVeigh debacle. Here, questions were raised about FBI records management when numerous field offices belatedly discovered a total of more than 3,100 pages of records that had failed to be disclosed as required by law to defense lawyers for Oklahoma City bomber Timothy McVeigh. Subsequently, an inspector general’s investigation blamed the missing document debacle on “*antiquated and inefficient computer systems, inattention to information management and inadequate quality control systems.*”

FBI Director Robert Mueller responded by creating a Records Management Division and, with almost 1,000 employees, 22 units and five Senior Executive Service managers, it is the largest division in the FBI’s headquarters in Washington, DC. In doing this, he has testified before a House committee that “*Records management is at the heart of the FBI’s integrity as a law enforcement organization ... [and] ... we must be able to eliminate any doubt about the accuracy, completeness and fairness of our investigations.*” But

Research and Further Information Guide

See www.cov.com/publications/297.PDF for a comprehensive summary of the Sarbanes-Oxley Act by the law firm of Covington & Burling (26 July 2002) and www.cov.com/publications/340.PDF for “New Compliance Obligations Under the Sarbanes-Oxley Act of 2002 and Related SEC Regulations” that identifies in table format the various provisions of the Sarbanes-Oxley Act and SEC rules and regulations adopted under that act.

in doing so, the director has acknowledged that the task will not be easy and that building a new records management system is not a unitary answer – also stating to Congress that “every employee at the FBI” will attend requisite, back-to-basics training that “focuses extensively on proper document production, retrieval and management.”

To implement this vision at the FBI, National Archives and Records Administration (NARA) alumni William Hooton and Michael Miller are leading the FBI’s new Records Management Division with necessary but daunting objectives: first, determine the scope and details of the FBI’s records archives (estimated at more than a billion pages of largely paper-based information); second, convert that material to electronic, retrievable form (for example, scanning extant paper documents and manually tagging as necessary) and, third, build an electronic record-keeping system that agents can use from desktop computers to create and find records relevant to any given case. Their effort is exactly on the mark.

Another difficulty in implementing ERKS in the view of many familiar with the issue is that NARA has been slow to move forward with guidance and to approve agency schedules for electronic systems. In substantial part, the system ground to a halt with the *Public Citizen v. Carlin* litigation over General Record Schedule 20 that allowed for preservation of e-mail by printing out to paper – a process ultimately deemed reasonable by the courts but hardly an aggressive step in the work of electronic records management. But in fairness, the lack of dynamic progress must be attributed in part to resource shortfalls at NARA as well as shortfalls in interest and resources at individual agencies. What is essential to progress is that senior management must uniformly recognize that records and information management is mission – not overhead.

Further information on government-wide progress comes from the June 2002 General Accounting Office (GAO) report entitled “Challenges in Managing and Preserving Electronic Records.” It found that “[t]he only real focus is printing e-records and perhaps less than 10% of the systems have this approach; everything else is at risk.” And NARA does not disagree; it admits that the government’s policies for preserving records remain focused on paper documents and that records management has not kept up with a federal govern-

ment that creates and uses most of its records electronically. According to a July 2002 NARA report, “... a large majority of valuable electronic records never make it to the archival custody ... instead ... records that are essential to the government accumulate in office computers, reside in agency tape libraries and often are lost when systems are replaced or shut down.” All of this and more is contained in that report – a 46-page proposal for redesigning federal records management policy that places the focus on saving the most important e-documents “knowing that we simply don’t have enough resources to deal with all of the records,” according to Lewis Bellardo, U.S. deputy archivist.

Critics of the NARA approach, including the American Library Association and Public Citizen, suggest that the agency is overwhelmed and that the proposals offer little in terms of direct and concrete response to the problems facing government. Individual initiative, whether at federal agencies or private businesses – will be the likely driver for success here in the coming year.

E-Government

An intrinsic element of records management in the government is the role and function of e-government – the fastest growing medium by which records and information are maintained and made available to primary users. And it presents so many questions and so many different answers and approaches. *Is the proper focus “information” or “services” or both? Should e-government have a cost-recovery model? What is the impact of the threat of cybercrime and terrorism? Are government agencies meeting the challenge as well as private enterprise?*

At one level, the chilling anthrax-based terrorist attacks on the U.S. mail of October 2001 caused many to reconsider e-government, including specifically the need for new communications paradigms (such as Web-based) as paper-based communications and traditional government services were substantially impacted. We saw the U.S. Supreme Court, a classic mail and paper-centric business, effectively closed for many weeks as people scrambled for *ad hoc* solutions. We saw similar adverse effects at other businesses dependent on reliable mail service – public utilities, mortgage holders and credit card issuers – and for them there was little in the way of replacement services.

