

Advisor

An update on issues regarding liability protection for the legal profession.



Electronic Discovery is Here! By Retired Circuit Judge Ralph Artigliere & William Hamilton, Esq.

Would you represent a client in a litigated matter without knowing the Rules of Civil Procedure and the Evidence Code? Would you write a letter of engagement in a secured transaction without current knowledge of the applicable statutes and regulations? Of course not. However, many lawyers today are unwittingly taking risks by doing something very similar when representing clients in matters involving electronically stored information (ESI) without a full understanding of electronic discovery and the admissibility of ESI. The line between discovery and eDiscovery has been obliterated by the use of computers and digital devices for creation, modification, communication, and storage of virtually all written and much of the recorded information in business, personal, and government milieus. Much of today's electronic information is created and communicated in an unguarded and unprotected fashion and widely distributed with a vague awareness of the potential consequences. Before the current ESI era, an important business memo or report would likely be highly edited, reviewed by counsel, distributed to a discrete number of individuals, and stored in secure files. Today that same information may be stored electronically in dozens of locations and in a variety of forms with electronic "markers" or riders, called metadata, that secretly contain information about the date and time the document was created, modified, and transmitted, and who created, modified, and received it.

Finding the proverbial "smoking gun" has never been easier than in today's digital world. Key documents are often stored in multiple locations making a systematic and thorough deletion or erasure of such digital data almost

impossible. More to the point, vast amounts of data can be effectively searched provided the right tools are matched to the search project. Lawyers who understand the digital world and the body of procedural, substantive, and professional conduct law that governs discovery and admissibility of ESI better control their own destiny and that of their clients. Those who do not have such knowledge risk substantial downside for their clients, their firms, and themselves. At a minimum, lawyers unfamiliar with the digital-legal arena are dependent on more knowledgeable lawyers or experts as they navigate this area of the law. Such experts may be lawyers and IT personnel in their own firm or they may be IT personnel, consultants, and/or lawyers retained or associated in matters to provide the needed expertise. However, retaining an e-discovery expert is not a simple chore: experts can be expensive and vetting the right expert for the case demands a significant amount up front research and knowledge to understand who to hire for help.

The good news is that while understanding electronic discovery and the admissibility of ESI requires effort and diligence, it is not beyond the keen of everyday practitioners. ESI may be the new "information container," but the principles governing e-discovery and the admissibility of ESI are based largely on existing law that every litigator should already know. With commitment, every lawyer can learn enough about electronic information and evidence to identify e-discovery issues and address them competently, whether during document drafting and transmittal or during contested proceedings where such documents are at issue. However, because of the ubiquity of



computers and digital media, a basic understanding of electronic discovery is not an option for litigation, business, family law, and government attorneys: it is required to practice competently.

Learn About the Digital World

Here is an outline of a process to learn about electronic discovery along with some caveats and warnings regarding pitfalls that can lead to legal malpractice claims. First, lawyers must obtain some basic technical knowledge of digital systems and equipment and learn a new vocabulary sufficient to accurately discuss e-discovery issues with clients, IT personnel, opposing counsel, other attorneys and the court. Understanding digital systems and equipment includes a basic understanding of how digital devices create, store and transmit digital information and how these digital devices are bundled and tied together to create public and private networks, including the Internet. For example, an understanding of email would include how electronic messages are created, stored, modified, and transmitted. Different email software applications appear to operate similarly on the surface, but in fact may have very different and important features. Email within a business network will be transmitted directly to recipients within the system. Emails sent to different companies or domains travel over public Internet. Discovery of email often requires that a search be conducted of the server(s) in which the emails reside. All locations of the “same” relevant email must be identified, and then after identification they must be preserved. Email systems can be designed in numerous ways, and it is difficult to make any statement concerning a “typical” email system. Most email systems are configured to routinely archive or delete messages. Individual “custodians” may have personalized storage and deletion practices that must

be uncovered. In litigation, counsel must understand the client’s computer system, and the computer systems of the opposing party, to conduct and to comply with discovery. Beyond pure discovery ramifications, every lawyer must have a sufficient understanding of email to safely protect client confidentiality and privileges while communicating with others.

