Mining Evidence Under the New Electronic Discovery Act
by Christopher C. Melcher

Most information is created and stored electronically, yet document productions are still largely done by paper. Printing out electronic documents for discovery not only wastes paper, it also results in the loss of potentially significant evidence. California has taken a major step toward modernizing its discovery laws by enacting the Electronic Discovery Act to facilitate the discovery of writings created in digital form. E-Discovery ranges from a simple request that a party produce files or data from a computer, cell phone, or other electronic device on a CD-ROM, to the physical inspection of a computer system by an expert.

E-Discovery has been around for years and is routine in larger cases. Where the litigation budget is tight, lawyers have abstained from E-Discovery, concerned that the expense of hiring a computer expert will outweigh the benefit of obtaining the information. Not all E-Discovery requires the use of an expert. In fact, the use of an expert is usually required only where a party wants to recover data believed to have been intentionally erased or altered, or where a party wants to search a computer for data. In all other cases, it should suffice to simply ask for the production of computer data, as would be done for any other type of writing. For example: "Produce the premarital agreement between the parties dated June 5, 2008, in the electronic form in which the document was created."

Relying on the opposing party to produce a paper version of electronically stored information ("ESI") can be a mistake. It is usually better to demand that the data itself be produced. Viewing a document in electronic form can tell the reader the history of the document (such as when it was created and who created it), things which cannot be seen on paper. It is also easier to work with information in electronic form, rather than thumbing through a stack of papers to find information or having to enter financial information into a spreadsheet by hand for analysis.

When a document is created on a computer, an electronic fingerprint is left behind called "metadata." In the case of a document created using a word processor program, the metadata can reveal the name of the computer user who was logged into the computer when the document was created, when it was first created, the date it was last edited, the number of revisions, and how many times the document was printed. It may also be possible to see each change made to the document and the user who made the change. Comments about the document by the creator of the document (electronic sticky notes) may also be present. Basic metadata can be viewed in Microsoft Word and Excel by opening a document and clicking on the Office button, then Prepare, then Properties, then selecting Document Properties and clicking on Advanced Properties. Metadata is a rich, but often unexplored, source of evidence which could be used to resolve disputes over the genuineness of a document, to show when it was created, who created it, or to establish that it was the product of negotiation. However, this information can only be seen if the document is produced in the electronic form it was created.

Getting electronic data, in lieu of a printout, can also ensure that the entire document is produced – not just the portion the responding party decided to print out. For example, large spreadsheets are often wider than paper, so the user selects only part of the spreadsheet to print,

leaving out a column of notes or other valuable information. Finally, it is easier to search for a keyword or create customized reports when the information is produced electronically.

E-Discovery was always possible under California law, but until recently there were no special provisions for the production of electronically stored information ("ESI"). Effective June 29, 2009, the Electronic Discovery Act provides a comprehensive framework for obtaining ESI through discovery. The Act applies to inspection demands for ESI to parties, and also to subpoenas for ESI directed to witnesses. The new rules are similar to provisions for E-Discovery found in the Federal Rules of Civil Procedure.

Requesting ESI is just like demanding any other type of writing – a demand is served identifying the ESI to be produced. The difference is that a request for ESI should specify the form in which the data is to be produced. (CCP 2031.030, subd. (a).) The choice is whether the ESI is produced in the form in which it is ordinarily used by the responding party (called "native format") or in a "reasonably usable" form, typically a conversion of the data from its native format to a PDF file using Adobe Acrobat or as a TIFF image. The distinction is vital: native format contains metadata but is only readable if you have the software program used to create the data; a PDF or TIFF file can be opened by everyone but lacks the metadata from the original document.

For example, if accounting data is maintained by a company using a spreadsheet program like Excel, the request should be made for production of the file in its native (Excel) format, as Excel is a program most of us already have which can be used to open the file and view the metadata. On the other hand, if the company uses an accounting program to maintain its data, the propounding party will need to purchase a license for that software to even open the file. It could cost thousands of dollars to buy the license to view the data and any metadata. A more cost-effective option in this situation would be to request that the responding party export the data to a spreadsheet file, but the trade-off is that the metadata will not be exported. It is still beneficial to have the data in electronic form rather than paper to facilitate searching the data for key information and to use the data to create specialized reports. Ideally, the parties should agree on the format in which the ESI will be produced prior to the date of production. This will avoid delay when documents are produced in a format not readable by the propounding party, or in a format stripped of its metadata.

If the demand does not specify the form in which the ESI is to be produced, the responding party may elect to produce the information in native form or in a reasonably useable form, unless the court orders otherwise. (CCP 2031.280, subd. (d)(1).) Even where a demand is made for the production of ESI in a particular format, the responding party may object and specify "the form in which it intends to produce each type of the information." (*Id.*, subd. (b).) A responding party usually wants to produce ESI in a "reasonably usable" form, such as a secure PDF or TIFF image, in order to avoid producing hidden metadata and to prevent tampering with the data after it is produced, which is possible if the data is produced in its native format. However, when the data is converted into a secure image, the metadata is not transferred. One possible resolution to disputes over the production of ESI in native format versus as a secure image would be an agreement or court order that the information be produced in both formats.