But we saw others, such as Senator Kennedy – who had

Research and Further Information Guide

For the final decision in *Public Citizen v. Carlin*, see 184 F.3d 900 (D.C. Cir. 1999); *cert. denied*, 529 U.S. 1003 (2000). The cited GAO report may be found at www.gao.gov/new.items/d02586.pdf and the NARA report at www.archives.gov/records_management/initiatives/rm_redesign.html. For a case study on one of the most significant current ERM efforts, go to www.nmci-info.usmc.mil/ or the EDS contractor site at www.nmci-ist.com/ and consider the progress made to date on the Navy/Marine Corps Intranet. This effort builds on work by the FDIC with TRIM software and will ultimately serve 400,000 desktop PCs with a unitary repository and integrated records management, data management and workflow services. A prescient observation offered by the Navy CIO in this regard: “*Before ERM technology can be effectively implemented, it is necessary to address the cultural impact of an enterprise ERM solution.*”

It is incumbent upon every information business to plan for redundancy in the delivery of services and communications with critical partners and customers.

not perceived this specific threat but understood the value of e-government and business redundancy – maintain services through a robust, redundant electronic information and communications processing system that prevailed over the U.S. Senate facilities closure. Since that time, in which four workers died from inhalation anthrax and an additional 13 developed various forms of the disease, there has been a slow but steady move to electronic services across the private and government spectrum. It is incumbent upon every information business to plan for redundancy in the delivery of services and communications with critical partners and customers.

But Are the Electronic Solutions Meeting the Requisite Need? The issue generally presented by each of these questions (including the challenge of terrorism) is simply that of performance. In August 2002 the PriceWaterhouseCoopers (PWC) Foundation sponsored a detailed survey by California State University. It concluded that most sites remain hard to navigate and offer little more than the most basic elements of e-government; more specifically, it found that a few are exemplary (the U.S. Patent & Trademark Office is among the best) but that most lack a “*thoughtful information architecture.*” It found that while most offer basic information and documents and elementary services such as employment information, only about half offered such useful items as downloadable forms, fewer still offered interactive forms and databases, and less than 13% offered e-commerce applications. Strikingly, the survey found that almost 90% failed to meet accessibility standards for people with disabilities despite the law in this regard.

To improve performance, agencies are called upon to solve both legal and technical challenges. While uncertainty as to legal requirements has bedeviled many eager implementers, the Department of Justice has issued excellent guidance to federal agencies with respect to implementing electronic government systems. The four keys in their opinion: availability (that is, the records persist and are accessible in an ERKS environment), legal sufficiency (for example, signatures), reliability (that is, integrity) and compliance with other laws (such as privacy or disability access).

Technical challenges on the other hand are often predicated more on cost efficiency than any other element. Here, the Office of Management and Budget (OMB) has the lead for e-government development and policy, and its February 2002 report on e-government strategies is well worth reading. More recently, OMB has embarked on supporting 24 separate initiatives at various agencies that have the potential for developing “plug-and-play” e-government components. It is an effort to watch although the GAO has offered some recent criticism on selection and accountability.

The final development of note in this arena is the E-Government Act of 2002. Lauded by many, it provides for funding and the creation of an e-government division at OMB, directs the Library of Congress to develop a national online library, requires the implementation of online court records (but with the Supreme Court to develop rules on privacy and security), requires Internet sites for federal agency rulemaking and docket information and makes permanent Congressional oversight of federal agency computer security.

But there is also criticism. Many believe that the act weakens the Federal Depository Library Program and that failure to provide guidance on electronic formats or to apply the act to Congress itself were significant errors.

The Cobell Litigation

If there is one litigation that should be in clear focus for every records and information manager in the government and in private industry – and for every senior mission manager – it is the Cobell civil action. Indeed, it is the quintessential object lesson for both information professionals and corporate managers in the importance of records management. Through multiple findings of contempt against cabinet secretaries and millions in fines and penalties, there are significant learnings: the critical role of records management in executing the direct mission of an agency, the equally critical role of RM in litigation and the fallacy that technology is a solution to pervasive data shortcomings.