How does one become a wise denizen of the digital world? E-discovery lawyers are not born. They are created from diligent effort. But the effort must be properly directed. There is a great deal of information out there. Maintaining an efficient learning track can be challenging. As with any significant learning challenge, systematic learning is best. Obtain reliable resources and establish a plan of learning that suits your schedule, ability, and practice area. Frequently, reliable resources that cover electronic discovery also include ancillary information about digital equipment, software, and systems so that the application of the rule of law to ESI may be understood and applied in practice. See Artigliere & Hamilton, LexisNexis Practice Guide Florida e-Discovery Law and Evidence (LexisNexis Mathew Bender 2011), Ch. 1, Understanding Electronic Evidence and its Role in Florida State Courts. Additionally, there are a number of emerging e-discovery certification and training programs. For example, the Association of Certified E-Discovery Specialists has developed a rigorous psychometric examination and training program. www.aceds.org. The Organization of Legal Professionals offers its own training and certification by distinguished practitioners. www.tholp.org. Ralph Losey’s E-Discovery Team Blog offers a full curriculum of online courses. www.e-discoveryteam.com. Some of the best “best practices” and toolkits are located at The Sedona Conference website. www.thesedonaconference.org and there may be other worthy programs available beyond those mentioned here. Of course, practical training and knowledge is important. Visit the EDRM website for up-to-date information on what is happening on the vendor side of e-discovery. www.edrm.net.

Some Common E-Discovery Errors and Mistakes

Your e-discovery learning adventure will provide a number of eye-popping surprises. For example, many Microsoft Windows® operating systems preserve a record of every Internet website visited by the computer, independent of the Internet browsing history! Obviously, a full e-discovery course and curriculum are beyond this article, but below are a few tips and insights to encourage your journey.

Court Bonds
Anytime...
...Anywhere.
www.florida.onlinecourtbonds.com
Florida Lawyers
INSURANCE AGENCY, INC.
877.553.6376
24/7

2012 Florida Law Student Essay Contest

Co-Sponsored by Florida Lawyers Mutual Insurance Company
& The Florida Bar Young Lawyers Division

Topic: Best Practices for Small Firms and Solo Practitioners to Manage Risk Associated with E-Discovery

Deadline: March 1, 2012 by 5p.m.

- \$500 first prize, \$250 honorable mention prize provided by FLMIC.
- Free admission to ACEDS Annual Conference, April 2-4, 2012, and two nights at the Westin Diplomat, Hollywood, FL, Courtesy of the Association of Certified E-Discovery Specialists.

1. *Protect Confidential Communications*: The protection of privileged, work product, and confidential information is an absolute priority for every attorney. Safeguarding your own communications with the client is the starting point. If you use email or electronic communication as almost every attorney does, you must understand your email system and communications devices (smart phones, blackberries, iphones, etc.) and employ a reasonable, effective methodology to safeguard client communications. For example, counsel should consider disabling features in email programs that anticipate the recipient's address once the attorney begins typing the recipient's name into the email address field. Such "helpful" features make it all too easy to send a privileged email to the wrong party. In the uncomfortable event that an attorney mistakenly discloses (or receives from the opponent) privileged information, it is essential to know the steps that must be taken under current rules, including new Fla. R. Civ. P. 1.285, to recover inadvertently disclosed privileged information.

2. *Inform Your Clients*: Educating the client on safeguarding private information and confidential communications requires knowledge and understanding of the client's systems and procedures. Remember that the client probably does not realize that electronic communications are susceptible to unintended recording, distribution, and automatic storage. An email sent in a moment of anger lasts for an eternity. Instruct your clients on good email etiquette. Clients should also be instructed not to "copy" unnecessary parties on attorney-client communications and of the dangers of forwarding privileged communication. Privilege waiver by unnecessary distribution is a constant threat.

3. *Deletion is often a fiction*: For any electronic document, be it email, word processing document, or other types of ESI, simply "deleting" the file or document does not remove it from the computers and servers that processed the document. In fact, deletion does not even remove the document from the computer on which the "delete" was attempted. In almost all cases, "hitting" delete button on a computer or smart phone simply renames or reassigns the document in a way that it is retrievable only through forensic effort. However, it is likely that the "deleted" document is still accessible, along with metadata that tells among other things how and when the deletion was attempted and by whom, who created the document, and who received it and when. It is easy to see that a client or attorney can intentionally or innocently scuttle a case through lack of understanding digital equipment, software, and systems.

Conclusion

The question is not whether to learn about e-discovery and ESI. The only question is how to go about it. One hour CLE programs on e-discovery and brief articles like this one are only introductions. Learning about ESI requires an assessment of your current knowledge of the area, development of a goal on level of competence you wish to achieve, and a systematic effort to learn what you don't know and need to know. The good news is that it is doable. Start today. ©2011 Ralph Artigliere and Bill Hamilton

Ralph Artigliere is a retired Circuit Judge who teaches e-Discovery and Evidence in the Florida Judicial College and the Florida College of Advanced Judicial Studies.

William Hamilton is a partner in Quarles & Brady, LLP and is Florida Bar Board Certified in Business Litigation and Intellectual Property Law. Mr. Hamilton teaches e-discovery and electronic evidence at the University of Florida Levin College of Law and the Florida College of Advanced Judicial Studies. Mr. Hamilton is the Chairman of the Advisory Board of the Association of Certified E-Discovery Specialists ("ACEDS").

