Bloomberg BNA

Digital Discovery & e-Evidence®

Professional Responsibility

The authors update their popular article from 2015 (15 DDEE 134, 4/2/15) to remind litigators about their current obligations to understand the benefits and risks associated with technology when they represent clients in litigation, investigations and dispute resolution.

Competence With Electronically Stored Information: What Does It Currently Mean In the Context of Litigation and How Can Attorneys Achieve It?

BY RONALD J. HEDGES AND AMY WALKER WAGNER

Competence is the fundamental principle upon which an attorney's obligations to her client are based.

Rule 1.1 of the American Bar Association's Model Rules of Professional Conduct provides:

> ''A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.'' [1]

Attorneys should develop this competence in order to meet their ethical obligations to clients and potential clients.

In addition, an attorney has ethical obligations to third parties, such as adversaries, witnesses, jurors and the courts. [2]

As the world has changed, so too has the definition of competence, and attorneys are required to keep pace with the evolution.[3] Practitioners, rule makers, ethics tribunals and the courts have acknowledged the significant impact of technology on the practice of law.

For example, The American Bar Association has explicitly recognized, in a revised comment to Rule 1.1, that an attorney's obligation to be competent includes the obligation to ''keep abreast of changes in the law and its practice'' and understand ''the benefits and risks associated with relevant technology.'' [4]

The purpose of this article is update litigators about the obligations of attorneys involved in litigation, inves-

Ronald J. Hedges is Senior Counsel at Dentons, where he is a member of the Litigation and Dispute Resolution practice group. He has extensive experience in eDiscovery and in the management of complex litigation and has served as a special master, arbitrator and mediator. He also consults on management and discovery of electronically stored information.

Amy Walker Wagner is a partner at Stone & Magnanini LLP, Berkeley Heights, New Jersey. She focuses her practice on False Claims Act, complex commercial, and intellectual property litigation.

[1] ABA Model Rules of Prof'l Conduct (hereinafter cited as MRPC), Rule 1.1 (2010).

[2] *See, e.g.*, MRPC 3.3 (Candor Toward the Tribunal); 3.4 (Fairness to Opposing Party & Counsel).

[3] MRPC 1.1 cmt. 6 (2012 revision) (''[t]o maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.''

[4] *See id.*

 ISSN 1941-3882

tigations, and dispute resolution [5] to understand the benefits and risks associated with technology. This article should encourage attorneys representing a client in any of those arenas to consider their proficiency with the specific technology applicable to the engagement.

If an attorney is not competent to provide the counsel required in light of the technology involved, she should seek competent assistance, refer the matter to another attorney or decline the representation. An attorney should not blindly use technology in which she has no level of competence.

Competence Fundamentals

In order to be competent when investigating and using relevant technology and electronic data, an attorney must recognize that this endeavor implicates issues of law, technology, privacy and security.

Decisions about technology can materially impact the cost, course and context of litigation (including the ability to ensure that data is not inappropriately altered, to present evidence to support the claims and defenses at issue in the matter, to meet court or other deadlines for the production of data, and to comply with legal and ethical obligations to protect the data at issue).

These considerations require an attorney to evaluate, recommend or implement appropriate decisions regarding technology and electronic data. Attorneys should understand basic technological terminology and know where to search for additional information and continuing education. [6]

All Discovery is eDiscovery. The obligation to ensure competence in evaluating, recommending and implementing appropriate decisions regarding technology and electronic data is overarching in a practice focused upon litigation, dispute resolution, investigations and regulatory inquiries.

Virtually all evidence that supports an alleged claim, regulatory violation or defense will be electronic in nature and will require an understanding of technology.

It is no longer credible for an attorney to contend that her practice does not involve the collection, review, production or receipt of electronically stored information (ESI).

The Matter Defines the Competence Required. While all attorneys should be competent to discuss, manage and determine strategy related to the discovery of ESI, the ESI at issue in a particular matter will dictate the level of sophistication required in order to be competent.