The case – a class action lawsuit filed on behalf of individual Native Americans in 1996 and continuing

Research and Further Information Guide

The PWC report can be found at www.endowment.pwcglobal.com/pdfs/StowersReport0802.pdf; the Department of Justice guide to electronic government systems is at www.cybercrime.gov/eprocess.htm; and the OMB report on e-government is at www.whitehouse.gov/omb/inforeg/egovstrategy.pdf.

today – is predicated on the government’s alleged mismanagement of the Individual Indian Money (IIM) trust accounting system and is critical for information professionals to understand. At the heart of any trust litigation are financial records, and this case came to extensive public and media notice after the government failed for almost three years to respond to various discovery demands and exhausted the patience of the trial court after multiple efforts at compliance. By February of 1999 the matter was before the court on a motion to hold the heads of the defendant agencies (Treasury and Interior) in civil contempt of court. And the testimony of Paul Homan – a former special trustee appointed by the President, whose specific task was to oversee and reform the trust system – set the framework for the contempt hearing: “*The record-keeping system [for the IIM accounts] is the worst that I have seen in my entire life.*” Further, in his opinion, the Department of the Interior had become less, rather than more, responsive, due to repeated reorganizations. The trial court concluded that contempt was warranted from a combination of noncompliance, lack of good faith, cover-up and misconduct, noting “*The way in which the defendants have handled this litigation up to the commencement of the contempt trial is nothing short of a travesty.*” The result was findings of contempt against Treasury Secretary Robert E. Rubin, Interior Secretary Bruce E. Babbitt and Assistant Secretary Kevin E. Gover and an order for the government to pay \$625,000 of the Indian’s legal fees as a penalty. The censorious nature of the penalty and the language describing the defendant’s actions should speak clearly to every organization.

Yet, the matter did not end here since the February civil contempt proceeding had also concluded with the appointment of a special master to help oversee the production of documents. And, despite the clarity of the court’s judgment, the defendants had additional bad news that was withheld – specifically that in January it had come to the attention of senior department officials that some 162 boxes of relevant records had been destroyed, notwithstanding pending discovery motions and orders. But no mention of that destruction was made in February during the court proceedings nor afterwards until a letter on May 11, 1999, was delivered to the special master. The trial court immediately ordered an investigation that concluded with a detailed report adopted by the court on December 3, 1999, wherein the special master concluded that the destruction and notification delay stemmed from a lack of understanding of both records management and the obligations imposed by the court’s various orders.

But things did not improve in the following months. First, on December 6, 2001, the judge forced the Department of the Interior to disconnect from the Internet as a result of a computer security test ordered by the court after allegations by the plaintiffs that the trust fund data was at risk not only internally but also by outside hackers. The Department was crippled from its inability to communicate – internally among employees, to receive data from remote sensors and sites, and to disseminate information to government, business and private customers. And, second, on December 10, 2001, another contempt trial began – now involving Interior Secretary Gale A. Norton and an assistant secretary for Indian Affairs. These charges centered on the failure to perform a historical accounting project, computer records failures and the filing of a false quarterly report on departmental progress.

The magnitude of the records problems was apparent in the testimony of Thomas M. Thompson, the deputy special trustee of the fund. He stated that when the court ordered the probate section of the trust fund resolved two years ago, the Interior Department thought there might be 7,000 backlogged cases; he now believes there

may be 15,000 cases and even that number may be inaccurate. Contempt citations and the award of additional attorneys fees resulted on September 17, 2002 (estimated to be more than \$1.5 million), and on February 5, 2003, the court ordered personal sanctions and fines against a number of government attorneys, including the chief of the Department of Justice Civil Division for “*attempting to cover up*” false statements and misrepresentations by the defendants. The bottom line is that despite (or irrespective of) the infusion of substantial sums for technology, the grasp on the data is little better today.

What Lessons Do These Troubling Facts and Draconian Results Present to Us as Information Professionals? First, they highlight once again that records are assets, not overhead, and that, as such, records management is a critical facet of asset management. Second, they serve as an example that the demands of law are becoming ever more central to the work of every records manager – whether in government or private enterprise. Third, they confirm that information managers are key members of every litigation team – without this requisite linkage, the best legal representation will be ineffectual. Lastly, they confirm that resolving compromised data remains a uniquely human effort.

In Part 2 of this article, we will turn to the policy debate over access to public information.

Research and Further Information Guide

Relevant opinions are reported at 37 F.Supp.2d 6 (1999) (holding defendants Secretary of the Interior and Secretary of the Treasury in civil contempt of court for discovery abuse); 1999 U.S. Dist. LEXIS 20918 (D.D.C. 3 December 1999) (adopting report of the special master as to additional discovery abuses including unlawful destruction of records), affirmed, 240 F.3d 1081 (D.C. Cir. 2001); and 226 F.Supp.2d 1 (D.D.C. 17 September 2002) (finding additional contempt).