League of California Cities
Annual Conference
City Attorneys' Department
September 17-19, 2004

Oh Where, Oh Where Have My E-Data Gone?: Electronic Data, Records Retention and Spoliation

Susan Burns Cochran
City Attorney
City of Lathrop
16775 Howland Road, Suite 1
Lathrop, California 95330
(209) 858-2860, Ext. 334
sbc@ci.lathrop.ca.us

Oh Where, Oh Where Have My E-Data Gone?: Electronic Data, Records Retention and Spoliation

By

Susan Burns Cochran[1]

During the May 2004 City Attorneys Department conference in San Diego, the presentation on "Electronic Communications as Public Records: The Sequel" contained discussion focused on the deletion of email and other electronic data (hereinafter "e-data'). The question presented was how, if at all, the usual rules relating to records retention by public entities differ in their application to e-data from their application to conventional records. This paper seeks to expand that discussion by outlining the basic rules governing records retention; asserting that e-data are treated no differently by the law than are paper records; and identifying potential outcomes if e-data are improperly eliminated or destroyed.

I. Electronic Data: An Overview.

In recent years, there has been an explosion in the use of email and other electronic data. For example, in January 2002, the *Wall Street Journal* reported that the United States Postal Service delivered over 207 billion pieces of mail in 2001. During that same time period, 1.4 **trillion** email messages were sent from businesses in North America, up from 40 billion in 1995. As the use of information technology has exploded, the legal profession's handling of this technology has not kept pace. Nevertheless, how your city handles its e-data has far-reaching consequences, particularly within the context of litigation, including criminal prosecutions. The impact is not limited to court proceedings, but also can be felt in the public perception of how the city handles its operations and potential Brown Act and Public Records Act violations.

The first question then is "What are e-data?" Before discussing how to retain electronic data, the definition of e-data is critical. While most of us are familiar with the more accessible types of electronic data, such as email, attachments to email, AutoCAD drawings and the like, there are other data out there.

[1] The author would like to express her gratitude to Robert Hambrick, Information Systems Manager for the City of Lathrop, for taking the time to bring her out of the darkness and into the information age.

Another important feature of e-data that distinguishes it from the paper documents with which we are more familiar is that e-data can exist in a variety of forms. There are essentially four types of e-data.

Active Data: Active Data is information residing on the direct access storage media of computer systems, which is readily visible to the operating system and/or application software with which it was created and immediately accessible to users without undeletion, modification or reconstruction. This is the type of data most familiar to users of word processing and spreadsheet programs. It includes "meta data" or information retained by a computing system of which a user may not be aware, such as recent deletions from a word processing document; dates a document was created, accessed, or copied; data regarding who created, edited or viewed a document, etc.

Archival Data: Archival Data is information that is not directly accessible to the user of a computer system but that the organization maintains for long-term storage and record keeping purposes. Archival data may be written to removable media such as a CD, magneto-optical media, tape or other electronic storage device, or may be maintained on system hard drives in compressed formats.

Backup Data: Backup Data is information that is not presently in use by an organization and is routinely stored separately upon portable media, to free up space and permit data recovery in the event of data loss.

Residual Data: Residual Data (sometimes referred to as "Ambient Data") refers to data that is not active on a computer system. Residual data includes (1) data found on media free space; (2) data found in file slack space, such as print buffers, temporary files, and directories; and (3) data within files that has functionally been deleted in that it is not visible using the application with which the file was created, without use of undelete or special data recovery techniques.

The sources of e-data vary as well. Not only are they in computers, they exist in floppy disks, CD-ROMs, personal digital assistants ("PDAs"), wireless communication devices (*e.g.*, Blackberry and Palm Pilot devices), zip drives, Internet repositories such as e-mail hosted by Internet service providers or portals, web pages, and the like.

The result of this maze of types and sources is that, unless a specialized program is used to "wipe" a computer's disk drive clean, some recovery of e-data is possible. In short, just because you deleted it, doesn't mean it is gone.

II. Records Retention: The Basics

Given the many states and sources of e-data, what is the best way to manage this information? The fundamental rule regarding the retention of documents by public entities in California is found at Government Code section 34090, which states:

> *Unless otherwise provided by law, with the approval of the legislative body by resolution and the written consent of the city attorney the head of a city department may destroy any city record, document, instrument, book or paper, under his charge, without making a copy thereof, after the same is no longer required.*
>
> *This section does not authorize the destruction of:*
>
> *(a) Records affecting the title to real property or liens thereon.*
> *(b) Court records.*
> *(c) Records required to be kept by statute.*
> *(d) Records less than two years old.*
> *(e) The minutes, ordinances, or resolutions of the legislative body or of a city board or commission.*
>
> *This section shall not be construed as limiting or qualifying in any manner the authority provided in Section 34090.5 for the destruction of records, documents, instruments, books and papers in accordance with the procedure therein prescribed.*