Mr. Artigliere and Mr. Hamilton are co-authors of the LexisNexis Practice Guide Florida e-Discovery Law and Evidence (LexisNexis Mathew Bender 2011) available from LexisNexis or from The Florida Bar.

A FUTURE ISSUE OF THE *ADVISOR* WILL FEATURE AN ARTICLE REGARDING J-M MANUFACTURING COMPANY, INC. V. MCDERMOTT, WILL & EMERY. MCDERMOTT IS THE FIRST LEGAL MALPRACTICE CLAIM FILED CONCERNING THE OUTSOURCING OF E-DISCOVERY WORK.

Mark Your Calendars...

September 8, 2011, FLMIC sponsors the Board of Legal Specialization's Leadership Conference, Orlando

September 8, 2011, FLMIC presentation to the Plant City Bar Association, Plant City

September 22-23, 2011, FLMIC exhibits & sponsors the reception at The Florida Bar's Mid-Year Meeting, Orlando

September 23, 2011, FLMIC sponsors, exhibits & presents at the General Practice, Solo & Small Firm Section's Extraordinary Technology Event

September 30-October 1, 2011, FLMIC exhibits at the Florida Legal Education Association Conference, Orlando

See our website for more information on these and other events

FLORIDA LAWYERS MUTUAL INSURANCE COMPANY (FLMIC) Risk Management services are available to FLMIC policyholders and as a benefit to the legal profession.

This publication is intended to provide general information presented in order to assist lawyers and their staff to develop and enhance firm risk management procedures. For advice on specific legal questions, consult experienced legal counsel; specific questions on ethical conduct may be posed to The Florida Bar's Ethics Hotline, 800-235-8619. Implementation of suggestions in this publication is not warranted, expressed or implied, to prevent claims. This information is not intended to establish a standard of due care; information may describe conduct that is well above the standard of due care. While all materials presented herein are carefully researched, no warranty, expressed or implied, is offered to the accuracy of this information. Reproduction, in any manner, of the material herein requires written permission. For more information, contact Nancy Stuparich, Risk Manager, at nancys@flmic.com.

© 2008 Florida Lawyers Mutual Insurance Co. All rights reserved.

www.flmic.com • Phone 800.633.6458 • Fax: 800-781-2010



541 E. Mitchell Hammock Rd.
Oviedo, Florida 32765

BULK RATE
US POSTAGE
PAID
PERMIT #1365
ORLANDO FL



"We've built our reputation on vigorously defending yours."

Test your E-Discovery IQ

Supplement to “Electronic Discovery is Here!”
by Retired Circuit Judge Ralph Artigliere
& William Hamilton, Esquire in FLMIC’S
3rd Quarter *Advisor* Newsletter



Turn the page for the answers to the following e-discovery questions:

- 1. Your [family][business][employment law] client comes to the office with explosively damaging documents, including emails between the opposing party and the opposing party’s lawyer. The client says she downloaded the documents from a computer formerly shared with the opposing party using a password that the opposing party willingly gave her months before the [marital][business] split that gave rise to the litigation. What are your obligations?*
- 2. You receive an email from the opposing party in conjunction with ongoing litigation with an attached email “string” between the opposing party and his attorney. The email and perhaps some of the attached emails are intended for you, but it is doubtful that the attorney-client emails were intended to be sent to you because of compromising attorney-client information in the emails. What are your obligations?*
- 3. You are preparing a request for production of electronically stored information (ESI) from the opposing party. The request calls for production of emails, word processing documents such as contracts and memoranda, and the relevant content of the opposing party’s principal business website and other social media websites such as Facebook and Twitter. What descriptions are needed in your request to ensure that you obtain all the relevant information for your case and the foundation data to later authenticate and introduce the ESI into evidence? How can you secure and store current information from the website and social media in order to ultimately authenticate and introduce the information into evidence?*
- 4. In your request for production, you asked for the information from the opposing party in native form, but received it in format without metadata. The opposing party says the production is fully compliant in scope and content because the ESI produced is in a reasonably usable, searchable format. What is your responsibility?*
- 5. The opposing party sends a comprehensive document request for the production of ESI. Your client balks at your recommendation to have you and your staff conduct the search, collection, and review of the client’s systems for relevant and responsive ESI. Instead, to save money, the client wants in-house IT and management personnel conduct the work. What is your response?*

Answers to Questions 1-5

1. Answer: Investigate thoroughly before reviewing the information to assure legal access to the ESI to avoid disqualification. Make sure any review screens out any potential privileged information. Seek court guidance in gray or doubtful circumstances. See *Castellano v. Winthrop*, 27 So. 3d 134, 137 (Fla. 5th DCA 2010)(where a client misappropriated a flash drive full of confidential and privileged documents and gave it to her attorneys who spent hundreds of hours reviewing the documents and preparing pleadings based on the content of the documents, disqualification of counsel, while an extraordinary remedy that should be used sparingly, was the only appropriate civil remedy to offset the unfair informational or tactical advantage gained by the wrongdoing and disclosure to counsel); *Minakan v. Husted*, 27 So. 3d 695, 700 (Fla.4th DCA 2010)(order disqualifying attorney reversed where wife was not permitted to testify concerning the lack of safeguards as to privileged information on the part of the husband).

