THE STATE BAR OF CALIFORNIA

FAMILY LAW NEWS

Issue 4, 2017 | Volume 39, No. 4

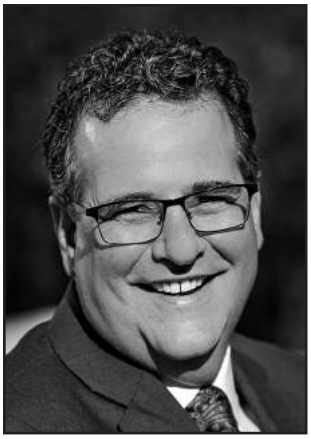
MCLE Article: Emerging Issues in Three Parent Law
By Denise Treviño

The Use of Motions in Family Law
By Dorie A. Rogers, CFLS

The New Divorce By Mutual Consent in France
By Delphine Eskenazi, Carmel Brown, and Jeremy D. Morley

Why ESI Scares Me as a Solo Practitioner

Stephen D. Hamilton



Stephen D. Hamilton has been an attorney for 22 years, with a practice devoted almost exclusively to family law for 20 of those years. He has been a Certified Specialist in Family Law since 2004. He is currently a member of the California Family Law Executive Committee, for which he is the Legislation Chair. He is a member of ACFLS and serves on the ACFLS Outreach and Amicus Committees. He is also chairperson of the San Luis Obispo County Family Law Section.

ESI, or "Electronically Stored Information," frightens me. I am afraid because the California State Bar has told me to be afraid. Each of us has specific, mandatory responsibilities when it comes to identifying, producing and securing our client's ESI. The scope of those responsibilities can be daunting for the solo practitioner.

I am confident I am not alone in my fear. I recently presented "Ten Things You Need to Know about ESI" to the San Luis Obispo County Family Law Section. Midway through my presentation, I noticed concerned looks and ashen faces in the audience. I halted my presentation and asked the attendees what they thought so far of the topic. The most memorable response: "This is scary stuff." On one of the Activity Evaluation Forms, an attendee wrote, "Terrifying."

What is intimidating to me and other solo practitioners is the tremendous amount of responsibility we now have regarding our client's ESI. Understanding what ESI is and what responsibilities we have as counsel are crucial. ESI consists of any information stored electronically, including:

- Computer records and metadata;
- Cell phone data (including voice mails, photographs, text messages and records of telephone calls);
- Electronic mail;
- Accounting data, including bookkeeping program files and banking records;
- Social media; and,
- Digitally stored photographs and videos.

This is by no means an exhaustive list, but one intended to indicate the expansive scope of ESI.

Our current duties as attorneys regarding ESI are set forth in Formal Opinion No. 2015-193 of The State Bar of California Standing Committee on Professional Responsibility and Conduct. That opinion interprets Rules 3-100 and 3-110 of the Rules of Professional Conduct as they apply to electronic data. In summary, Formal Opinion No. 2015-193 concludes that to be competent and satisfy the ethical duties regarding ESI, attorneys must:

1. Have at a minimum a basic understanding of ESI to assess at the outset of each case what electronic discovery issues might arise during the litigation, including the likelihood that e-discovery will or should be sought by either side;
2. Assess your own e-discovery skills and resources to determine if you can competently handle e-discovery in a particular matter; and
3. If you determine you cannot, then you must either try to acquire the skills or resources necessary or associate or consult with someone with expertise to assist.

This assessment should be done on a case-by-case basis and at the beginning of your representation.

Basic ESI competency demands that counsel protect and preserve any relevant ESI and take steps to ensure that opposing counsel and parties do so as well. These requirements are typically satisfied by:

- Notifying your client in writing of the obligation to preserve and maintain any currently existing ESI;
- Sending an ESI hold letter to opposing counsel, requesting that the other party preserve any ESI;
- Informing both your client and the opposing party of the consequences of failing to preserve ESI;
- Meeting not only with your client but also with any persons who may be in control of ESI

(for example, the bookkeeper or CFO for a community-owned business); and

- Meeting and conferring with opposing client early to determine the types of ESI that may be relevant to your case; where the information is stored; who controls the information and passwords; the time span of the data, and in what format the data is stored and will be produced in your case.