In addition to section 34090, and as recognized by that section, other statutes provide timelines for the length of time that public agencies are required to keep certain records. Certain types of records have specified retention cycles. Examples include:

Records Regarding the Disposition of Animals at Shelters	2 years (Food & Agriculture §32002)

Water Test Reports	18 years (22 California Administrative Code § 64692)
Backflow Test Reports	3 years (17 California Administrative Code § 7605(f)
Initiative Petitions	8 months after the certification of the results of the election for which the petition qualified OR, if the measure, for any reason, is not submitted to the voters, 8 months after the final examination of the petition by the elections official. (Elections Code §17200)
Citizen Complaints against Peace or Custodial Officers	5 years (Penal Code § 832.5(b)
Telephone and Radio Communications	100 days (Government Code §53160)
Video Recordings of Events	90 days [subject to specific conditions] (Government Code §34090.7)
Audit Papers for any Entity Issuing Securities	5 years (18 U.S.C. §1520(b)

The courts have held that, the plain meaning of section 34090 requires that a city not destroy any records less than two years old. See, e.g., People v. Zamora (1980) 28 Cal.3d 88, 98 (destruction of criminal complaint records less than two years old violated requirements of section 34090). The difficulty, however, is that the statute does not clearly define "city record, document, instrument, book or paper", especially as these terms apply to e-data.

While section 34090 may not provide a definition, the Public Records Act (Cal. Gov't. Code § 6250, et seq.) does. A "public record" is broadly defined by the Public Records Act to mean "any writing containing information relating to the conduct of the public's business prepared, owned, used, or retained by any state or local agency regardless of physical form or characteristics." Cal. Gov't Code § 6252(e). Similarly, the Public Records Act defines a "writing" as "any handwriting, typewriting, printing, photostating, photographing, photocopying, **transmitting by electronic mail or facsimile**, and

every other means of recording upon any tangible thing any form of communication or representation, including letters, words, pictures, sounds, or symbols, or combinations thereof, and any record thereby created, regardless of the manner in which the record has been stored." Cal. Gov't Code § 6252(f) (emphasis added).

Courts have noted that the definition under section 6252 is broad and intended to cover every conceivable kind of record involved in the governmental process. *San Gabriel Tribune v. Superior Court* (1983) 143 Cal.App.3d 762, 774, 192 Cal.Rptr. 415. The intent of the Public Records Act is "to safeguard the accountability of government to the public ...." *Wilson v. Superior Court* (1996) 51 Cal.App.4th 1136, 1141, 59 Cal.Rptr.2d 537.) In order to promote accountability, individuals must have access to government files to check the arbitrary exercise of official power and secrecy in the political process. *CBS, Inc. v. Block* (1986) 42 Cal.3d 646, 651, 230 Cal. Rptr. 362, 725 P.2d 470.

Given important policies served by public records, and their required openness to public inspection, the safest course of action thus seems to be to consider city records under section 34090 to be as broad as the definition contained in the Public Records Act. Because the Public Records Act expressly includes electronic mail within its definition of a "record", destruction of email would be subject to the same strictures as any other paper record: (1) being at least two years of age; (2) approval by the City Attorney; and (3) a resolution of the City Council authorizing its destruction.

Further support for the view that e-data are treated the same as paper data can be found in California Government Code section 34090.5. This section allows for the destruction of paper items before the expiration of the two years mandated by section 34090 provided that electronic storage of the document through various means, including e-data. By equating e-data to paper documents for purposes of retainage, the legislature arguably viewed them as comparable sources of information about governmental activities.

III. Pitfalls For Failure To Manage E-Data Properly

Many if not most California jurisdictions currently have email policies that provide for the periodic deletion of those files, almost universally after retention of less than two years. What penalties can flow from failing to properly destroy the e-data resulting from this

email? Secondly, what can a jurisdiction and its legal counsel do to protect themselves from these consequences?

A. Spoliation

"Spoliation of evidence is the destruction or suppression of evidence. A first-party spoliator is a party to the litigation in which the spoliated evidence is deemed relevant." *Johnson v. United Services Auto. Assn*. (1998) 67 Cal.App.4th 626, 629, 79 Cal.Rptr.2d 234. Third-party spoliation is the destruction of evidence by a person not a party to the action in which the evidence is relevant. *Id.*

The Supreme Court held in *Cedars-Sinai Medical Center v. Superior Court* (1998) 18 Cal.4th 1, 12, 954 P.2d 511, 74 Cal.Rptr.2d 248 that there is no cause of action in tort for intentional spoliation of evidence among parties to pending litigation. The following year, in *Temple Community Hospital v. Superior Court* (1999) 20 Cal.4th 464, 84 Cal.Rptr.2d 852, 976 P.2d 223, the Supreme Court answered the question it had left open in *Cedars-Sinai* and declined to extend tort liability for intentional spoliation against non-litigants.

