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

Ethical and other Issues Concerning Technology and Your Law Practice

by Gregory W. Herring

As our modern lives are increasingly dominated by e-mails, texts, social media, electronically stored information ("ESI") and related technology, so are our law practices. We have ethical and other obligations toward identifying and handling it all, and a "head in the sand" approach will not cut it. This percolates some ethical and other issues. This also provides practical tips.

E-mails:

E-mails are not (and never were) a secure method of communication. The increasing frequency and sophistication of hacking, spying, phishing schemes, ransomware attacks and internet infiltrations should make this impossible to ignore. Los Angeles lawyer and friend, Steve Kolodny, emphasizes that any e-mail that is sent may be copied and held by the various computers through which it passes as it goes from law office to client or *vice-versa.* E-mails are subject to being accessed or copied by persons innocently or with a hostile agenda.

Based on Steve's early consciousness-raising, our family law firm systematically emphasizes to our clients in writing a wide variety of concerns including the following:[1]

- E-mails may be inadvertently accessed by, or delivered to, persons not intended to participate, nor authorized to being a part of, particular communications.
- E-mails may be intercepted by persons improperly accessing a client's or your law firm's computer, or even some computer unconnected to either through which the e-mail passes.
- By inadvertence, someone may reply to an e-mail and mistakenly include an unauthorized person, even opposing counsel or the opposing party, because of using the "reply to all" feature.

[1] Steve's firm has a standard letter that he generously shares with other attorneys. On request, Herring Law Group would be pleased to share our own modified version. E-mail us at info@theherringlawgroup.

ABA Formal Opinion 477, dated May 2017, provides that law offices should always determine and implement appropriate and measured levels of protection for electronic communications dependent on the particular circumstances involved. "The use of unencrypted routine e-mail generally remains an acceptable method of lawyer-client communication." "However, [because] cyber-threats and the proliferation of electronic communications devices have changed the landscape it is not always reasonable to rely on the use of unencrypted e-mail."

California now requires technical competence. As such, law offices must constantly analyze how they communicate electronically about client matters using a case-by-case method for their decision-making.

The Opinion suggests some considerations as guidance for the law office in the case-by-case analysis about whether to use unsecure or secured electronic communications or some other nonelectronic method of communications about confidential client matters:

- Understand the nature of the threat.
- Understand how client confidential information is transmitted and where it is stored, making sure it is not open to inappropriate access.
- Understand and use reasonable electronic security measures on a case-by-case basis considering the nature of the communication and information contained.
- Determine how electronic communications about client matters should be protected in each instance.
- Appropriately label confidential client information and privileged attorney-client communications.
- Train lawyers and nonlawyer assistants in appropriate technology and information security protocols and practices.
- Conduct regular due diligence reviews on vendors that provide communications technologies for the lawyer, including e-mail, document storage, internet and wi-fi access, and other related services.

Other ways of addressing e-mail concerns include:

- Warn clients through a standard written "personal privacy" memo (see Footnote No. 1).
- Consider "old-fashioned" alternatives including overnight delivery services or direct messengers.
- Investigate and offer encrypted e-mail systems.
- Use encrypted attachment systems for sending confidential documents, like client reports and tax returns. Even if the **e-mail** maybe not be confidential, at least the **attachment** would be. "Dropbox," alone, is not enough without using an associated encryption service. Our office has productively used "Sharefile." We are presently moving to Clio's practice mangagement system, which includes a client portal for encrypted communications at the industry standard. Certainly there are other tools and systems.

Personal e-mails to and from an employer's computer are non-confidential. Tell your clients to set up a new personal e-mail address, and with a nondescript user name.

Texts:

Does your office text with clients? If so, are these communications documented? Do they make their way into the file? The ethereal nature of texts make them particularly problematic. This is especially in the new era of "instantly deleted" texts, for instance through Snapchat and like applications. Either bar the practice or develop methods of systematically downloading them into the file.

Social Media:

Modern lives are increasingly dominated by social media, and managing clients' social media is a major and growing concern. Facebook and like posts constitute potential evidence potentially favoring or else harming your clients' cases. They are non-confidential by definition. Advise your clients to **cease** posting.

But you have an affirmative ethical duty to **preserve** existing posts. The duty is a serious one, with potential consequences including disbarment to attorneys who might advise or otherwise cooperate with spoliation. Immediately advise your clients to refrain from deleting old posts. If posts "must" be deleted, ensure that that they are first preserved by taking "snapshots" through appropriate software. Professional assistance may be appropriate.