2. Answer: An attorney who receives confidential documents of an adversary as a result of an inadvertent release is ethically obligated to promptly notify the sender of the attorney's receipt of the documents. See Fla. Ethics Op. 93-3; Fla. R. Prof. Cond. 4-4.4(b)("[a] lawyer who receives a document relating to the representation of the lawyer's client and knows or reasonably should know that the document was inadvertently sent shall promptly notify the sender."); *Applied Digital Solutions, Inc. v. Vasa*, 941 So. 2d 404 (Fla. 4th DCA 2006) (automatic disqualification is not required every time an attorney inadvertently receives privileged documents; but instead, in deciding a motion for disqualification, the court should consider whether the party receiving the privileged material actually obtained an unfair advantage). Note: This pertains to information in the content of the email. Metadata is another matter. When a Florida lawyer receives a communication from another lawyer that contains metadata, the receiving lawyer is ethically prohibited from mining the metadata because it is an "unintended" communication. See Fla. Ethics Op. 06-2.

3. Answer: Because information on websites and social media is dynamic and subject to constant change, access and copy ("download") the ESI publicly available from social media and website before requesting it in discovery and employ software tools to constantly monitor the websites for changes; request that the opposition preserve the initial native copy of the websites and all incremental changes; safely secure the downloaded information; hash it (hashing assigns a unique number to the file downloaded); and store it in a manner to secure chain of custody. If you do not know how to do this, obtain expert assistance, assuming the information is important to the case.

4. Answer: Metadata is discoverable if it contains relevant information. Ask for the ESI to be reproduced in native form with the metadata intact or request the metadata in a searchable format in a load file relating the metadata to the image file or the extracted original searchable text you have received. If it is not forthcoming, file a motion to compel. Notify the producing party that preservation of the documents with metadata intact is required and that destruction of metadata will be regarded as spoliation. Removing or scrubbing metadata may unreasonably exclude discoverable information. See, e.g., *Bray & Gillespie Mgmt. LLC v. Lexington Ins. Co.*, 2009 US Dist LEXIS 21250 (M.D. Fla. Mar. 4, 2009)(sanctions for producing in TIFF only when metadata was requested).

5. Answer: Ensure that preservation, search, and collection are done properly. If the client has the resources and motivation to properly conduct the work, it is possible to let the client do it. However, spoliation or inadequate search and production, or both, can result in sanctions against client and counsel. How much do you trust the client with your reputation? Interview the IT Department employees responsible for the tasks, supervise and check the work, and make sure you are conversant with their efforts to be able to accurately explain and defend the e-discovery work to the court. Demand a preservation, collection, search, review and production project plan for your approval before implementation by the client. Make sure that: (i) the client has the skill sets, experience, and resources to accomplish all tasks; (ii) the client identifies a capable project manager for discovery who may be required to testify in court regarding the e-discovery tasks; and (iii) the client understands the potential consequences of spoliation of relevant data. See *Artigliere and Hamilton, LexisNexis Practice Guide Florida e-Discovery Law and Evidence*, § 9.04 Assessment of Client and Potential E-Discovery Team (LexisNexis Mathew Bender 2011).

Ralph Artigliere is a retired Circuit Judge who teaches e-Discovery and Evidence in the Florida Judicial College and the Florida College of Advanced Judicial Studies. **William Hamilton** is a partner in Quarles & Brady, LLP and is Florida Bar Board Certified in Business Litigation and Intellectual Property Law. Mr. Hamilton teaches e-discovery and electronic evidence at the University of Florida Levin College of Law and the Florida College of Advanced Judicial Studies. Mr. Hamilton is the Chairman of the Advisory Board of the Association of Certified E-Discovery Specialists. Mr. Artigliere and Mr. Hamilton are co-authors of the *LexisNexis Practice Guide Florida e-Discovery Law and Evidence* (LexisNexis Mathew Bender 2011) available from LexisNexis or from The Florida Bar. ©2011 Ralph Artigliere and William Hamilton.



"We've built our reputation on vigorously defending yours."