All of the above subjects will assist you in preparing a data map. I have attached as an addendum to this article a sample data map prepared by James Schaefer, CPA/CFF [www.shaefercpa.com], which he has graciously agreed to share with the family law bar from his ESI Toolkit.

These obligations are not a one-size-fits-all requirement in each case. The letters, data map and protocols must be tailored to the specific facts of your case. Further, these duties are ongoing. Assessing ESI issues at the onset of the case is not enough. You must periodically confer with your client and others in possession or control of your client's ESI to satisfy your duty to protect and preserve ESI.

Formal Opinion No. 2015-193 is not just limited to e-discovery. It also applies to how we store and protect our clients' ESI within our office. The duty of confidentiality imposed by California Business and Professions code section 6068(e)(1) applies to the client information and files that we maintain in our office. Writing this article days after the Equifax data breach was announced, I am reminded that the very same type of information stolen from Equifax is also stored in our client files within our office. Tax returns, income and expense declarations, bank statements, Schedules of Assets and Debts and interrogatory answers would give a would-be identity thief all of the information they need to take advantage of one of our clients.

The following extended passage from Formal Opinion No. 2015-193 makes clear our responsibilities when it comes to protecting our client's ESI:

> The State Bar Court Review Department has stated, Section 6068, subdivision (e) is the most strongly worded duty binding on a California attorney. It requires the attorney to maintain inviolate the confidence and at every peril to himself or herself preserve the client s secrets. (See Matter of Johnson (Rev. Dept. 2000) 4 Cal. State Bar Ct. Rptr. 179.) While the law does not require perfection by attorneys in acting to protect privileged or confidential information, it requires the exercise of reasonable care. Cal. State Bar Formal Opn. No. 2010-179.

It is left for us as practitioners to determine what is "reasonable care," because Formal Opinion No. 2015-193 offers no specific guidance. In my own practice, and after attending multiple ESI courses since Formal Opinion No. 2015-193 was issued, I have:

- Installed a waterproof, fireproof and locked server in my office;
- Transitioned my web page and email from an offshore discount internet service provider to Microsoft;
- Maintained my network as a hard-wired network (i.e. disabled the wireless function on my office router);
- Disabled remote access to my office computers for technicians (instead, granting them access on a case-by-case basis and only in case of emergencies); and,
- Had my entire network inspected by a computer technician to ensure that I had adequate virus and ransomware protection as well as a safe and periodic backup system.

I am certain there is more that I can do. I am therefore continually evaluating the protection of ESI within my office to ensure that I am meeting my ethical and statutory duties to protect client information.

In conclusion, I leave you with three immediate recommendations:

1. Confirm that your email and any other cloud-based storage of electronic information within your firm is being stored on servers entirely within the United States;
2. Retain a computer consultant to verify that the ESI in your office is backed up and not vulnerable to viruses or hacking; and,
3. Attend as many ESI continuing education seminars as you can to demonstrate to the State Bar, if necessary, that you have taken affirmative steps to be competent and familiar with the handling of ESI.

While following these recommendations by no means satisfies the duties set forth in Formal Opinion No. 2015-193, they are good first steps.

ESI Baseline Toolkit

3. Prepare Data Map

A Data Map is a summary of What, Where and Who:

- **What** information is stored and for **What** time span,
- **Where** is the information stored, and
- **Who** has access to computer files and can make available — including administrative user name and administrative password.

Sample Data Map of ESI Under Husband's Control

What is Stored & What Time Span	Examples of Storage Location	Who Has Access	Native File Formats
1. Accounting system—since inception of company	Server at Company	CFO and accounting personnel—password protected	QuickBooks exportable upon request to Microsoft Excel
2. Spreadsheets—various times and subjects	Server at Company	CFO and accounting personnel—no passwords	Microsoft Excel
3. Social Media	Online	Both Parties	Twitter, Facebook, & YouTube
4. Bank statements—last 10 years	BofA and home computer	Husband—BofA site has password	Internet (pdf)
5. Brokerage statements	Charles Schwab & Merrill Lynch	Husband—password protected	Internet (pdf)
6. Email	Web & Company server	Both Parties—password protected	Microsoft Outlook & Hotmail

1. Gather information for Data Map in your Meet and Confer.
2. Be sure to obtain administrative user names and passwords.

James T. Schaefer, CPA/CFF MS-Tax
Jim@SchaeferCPA.com 909-455-5766