As for negligent spoliation of evidence by third parties, there is a split in the appellate courts. In *Johnson, supra*, 67 Cal.App.4th 626, 79 Cal.Rptr.2d 234, the Third District Court of Appeal recognized a cause of action for negligent spoliation of evidence where the duty to maintain the evidence grew out of a contract "or on a statute, a regulation (for example, record-retention statutes and regulations), or some analogous special relationship." *Id.* at 635, 79 Cal.Rptr.2d 234. However, the Fourth Appellate District disagreed in *Farmers Ins. Exchange v. Superior Court* (2000) 79 Cal.App.4th 1400, 95 Cal.Rptr.2d 51. Similarly, the Second Appellate District in *Coprich v. Superior Court* (2000) 80 Cal.App.4th 1081, 95 Cal.Rptr.2d 884 declined to follow *Johnson*.

Following *Farmers* and *Coprich*, in *Lueter v. State of California* (2002) 94 Cal.App.4th 1285, 115 Cal.Rptr.2d 68, the Third District Court rejected its earlier conclusion in *Johnson*. The *Lueter* court departed from the analysis of the *Johnson* court, which predated *Temple Community*, and found that public entities could not be susceptible to claims for negligent spoliation unless and until the Legislature acted to impose such liability. *Lueter, id.* at 1300, 115 Cal.Rptr.2d 68. Part of the analysis in *Leuter* also focused on the fact that "threat of liability might cause individuals and entities to engage

in unnecessary and expensive retention policies." *Id.* at 1297, 115 Cal.Rptr.2d 68 (internal cits. om.)

This conflict continues to date, as the Supreme Court has not depublished *Johnson* or taken review of any other case dealing with the cause of action for negligent spoliation. Thus, potential liability still exists.

B. Additional Sanctions

Regardless of whether the courts recognize a cause of action for negligent spoliation of evidence, other penalties await those who improperly erase or eliminate evidence, especially e-data.

1. State Bar Disciplinary Proceedings: In declining to recognize a cause of action for intentional spoliation, the *Cedars-Sinai* court discussed the availability of alternate remedies in the context of litigation as the justification for not extending tort liability. The court discussed one potential disincentive this way:

> *Another important deterrent to spoliation is the customary involvement of lawyers in the preservation of their clients' evidence and the State Bar of California disciplinary sanctions that can be imposed on attorneys who participate in the spoliation of evidence. As a practical matter, modern civil discovery statutes encourage a lawyer to marshal and take charge of the client's evidence, most often at an early stage of the litigation. In doing so, a lawyer customarily instructs the client to preserve and maintain any potentially relevant evidence, not only because it is right for the client to do so but also because the lawyer recognizes that, even if the evidence is unfavorable, the negative inferences that would flow from its intentional destruction are likely to harm the client as much as or more than the evidence itself.*
> *In addition, the risk that a client's act of spoliation may suggest that the lawyer was also somehow involved encourages lawyers to take steps to protect against the spoliation of evidence. Lawyers are subject to discipline, including suspension and disbarment, for participating in the suppression or destruction of evidence. (Bus. & Prof. Code, § 6106; Rules Prof. Conduct, rule 5- 220 ["A member shall not suppress any evidence that the member or the member's client has a legal obligation to reveal or to*

produce."].) The purposeful destruction of evidence by a client while represented by a lawyer may raise suspicions that the lawyer participated as well. Even if these suspicions are incorrect, a prudent lawyer will wish to avoid them and the burden of disciplinary proceedings to which they may give rise and will take affirmative steps to preserve and safeguard relevant evidence.

Cedars-Sinai Medical Center, supra, 18 Cal.4th at 13, 954 P.2d 511, 74 Cal.Rptr.2d 248.

2. Criminal Prosecution: Further sanctions for destruction of evidence can be found in Penal Code section 135, which creates criminal penalties for spoliation.

"Every person who, knowing that any book, paper, record, instrument in writing, or other matter or thing, is about to be produced in evidence upon any trial, inquiry, or investigation whatever, authorized by law, willfully destroys or conceals the same, with intent thereby to prevent it from being produced, is guilty of a misdemeanor."

Penal Code section 135 presents a very dangerous trap for the unwary. By broadening the class of activities to which the section applies to include inquiries or investigations authorized by law, potential liability could exist to those employees who destroy records, including e-data, when a Public Records Act request is pending.

3. Evidentiary Sanctions at Trial: The *Cedars-Sinai* court also pointed to the evidentiary inference contained in California Evidence Code section 413:

In determining what inferences to draw from the evidence or facts in the case against a party, the trier of fact may consider, among other things, the party's ... willful suppression of evidence relating thereto....