(See *Id.*, subd. (d)(1) (production is only required in one format unless the parties agree or the court orders otherwise).)

When a document is requested in discovery in its native form, the entire document must be produced, including its metadata. Stripping the metadata is technically possible, but would constitute an alteration of the document. A party wanting to redact the metadata before production must have a legitimate objection why the metadata should not be produced (other than it might be harmful to the responding party's case). If the responding party decides to redact metadata, the party must state in the response that metadata has been removed from the copy and will have to preserve the original, un-redacted file in case the court orders it to be produced. Otherwise, the party will be subject to a spoilation of evidence claim.

When a demand for ESI requires the responding party to produce ESI from a source which is not reasonably accessible (such as from a backup file or data created by an old computer program no longer used by the business), an objection may be made that specified data "is from a source that is not reasonably accessible because of undue burden or expense and that the responding party will not search the source in the absence of an agreement with the demanding party or court order. . . ." (CCP 2031.210, subd. (d).) The party making the objection has the burden of proof to show that production would be unduly burdensome or expensive on any motion to compel the information. (CCP 2031.310, subd. (d).) Even if the party meets its burden, the court may nonetheless order production of the ESI if good cause is shown by the moving party, subject to an allocation between the parties of the expense of producing the information. (*Id.*, subds. (e) & (f); *Toshiba v. Sup.Ct.* (2004) 124 Cal.App.4th 762 (allocating estimated $1.9 million cost of recovering and translating data from a computer back-up to the requesting party).)

Due to the vast amount of information which may be stored on a computer, including possibly privileged, confidential, or irrelevant information, a protective order may be needed to limit what information may be discovered. The concern exists especially when there is an inspection demand for direct access to a computer system for purposes of "copying, testing, or sampling." (See CCP 2031.010, subd. (a.).) This would entail the inspection of the opponent's computer system by a computer expert, allowing the expert to view, search for, and copy data from the system. The Act, however, does not "create a routine right of direct access to a party's electronic information system, although such access may be justified under some circumstances. Courts should accordingly guard against undue intrusiveness resulting from inspecting or testing electronic information systems." (Senate Judiciary Comm. Analysis, 6/8/09, p.6.) Requests for inspection of a computer system will invariably be conducted under a protective order, limiting access to or use of certain data.

When privileged information or work product is inadvertently produced, the Act allows a "claw back" of the information. The party who produced the information may give notice of the privilege claim, requiring the receiving party to "immediately sequester" the information and either return the information or present it to the court conditionally under seal. (CCP 2031.285.) The receiving party may not use or disclose the allegedly privileged information until the claim is resolved. (*Id.*) In addition, there is a duty created by case law which must be observed. When the receiving party learns that privileged information has been produced, that party "should

refrain from examining the materials any more than is essential to ascertain if the materials are privileged" and has an affirmative duty to notify the producing party "that he or she possesses material that appears to be privileged . . . ." (*Rico v. Mitsubishi Motors Corp.* (2007) 42 Cal.4th 807.)

Nothing in the Act creates a duty to preserve ESI before a discovery request has been made for the information. If it is clear from the beginning of the case that ESI will be crucial evidence, a litigation hold notice should be served demanding that the party or witness retain the evidence pending discovery. The notice may be served prior to the commencement of litigation and must specify the evidence to be preserved. The notice, itself, does not impose a duty to preserve evidence, but if a party subsequently destroys the requested information it may establish that the party acted intentionally, possibly giving rise to sanctions. These notices are important where the information is held by a large business, which may have a policy of deleting electronic information (such as email) after a specified period of time. The notice should request that the business suspend its document retention/destruction policy with respect to the requested ESI, so the information is not destroyed pursuant to that policy.

Once a discovery demand has been made, there is no question that the subsequent and intentional destruction of the requested information is illegal and will result in severe penalties. (*Cedars-Sinai Medical Center v. Sup.Ct.* (1998) 18 Cal.4th 1, 4; see CCP 2023.010, subd. (d).) The Act provides a safe harbor defense for any ESI which is "lost, damaged, altered, or overwritten as the result of the routine, good faith operation of an electronic information system," but does not alter any obligation to preserve discoverable information (CCP 2031.060, subd. (i).) Therefore, if the information was destroyed as a result of "routine maintenance" after a litigation hold notice was served, the party may not be able to avail itself of the safe harbor protection.

Now that California has adopted procedures for conducting E-Discovery, requests for ESI should be part of a routine discovery plan. Getting ESI in electronic form is better than paper because it contains more information, is easier to use and distribute, and eliminates wasteful printing.