KATHY PARKER, CP,
has been a member of Humboldt County Legal Professionals Association for 18 years, holding numerous chair and board positions. She is the current Governor and Executive Advisor, most recently sitting as president in 2012-2013. She is a certified paralegal employed in civil litigation and insurance defense at the Law Offices of Mitchell, Brisso, Delaney & Vrieze, LLP, in Eureka, California.

To Shred or Not to Shred – That is the Question

BY KATHY PARKER, CP — SUBMITTED BY HUMBOLDT COUNTY LPA

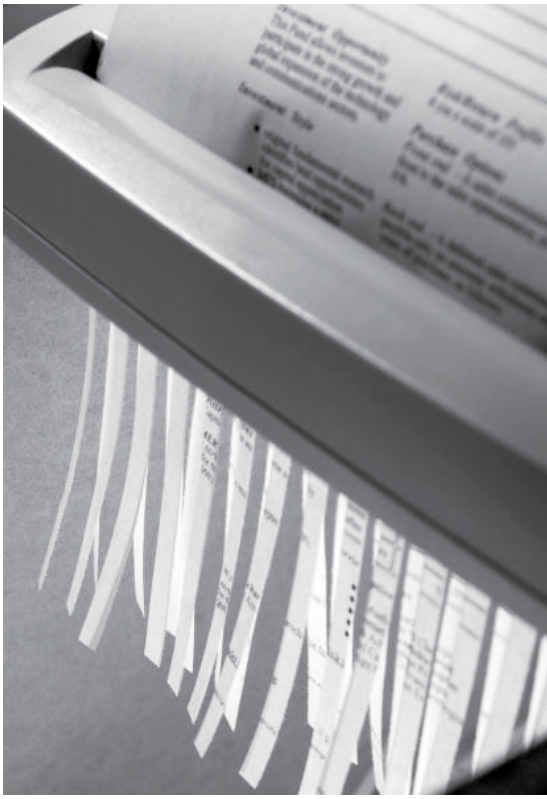
We have an annual "cleaning day" at our office, where the staff vaguely become aware that the numerous and/or voluminous files that have been closed and stored upstairs during the last year have filled storage to capacity and some must either be carted to off-site storage or destroyed.

The basic understood principle that readily comes to mind has always been "records must be retained for seven years . . . or is it ten?" -- a vague misunderstanding that rises to the surface annually when contemplating ones own tax records (for clarification, see: http://www.irs.gov/Businesses/How-long-should-I-keep-records). But what does "records retention" mean in the law office and when can documents be shredded? That answer is not as simple as it once was considered to be, and for the purpose of this article, will basically cover the background for requirements pertaining to retention or shredding of data.

The procedures for preservation and non-preservation of information have become more complex due to the electronic age and privacy issues. Of course, different kinds of documents require different handling or retention periods. (For example, a client's estate plan or corporate records should be kept in perpetuity, pending death or dissolution; but a paper file containing a lawsuit that settled a number of years ago may not need to be kept, while its key electronic storage may be useful for future or separate litigation purposes.) However, eventually, even legal documents lose their value and become obsolete. Keeping them indefinitely can expose your clients to unnecessary risks that can be avoided with a document destruction strategy. Regulatory compliance and increased emphasis on ethical conduct and accountability demand that you safeguard your clients' privacy and administrative records. [i]

The United States Supreme Court determined a case that helped define privacy rights relating to material discarded as trash. (*California v. Greenwood*, 486 U.S. 35 (1988).) In this case, the Supreme Court held that the Fourth Amendment does not prohibit the warrantless search and seizure of garbage left for collection outside the curtilage of a home. [ii]

Greenwood had thrown out information in his trash that incriminated him in a crime, and the information was used to gain a conviction. Greenwood claimed that he was the victim of an unlawful search and that his privacy rights had been violated. In its ruling, the Supreme Court stated that there could be no expectation of privacy in trash left accessible to the public. The Court further stated it is common knowledge that garbage is readily



accessible to animals, children, scavengers, snoops, and other members of the public (including criminals, investigators, journalists, garbage collection agencies, law enforcement, etc.).

Privacy protection is experiencing a rebirth in legislative activity. The runaway crime of "identity theft" is causing a groundswell of interest in the electorate; hence, also in our state and federal politicians. "Identity theft" also has a connection to national security issues.

