HERRING LAW GROUP

Certified Specialist, Family Law, The California Board of Legal Specialization of the State Bar of California

Fellow of the American Academy of Matrimonial Lawyers
Fellow of the International Academy of Family Lawyers

Writer's direct email: gherring@theherringlawgroup.com

The State Bar Issues Welcome ESI/E-Discovery Guidelines

by Gregory W. Herring

Electronically stored information ("ESI") is information that is stored in technology having electrical, digital, magnetic, wireless, optical, electromagnetic or similar capabilities. Electronic Discovery, or e-discovery, is the use of legal means to obtain ESI in the course of litigation for evidentiary purposes. Together, they constitute interesting and important considerations and challenges that overlay family law as well as traditional civil litigation.

Until now, California lawyers have had little ESI/e-discovery guidance at the state level. Ideas and legal opinions have issued from other states and from federal law, but none had considered California's particular ethical rules and standards. Thankfully, the State Bar of California's Standing Committee on Professional Responsibility and Conduct ("COPRAC") has now done this. In early July it issued Formal Opinion No 2015-193.

The Opinion points out that electronic document creation and/or storage, and electronic communications have become commonplace in modern life. It acknowledges that discovery of ESI is now a frequent part of almost any litigated matter. It emphasizes that attorneys who handle litigation may not ignore the requirements and obligations of electronic discovery.

While not every litigated case involves e-discovery, in today's technological world almost every litigated case *potentially* does. "The chances are significant that a party or a witness has used email or other electronic communication, stores information digitally, and/or has other forms of ESI related to the dispute."

Under the Opinion, attorneys handling e-discovery should be able to perform (either by themselves or in association with competent co-counsel or expert consultants) the following:

- Initially assess e-discovery needs and issues, if any;

- Implement/cause to implement appropriate ESI preservation procedures;
- Analyze and understand a client's ESI systems and storage;
- Advise the client on available options for collection and preservation of ESI;
- Identify custodians of potentially relevant ESI;
- Engage in competent and meaningful meet and confer with opposing counsel concerning an e-discovery plan;
- Perform data searches;
- Collect responsive ESI in a manner that preserves the integrity of that ESI; and
- Produce responsive non-privileged ESI in a recognized and appropriate manner.

Practitioners will have to proactively recognize and inform clients of the risks and responsibilities, and in a systematic and realistic manner. (*See Metro Opera Ass'n. v. Local 100, Hotel Employees and Restaurant Employees Int'l Union* (SDNY 2003) 212 FRD 178, 222 (regarding an attorney's affirmative duty to explain discovery obligations to a client); *and see Green v. McClendon* (SDNY 2009) 262 FRD 284 (regarding the duty to advise a client of the type of information relevant to the suit and the necessity of preventing its destruction).) It is insufficient to "wait and see" if an opponent might press for e-discovery late in a case. What if its pertinent ESI has, in the interim, been compromised by neglect? Under the Opinion, the answer is that counsel failed his ethical duties and can expect multi-level exposure. (*See also Zubulake v. UBS Warberg LLC* (SDNY 2004) 229 FRD 435.)

Commonly heard pushback includes complaints that many clients cannot financially afford substantial ESI attention and that attorneys want to practice law, not computer forensics.

But properly handling these issues and tasks need not cause heartburn. Rather, a practical and economical standard plan can easily include:

- Screening each incoming new case for ESI/e-discovery issues and tasks as part of the regular intake process – just add a new line to the usual intake checklist;
- Warning new clients through standard letters of the importance of ESI in the modern litigation environment and the need to preserve all hardware (smart phones, computers and other devices) and data while in litigation;
- Assessing clients' personal and business ESI storage systems. This can be as simple as learning whether an individual stores her personal data in a popular telecommunications cloud (icloud, etc.) or more complex, in the case of a businessperson, for instance. In the latter cases, a computer forensics professional can be retained to perform a basic audit, from which further assessments and planning can spring. At our firm, we regularly retain a local forensic who provides clients with no-charge initial audits, which we then use to budget and plan in concert with the client.
- Sending "ESI hold" letters to opposing counsel and then monitoring when it looks like ESI might be an issue. (*See Zubulake, supra*.)

If e-discovery is sought, then the opponent can be requested for an outline of its ESI custodians and systems. If that information is withheld, well-targeted "person(s) most knowledgeable" depositions and motions to compel can be initiated. Once these basics are known, e-discovery can follow. As the Opinion points out, Code of Civil Procedure section 2031.010(a) provides for "copying, testing, or sampling" of "electronically stored information in the possession, custody, or control of any other party to the action."

When ESI is received, it can be economically searched economically through certain proprietary systems. Rather than sifting through figurative "boxes of documents," counsel can efficiently upload and search the data, using keywords, for desired nuggets. This can be done in-house or by retained computer forensics.

If e-discovery is requested *against* a client, then have her assess and search her systems (maybe just a smartphone and a home computer, with cloud or harddrive back-up) in a simple case. In a more complex one, the above audit process with a computer expert is the way to go. Identify and protect confidential information, like business records, through pre-screening, protective orders and other steps where warranted.

Negligence or lack of basic knowledge regarding ESI and e-discovery requirements constitutes professional incompetence. (*Zubulake, supra*.) Formal Opinion No 2015-193 presents a roadmap toward understanding and negotiating this new world.