For example, attorneys involved in a single-plaintiff employment discrimination case that involves only ESI stored on a single computer, with no web-based, network, structured, or backup data of any kind will demand a less detailed understanding of the discovery of ESI than a complex securities fraud matter with sophisticated entities on both sides.

[5] This article does not address the technological competence associated with the practice of transactional law or law firm management (*e.g.*, document management, timekeeping, mobile computing and information security).

[6] *See*, *e.g.*, The Sedona Conference® Glossary: E-Discovery & Digital Information Management (Fourth Edition April 2014).

The Impact of the 2015 Amendments to the Federal Rules of Civil Procedure.

On December 1, 2015 the Federal Rules of Civil Procedure were amended. Given the fragility of ESI and technology, the specific references to preservation and Fed. R. Evid. 502 agreements underscore the need for federal litigators to be competent with technology. [7]

In addition, the explicit reference to cooperation in the Advisory Committee Note to amended Rule 1 suggests that attorneys need to engage in a cooperative attempt to reduce costs and delays in litigation, which necessarily implicates the need to discuss ESI.

The Need to Understand Technological Issues to Negotiate Scope of Discovery

Civil discovery is a cooperative, iterative process. An attorney's obligation to be competent includes the obligation to cooperatively conduct discovery in civil litigation. Such cooperation includes the disclosure of sources of potentially relevant ESI.

To be competent, an attorney should be aware of the rules and law that provide the framework for reasonable and proportional discovery.

An attorney should understand and be able to describe the sources and characteristics of potentially relevant ESI, both in her client's possession, custody or control, as well as data in the possession, custody or control of her adversary and third parties.

Furthermore, an attorney should be capable of understanding the burden—financial, temporal and otherwise—associated with the preservation, collection, review and production of particular sources of ESI, both for her client's own data and that of her adversaries and third parties.

To be competent, an attorney should be able to engage in a cooperative discussion about the scope of discovery in a particular lawsuit, including:

- The law applicable to the discovery of ESI, including the applicable rules of civil procedure and evidence, as well as common law;

- Any requirements with respect to the discovery of ESI set forth by the tribunal in which the attorney is representing the client (e.g., a model electronic discovery order endorsed by the district court in which the case is pending, a standing order related to the production of ESI entered by the judge before whom the case is pending, rules applicable to the alternative dispute resolution forum in which the case is pending);

- Any other guidance with respect to the discovery of ESI that is significant in the tribunal in which the attorney is representing the client (e.g., electronic discovery principles or guidelines adopted by the court in which the case is pending);

- As discussed in more detail below, how to identify and explain the potentially relevant ESI in the possession, custody and control of her client, including ESI in the possession of third parties that may be deemed to be under her client's control;

[7] *See* Fed. R. Civ. P. 16(b)(3)(B) and 26(f)(3).

  DDEE ISSN 1941-3882

■ As discussed in more detail below, how to request and identify potentially relevant ESI in the possession, custody, and control of the opposing party, including data in the possession of third parties that may be deemed to be under the opposing party's control;

■ How to craft, explain, negotiate and direct the strategy for the culling of the ESI to be discovered in the case, including specifically:

§ Whether a targeted search will be conducted;

§ Whether technology assisted review will be used, including:

§ Whether key word searching will be used, including:

■ To what fields such key words will be applied,

■ What particular key word syntax is used by the tool to conduct the searches, and

■ Whether there are any limitations to the tool used to conduct the searches (i.e., it lacks the capability to search attachments to e-mails).

■ How to craft, explain, negotiate and direct the format of production of the ESI to be discovered in the case, including specifically:

§ Whether any file formats of ESI are to be excluded from discovery;

§ The file format in which to produce ESI, including whether to produce in native or static format, or some combination of the two;

§ The potential need for redacting documents, and ensuring the efficacy of those redactions;

§ The handling of native file and production metadata for her client's and the opposing party's ESI, including:

■ The metadata fields available in her client's ESI;

■ The metadata fields to be produced to the opposing party; and

■ The metadata fields that may be available in the opposing party's ESI and those to be produced to her client.

Competence and Technological Issues Associated With Identification of Relevant ESI

A critical step of the process is identifying potentially relevant ESI. An attorney should know what constitutes ESI and electronic locations where potentially relevant ESI can be found.