The concept of protecting the privacy of ordinary citizens did not become significant until the beginning

Continued on page 10

Continued from page 9

of the information age. Problems arose from increased identity theft. The U.S. Congress responded with acts to protect privacy: the Social Security Act of 1934; Privacy Act of 1974; Right to Financial Privacy Act of 1978; Health Insurance Portability and Accountability Act of 1996 (HIPAA); Economic Espionage Act of 1996 (EEA); Gramm-Leach-Bliley Act (GLBA) of 1999; Fair Credit Reporting Act of 2001 (FCRA); Sarbanes-Oxley Act of 2002; and the Fair and Accurate Credit Transactions Act of 2003 (FACTA). These legislative acts have reinforced the overall need for organizations to take reasonable measures to safeguard private documents.

The 2003 FACTA expanded several FCRA provisions and provides protection for victims of identity theft (and includes one free credit report per year). The Federal Trade Commission (FTC) utilizes federal law and is responsible for enforcement. FACTA is a federal law designed to minimize the risk of identity theft and consumer fraud by enforcing the proper destruction of consumer information. The FTC developed the Disposal Rule in November 2004 to further implement the policies set forth in FACTA. The Disposal Rule applies to businesses that utilize consumer information; however it affects every person and business in the United States. The Disposal Rule requires disposal practices that are reasonable and appropriate to prevent the unauthorized access to – or use of – information in a consumer report.

The FACTA Disposal Rule, effective June 1, 2005, states that "any person who maintains or otherwise possesses consumer information for a business purpose" is required to dispose of discarded consumer information, whether in electronic or paper form. The Disposal Rule further clarifies the definition of compliance as "taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal." "Reasonable measures" include burning, pulverizing, or shredding physical documents; erasure or destruction of all electronic media; and entering into a contract with a third party engaged in the business of information destruction.[iii]

The "Comprehensive Identity Theft Protection Act" was passed in 2006. Almost every state is also passing laws to protect identity and privacy, and at the federal level additional new laws are being introduced. California and Georgia are being particularly aggressive, where new laws even require "self-reporting" of any security incident. The message is clear that private and confidential information should no longer be disposed of in the trash. Thus, if you look up "shredding laws" on the Internet, you will find numerous shredding businesses that provide much more detailed information regarding the congressional acts (see sources listed at the end of this article, as well as local advertisers in your area), and offers for professional shredding services are prolific.

Existing law requires a business to take all reasonable steps to destroy a customer's records containing personal information when the business will no longer retain those records. The existing laws provide civil remedies for violations of these provisions. California Senate Bill 1386 was introduced in July 2003 and was the first attempt by a state legislature to address the problem of identity theft. In short, the bill introduces stiff disclosure requirements for businesses and government agencies that experience security breaches that might contain the personal information of California residents. It is expected that many organizations in the United States (and possibly worldwide) are now subject to these requirements.

SB 1386 comes with the biggest recrimination, allowing for civil ligation against businesses that don't comply. If you fail to disclose computer security breaches, you become liable for civil damages and may face a class action lawsuit. However, the bill permits notifications required by its provisions to be delayed if a law enforcement agency determines that it would impede a criminal investigation. The bill would require an agency, person, or business that maintains computerized data including personal information owned by another to notify the owner or licensee of the information of any breach of security of the data, as specified. The bill states the intent of the Legislature to preempt all local regulation of the subject matter of the bill. This bill would also make a statement of legislative findings and declarations regarding privacy and financial security.

Civil Code sections 1798.80-1798.84 provide details pertaining to requirements, violation, rights, and remedies.[iv] The consequences for failing to maintain legislative compliance include serious fines and penalties.[v]

So it is clear that basic steps are needed to create and implement an effective document retention policy (a whole separate magazine article in itself). The reader here should utilize research tools available to effectuate a well-designed policy that ceases document destruction upon notice of a pending lawsuit or governmental investigation, as well as utilizing Government Code requirements for specific retention periods, depending upon the type of entity, or department within the entity, for which the document retention policy is needed.