Cedars-Sinai, supra, 18 Cal.4th at 12, 954 P.2d 511, 74 Cal.Rptr.2d 248.

4. Discovery Sanctions: Finally, the *Cedars-Sinai* opinion discussed the potential for discovery sanctions. *Id.* These sanctions include monetary sanctions, contempt sanctions, issue sanctions

ordering that designated facts be taken as established or precluding the offending party from supporting or opposing designated claims or defenses, evidence sanctions prohibiting the offending party from introducing designated matters into evidence, and terminating sanctions that include striking part or all of the pleadings, dismissing part or all of the action, or granting a default judgment against the offending party. *Id.*, citing California Code of Civil Procedure § 2023.

In the e-data age, these discovery sanctions take on frightening size. First, both the Federal Rules of Civil Procedure and the California Code of Civil Procedure recognize the discoverability of e-data. Fed. R. Civ. P. 34(a) ("Document" includes data compilations from which information can be obtained, translated, if necessary, by the respondent through detection devices into reasonably usable form); Cal. Code Civ. Proc §2016(b)(3).

Where active data, as described above, are still available, this requirement is not overly burdensome. But if that data have been erased or destroyed so that only residual or back-up data still exist, the costs of reproducing the e-data into readable or usable form can be passed onto the party charged with providing the information. See Fed. R. Civ. P. 26(c); Cal. Code Civ. Proc. § 2031(f)(1).

5. AB 3081: In an effort to increase the use of technology in the discovery process, the Legislature passed and the Governor signed into law AB 3081, which adds new provisions to the civil discovery statutes. These provisions, to be effective on July 1, 2005 and to be codified at California Code of Civil Procedure section 2017.710 *et seq.*, "permit and encourage" the use of electronic discovery and media, particularly in complex cases. In order to utilize these provisions, a notice motion is required and the case must fall into certain types. Cal. Code Civ. Proc. § 2017.730 (a).[2] The new sections also authorize use of these procedures by stipulation. In general, however, the use of electronic discovery should further several goals, including being cost-effective and efficient in undertaking discovery or motions relating

[2] Pursuant to a noticed motion, a court may enter an order authorizing the use of technology in conducting discovery in any of the following:
(1) A case designated as complex under Section 19 of the Judicial Administration Standards.
(2) A case ordered to be coordinated under Chapter 3 (commencing with Section 404) of Title 4 of Part 2.
(3) An exceptional case exempt from case disposition time goals under Article 5 (commencing with Section 68600) of Chapter 2 of Title 8 of the Government Code.
(4) A case assigned to Plan 3 under paragraph (3) of subdivision (b) of Section 2105 of the California Rules of Court.

to discovery, not imposing or requiring an undue expenditure of time or money, or requiring the parties or counsel to purchase exceptional or unnecessary services, hardware, or software.

IV. PROTECTING YOURSELF AND YOUR CITY

Against this backdrop of doom and gloom, there still exists a ray of sunshine. The best defense against claims of improper destruction of evidence is a good offense: a records retention and destruction policy that is consistently and diligently applied. A model records retention policy can be found at the California Secretary of State's website, Click here: California State Archives - Local Government Records Program (http://www.ss.ca.gov/archives/level3_locgovrec.html).

The efficacy of this approach was recognized in *Cedars-Sinai* in refusing to extend liability because of the adverse impact such liability could have on those corporations and other entities who have "document retention policies under which they destroy at stated intervals documents for which they anticipate having no further need. (See *Willard v. Caterpillar, Inc., supra,* 40 Cal.App.4th 892, 919-924, 48 Cal.Rptr.2d 607; *Akiona v. U.S.* (9th Cir.1991) 938 F.2d 158, 161; *Lewy v. Remington Arms Co., Inc.* (8th Cir.1988) 836 F.2d 1104, 1111-1112; Fedders & Guttenplan, *Document Retention and Destruction: Practical, Legal and Ethical Considerations* (1980) 56 Notre Dame L.Rev. 5, 7, 11-17, 53-55.)" *Cedars-Sinai, supra*, 18 Cal.4th at 15, 954 P.2d 511, 74 Cal.Rptr.2d 248.

This is not to say that slavish devotion should be followed. If you know or have reason to believe that there is litigation or an investigation pending or imminent, do not destroy relevant information, even if its time is up. Otherwise, you and your city could find yourself on the receiving end of the sanctions outlined in this paper. These consequences follow even if you think you have deleted the files or information. Given the rich archival data on a given city's computers, it is impossible to say something is ever really gone. Nothing could be more embarrassing than your opponent retrieving archival, retrieval or back up data from a hard drive made discoverable by improper records destruction.