An attorney should be capable of investigating the potentially relevant sources of ESI in the possession, custody and control of her client. In addition, an attorney should be able to assess the potentially relevant sources of ESI in the possession, custody and control of the opposing party.

An attorney should understand the right questions to pose, both to her client and the opposing party, as well as the information provided in response to those inquiries. As discussed in more detail below, an attorney also should be able to assess and comprehend the significance of the retention of potentially relevant ESI.

To be competent, an attorney should be able to identify potentially relevant ESI, including understanding:

■ The types of potentially relevant ESI in her client's possession, custody and control, including specifically:

§ Is there a document retention or destruction policy and how is it implemented?

§ What is the e-mail system in use currently and historically?

§ What are the implications, if any, on the availability of potentially relevant e-mail?

§ What non-e-mail sources of communication does the client allow (e.g., instant messaging application, text messages, etc.)?

§ What are the potential repositories of ''loose files'' (i.e., files not attached to an e-mail)?

§ What databases or structured data does the client maintain or access that may contain potentially relevant ESI (e.g., accounting, human resources, sales or customer relationship manager applications)?

§ What web-based sources of potentially relevant ESI exist?

§ What potentially relevant ESI, if any, is contained on users' computers or mobile devices?

§ What potentially relevant ESI, if any, is contained on a network or shared drive?

§ Are there any legacy systems, databases or repositories that may contain potentially relevant ESI?

§ What kind of data back-ups are created, at what intervals, for how long are they retained, and what information is contained?

§ What kind of newly developed technologies (e.g., wearable technology, telemetry) may be at issue in the case?

§ What kind of data may be in the possession of third parties that may be under her client's control?

■ How to request and identify the types of potentially relevant ESI in the opposing party's possession, custody and control; and

■ How to identify the employees and other users currently or formerly associated with the client that may have created, accessed or saved potentially relevant ESI.

Competence and Technological Issues Associated With Preservation of Relevant ESI

Common law has long recognized the obligation of a party or potential party to preserve evidence that may be relevant to a dispute.

The digitization of life in the 21st century through ever-evolving technology including e-mails, instant messaging, personal computing, file sharing servers, databases, web-based content, mobile applications and hundreds of other categories of ESI emphasizes the need for early action to ensure preservation of poten-

tially relevant data. Depending on the type of ESI and the repository in which the ESI is stored, it may be inadvertently and permanently lost.

An attorney responsible for the discovery of ESI should understand the technological characteristics and preservation implications of the potentially relevant ESI at issue in the case.

The sometimes protracted nature of litigation may exacerbate these concerns, as litigation often addresses events that occurred many years in the past, and discovery of that evidence does not occur until yet more time has passed.

To be competent, an attorney should be able to recommend sound preservation strategies for potentially relevant ESI, including understanding:

■ The implications of the length of time for which data is retained by her client or the opposing party, such as:

§ Whether an internet or cellular service provider automatically deletes logs of text messages after a particular amount of time;

§ Whether a web-based storage site automatically deletes files after a particular amount of time;

§ Whether a call center retains tapes or digital recordings of calls for a particular amount of time.

■ Any automatic overwriting of data applicable to potentially relevant sources of ESI, such as:

§ Whether a corporation overwrites media containing backups of active data on a particular schedule;

§ Whether an individual overwrites data saved to her computer when she upgrades her operating system to a new version.

■ The procedures in place for data and devices used by an employee or other user who has left a corporate client, including:

§ The disposition of a former user's e-mail account;

§ The disposition of a former user's computer;

§ The disposition of a former user's smart phone;

§ The disposition of a former user's personal network drive;

§ The disposition of a former user's files saved to a shared drive.