ESI:

San Diego attorney, nationally-recognized ESI expert and friend, Gordon Cruse, explains the following:

- ESI is information that is stored in technology having electrical, digital, magnetic, wireless, optical, electromagnetic or similar capabilities. Both users and machines create ESI.
- **Users** create hidden data. Examples include background spreadsheet formulae, and revisions and notations in word processing programs.
- **Machines** create metadata & system level data. "Metadata" is "data regarding data." It is information used by a computer to manage and often classify the origin and other attributes of a computer file. It describes how and when and by whom a particular set of data was collected, and how the data if formatted. It is embedded information that is stored in electronically generated materials, and it is generally not visible when documents or materials are printed.

Sources of ESI include hardware, servers, old-fashioned discs and thumb drives. They also include personal devices including smartphones, tablets and automobile and other navigation systems. E-mails, Dropbox files, word processing files, accounting and billing systems and photo applications are other examples. Security systems (audio and visual recordings), voicemails, home Nest and Alexa systems, as well as other sources, add to the growing list.

Recognize the various sources of ESI. Learn how to **gain** it in litigation through e-discovery. **Maintain** confidential ESI when it is already in hand. What happened to the hard drive full of confidential data in the leased copier/scanner your firm turned in for a replacement?!

Technology outside the Law Office:

Generally, eavesdropping and recording private communications by another person is illegal. Warn your clients regarding hidden cameras, automobile tracking and other means of surveillance. This is reasonably extended to the reading of private e-mail messages/texts/chats and copying of electronic data. California law now extends the definition of "domestic violence" to include the unauthorized downloading and distribution of contents from cell phones and the unauthorized hacking of social media accounts.

Other Practical tips:

- Actively redact sensitive information, like social security and credit card account numbers, from clients' documents before producing them. Use computer technology, like Adobe Acrobat, that avoids transparency.
- Lock all USBs ("thumb drives") that leave your office.
- Use a password security program like Dashlane, OneNote or others. Use it to randomize your password for each account and change your passwords regularly.
- Pro-actively gather historical e-mails and other ESI from prior counsel when substituting into an existing case. Too often, prior counsel lazily refrain from transferring this often difficult-to-organize data. New counsel has an ethical duty to **affirmatively** acquire it. You will not have a complete file and you will not fully understand your new case until and unless you do this. Conversely, your office has an ethical duty to gather and provide such communications and data when transferring out of a case.
- Install a "find your phone" application so that mobile endpoints (cell phones, tablets, computers, etc.) can be retrieved if lost or stolen.
- Beware public Wi-Fi networks (including at coffee houses, hotels, airports and etc.) that can be exploited to steal your laptop's data.
- Calendar regular office privacy and security reviews.
- Sign all the way out of computers and devices including logging out of Remote Desktop and like programs. This includes erasing software log-in credentials after each use.
- Warn clients about security concerns, risks and obligations in writing and pro-actively monitor their ESI preservation efforts at periodic intervals. (See Footnote No. 1.)
- Regularly update your software so that you receive timely "fixes," and also update your anti-virus, anti-malware and other security systems.
- Consider installing an ad-blocker like uBlock Origin to protect against ads that carry malware.
- Consider providing your staff iPhones. Their updated operating systems are now more secure than ever. Even the default mail program's data is encrypted. The new iPhones include safeguards that will automatically wipe the phone if an outsider might probe it. • Work with your merchant services vendor to ensure your office's credit card processes

achieve Payment Card Industry Data Security Standard compliance. Failure to meet PCI standards can result in fines up to $50,000 per incident.

- Train your employees on the proper use of computers and devices and how to recognize threats while on them.
- Retain an ESI consultant, who can be a knowledgeable co-counsel or else a non-attorney vendor, when you might find yourself out-of-depth.

Conclusion:

Consider the issues and angles toward creating your own office policies and practices. These are no longer optional obligations in our rapidly-changing and challenging new world of law practice technology.

Greg Herring is a Certified Family Law Specialist and is the principal of Herring Law Group, a family law firm serving the 805 with offices in Santa Barbara and in Ventura County. He is a Fellow of the American Academy of Matrimonial Lawyers and of the International Academy of Family Lawyers. The AAML's Southern California Chapter named him "Family Law Person of the Year" for 2018. His articles and blog entries are at theherringlawgroup.com.