While paper shredding can elicit images of obstruction of justice a lá Enron, with today's technological advances and the information-sharing electronic age, the majority of information is now generated electronically, and 60 to 70 percent of all documents are never printed. Hence, discovery of electronic information is also critical in litigation today. The California state courts, as well as federal courts, allow discovery of information stored electronically. Revisions to the Federal Rules of Civil Procedure to incorporate electronic discovery continue to be updated. It is assumed that state

court judges will utilize federal rules to some degree for guidance when dealing with issues pertaining to discovery of electronic evidence. But, getting back to best practices for retention or shredding: Many businesses have adopted retention polices that require routine destruction of documents or information after a certain lapse of time. Under FRCP 37(f), absent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the routine operation of such a procedure.

Because technology is changing so quickly, new questions and issues continue to arise. The best policy is to have a policy that protects identity and privacy while regularly monitoring the status of files and data, as well as continuing to monitor how the courts use their inherent power to manage discovery and address issues as they come up. [vi]

Without a program to control it, the daily trash of every business contains information that could be harmful. This information is especially useful to competitors because it contains the details of current activities. Discarded daily records include phone messages, memos, misprinted forms, drafts of bids, and drafts of correspondence. All businesses suffer potential exposure due to the need to discard these incidental business records. The only means of minimizing this exposure is to make sure such information is securely collected and destroyed.

Again, while paper documents remain the most visible and tangible information that must be dealt with, they are not the only format where your confidential information is stored. Keep in mind that data is contained on all types of information storage: paper, x-rays, checks, promotions, cardboard, signage, binders, files, photographs, CDs, DVDs, hard drives and back-ups, portable drives, computers, videotapes, prototypes, and the list goes on.

Once a business no longer needs a document and its retention is not otherwise required, it should generally be destroyed. By not adhering to a program of routinely destroying stored records, a company exhibits suspicious disposal practices that could be negatively construed in the event of litigation or audit. Also, Federal Rule 26 regarding disclosure requires that, in the event of a lawsuit, each party provide all relevant records to the opposing counsel on a deadline. If either of the litigants does not fulfill this obligation, it will result in a summary finding against them. By destroying records according to a set schedule, a company appropriately limits the amount of materials it must search through to comply with this law. If a party makes a discovery request, the other party has a duty to diligently search for documents in its custody responsive to the request. (Code of Civil Procedure §2031.280(a).) And fewer necessary documents mean less expensive time-consuming search and production.

It is permissible to destroy documents, including deleting computer files and shredding documents, unless at the time of the destruction there was a duty to preserve them. A document retention policy can be critical in positioning a business to effectively and efficiently defend against future lawsuits, while allowing it to justifiably dispose of unneeded documents while managing only necessary documents. Such a retention policy also holds down litigation costs.

From a risk management perspective, the acceptable method of discarding stored records is to destroy them by a method that ensures that the information is obliterated, and documenting the exact date that a record is destroyed is a prudent and recommended legal precaution. For various important reasons, the choice of recycling as a means of information destruction is undesirable from a risk management perspective.

Every business entity, not just a law office, needs to have and enforce an appropriate document and data retention or destruction policy. The nature of that policy, its enforcement, and/or non-usage of the policy to avoid destruction of evidence may have significant ramifications in litigation.

ENDNOTES:

i. http://www.shredit.com/Legal-shredding-service.aspx

ii. http://en.wikipedia.org/wiki/California_v._Greenwood

iii. http://www.stopandshred.com/government_regulations.php; Stop and Shred Document Shredding Service

iv. http://www.goshredex.com/california-shredding-laws-senate-bill-1386.php

v. http://www.proshred.com/current-privacy-legislation; ProShred Security

vi. http://www.shrednations.com/articles/Shredding-Compliance.php; Shred Nations

OTHER SOURCES USED:

1.) Risk Management – Record Retention Policies – Electronic Data Changing the Way the Game is Played; July 2012, by Mark C. Russell, GORDON & REES; http://www.gordonrees.com/publications/viewPublication.cfm?contentID=2729.

2.) Lexis Nexis notes re document retention: http://www.lexisnexis.com/applieddiscovery/lawlibrary/whitePapers/ADI_WP_ElementsOfAGoodDocRetentionPolicy.pdf; by Timothy R. Sullivan of McLaughlin Sullivan LLP

3.) http://www.fresnocountybar.org/files/SELF-TEST-NewElectronicDiscovery-Rules2.doc

LS