■ How to communicate the need to preserve potentially relevant ESI to those individuals with the ability to ensure that preservation, including:

§ Whether to communicate a request that an individual with potentially relevant data preserve that ESI (a ''Litigation Hold'');

§ Whether anyone other than the individuals who have created or accessed the potentially relevant ESI must receive notice of the Litigation Hold, such as:

■ The corporation's Information Technology staff who must turn off any automatic e-mail deletion procedures applicable to a user's account;

■ Human Resources staff who receive notice of an employee's termination and set in motion a series of events that deletes the now former employee's ESI;

■ The corporation's Marketing staff who has the ability to access and modify content on the corporation's eCommerce site; and

■ The spouse or other associates of a client who access, use and have the ability to delete files contained on the computer that contains the potentially relevant ESI.

■ Ensuring that recipients of a Litigation Hold are complying with the hold by periodically reminding them of the need to preserve evidence;

■ The ability of the method of preservation to ensure the security of the potentially relevant ESI at issue, such as:

§ Ensuring there are no automatic deletions applicable to an e-mail account that houses e-mails you have instructed be preserved;

§ Understanding whether other users can unintentionally modify files saved to a shared drive that are to be preserved.

■ When and how a client can cease the preservation of potentially relevant ESI.

Competence and the Technological Issues Associated With Collection of Relevant ESI

ESI resides on many platforms. For example, a single user may have e-mail data:

■ In her active e-mail mailbox housed on her employer's exchange server,

■ In archive files she created on her laptop;

■ In an application on her smartphone;

■ Saved to a thumb drive;

■ Saved to a firewall repository that makes a copy of any incoming e-mail containing particular suspicious phrases or attachments;

■ In a journaling system implemented by her employer; and

■ Saved to a backup tape.

To be competent, an attorney should be able to assess locations are the best sources for the relevant ESI sought.

In addition, the way in which potentially relevant ESI is collected may impact the utility of that data.

For example, if a loose file is opened or copied during the collection process, certain of the metadata fields (like time and date-stamps and last user) associated with the file may be altered, which may have implications on the facts that can be demonstrated by the use of the file.

The facts of each engagement, the types of potentially relevant ESI, and the facts to be proven by the use of evidence will dictate what method of collection should be used.

To be competent, an attorney should be able to thoughtfully recommend collection strategies for potentially relevant ESI, including an understanding of:

■ The ways ESI may be collected, taking into account whether the collection method will alter evidence

  DDEE ISSN 1941-3882

in any manner and whether that alteration will be material;

■ The implications of the collection method on the issues in dispute in the matter, including:

§ An assessment of what data may be altered as a result of the collection method and ensuring the method of collection will not prevent the parties from discovering material facts, such as:

■ Whether the information available in various metadata fields (such as the date on which a file was created, the author of a file, and the file path of a document) may be relevant.

■ Whether a targeted collection (i.e., where potentially relevant ESI is collected from only particular locations) would be appropriate under the circumstances;

■ Whether a custodian-directed collection (i.e., where the individuals with knowledge search their own files for potentially relevant ESI) would be appropriate under the circumstances;

■ Whether a forensic collection (i.e., a complete bit-by-bit image of the machine that may include deleted content still available on the computer) would be appropriate under the circumstances;

■ Whether a particular searching technology has the capability to search data in the way in which a party has represented, such as whether a searching tool can search the content of e-mails and attachments, or whether a file searching tool can search the filename and the content of the file;

■ Whether the syntax used to conduct a key word search is appropriately drafted for the tool the attorney is using to conduct the search.

■ Whether the sources from which you are collecting are complete yet tailored to the potentially relevant ESI at issue, including:

§ Whether there is a need to collect data from a computer if all potentially relevant ESI is stored on a network server;

§ Whether there is a need to collect data from individual users' e-mail accounts when a corporation maintains a journaling system from which all e-mails can be collected.

Competence and the Technological Issues Associated With Hiring Service Providers

Many lawyers and clients partner with service providers to assist with the discovery of ESI.

An attorney is responsible for the conduct of a service provider or non-lawyer working under her supervision.[8]

Accordingly, an attorney should ensure that a service provider she retains to assist with the discovery of ESI is competent to undertake the tasks assigned, and to ensure compliance with the attorneys' other ethical obligations, such as protection of confidential client data [9] and adversaries' data.[10] The tools used by service providers vary significantly in their functionality, sophistication, and cost.

To be competent in the retention of service providers, an attorney should be capable of undertaking a reasonable investigation of the tools and services that will be provided by the service provider, testing the service provider's skills and maintaining sufficient supervision over the service providers' work, including an understanding of:

■ The service provider's experience in providing the service and tools sought;

■ The service provider's capacity to provide the service and tools sought;

■ The pricing structure imposed by the service provider;

■ The geographic location where the service provider will process and host the client or opposing party data collected, if any, and related implications, such as:

§ Whether the service provider will be transferring data to a different jurisdiction that could cause the client to violate an agreement or the law, or impact the client's ability to obtain the data at a later time;

■ The security applied by the service provider to the data;

■ The period of time for which the service provider will retain the data;

■ The service provider's ability to use the data for any other purpose.

Competence and Technological Issues Associated With Review And Production of Relevant ESI

Technology has allowed attorneys to become increasingly sophisticated in their review of potentially relevant data.

---

[8] *See* MRPC 5.3.
[9] *See* MRPC 1.6.
[10] *See* MRPC 3.4.

Among the various technological methods available to attorneys for narrowing the potentially relevant data are de-duplication, near duplication and e-mail threading.

Attorneys can also rely on certain types of technology assisted review to identify potentially responsive documents. Attorneys can use keyword searches and leverage metadata fields to assist in identifying particularly sensitive or potentially privileged communications.

To be competent in reviewing and producing potentially relevant ESI, an attorney should understand:

- The value of entering into formal agreements or orders regarding the preservation, identification and production of ESI;
- The value of entering into a claw-back or quick peek agreement;
- The methods of ensuring that privileged communications and attorney work product, including information embedded in metadata, are not inadvertently produced;[11]
- The law applicable to the production of protected data;
- The capabilities of the review tool used;
- The ways in which to use the technology to achieve the goals sought;
- The methods for using keyword searching and an understanding of its limitations;
- The methods for filtering metadata by custodian, date range, sender, receiver and file type;
- How to use de-duplication, near duplication and e-mail threading to reduce the overall size of the dataset;
- Whether there are any restrictions or limitations on the data to be searched and produced (e.g., encryption, password protection, legacy data); and
- The precedential case law regarding the use of advanced search techniques beyond key word searches (e.g., predictive coding, machine learning, concept clustering, other advanced culling and analytics tools).

Competence and Technological Experience Of Co-Counsel, Consultants, Experts and Scope of Their Work

Many attorneys participate in litigation with the assistance of co-counsel. In addition, attorneys retain consultants and experts to assist with litigation.

It is critical for attorneys to remember that, at the end of the day, they are accountable for the litigation and the resulting consequences that could arise as a result of delegating work to others, such as co-counsel, experts and consultants.

Similarly, it is critical for the attorney to understand the technological sophistication of their co-counsel and consultants/experts before any work is delegated or shared.

To be competent in working with co-counsel and consultants/experts, an attorney should:

- Understand the responsibility of co-counsel and consultants/experts;
- Understand the technological experience of co-counsel and consultants/experts;
- Confirm that client data is being stored and transmitted securely;
- Confirm that confidentiality protections are being maintained;
- Ensure that confidentiality agreements and protective orders are implemented and followed;
- Keep well-informed of the discovery process and supervise decisions; and
- Understand, at least generally, any technology that is the focus of an expert's opinion or advice.

Competence and Technological Issues Associated With Investigating and Communicating With Witnesses, Unrepresented Parties, Jurors and Courts

Attorneys should learn and follow the jurisdiction's limitations and requirements concerning the use of electronic resources (*e.g.*, text messages, search engines, commercial services like Bloomberg Law, Lexis and Westlaw, social media, online directories, websites, etc.) in investigating and communicating with witnesses, unrepresented parties and prospective or empaneled jurors.

To be competent in using technology to investigate or communicate with witnesses, unrepresented parties and prospective or empaneled jurors, an attorney should understand:

- The restrictions on the use of electronic resources for the investigation of witnesses and jurors;
- The reliability, credibility and accuracy of the electronic resources used for the investigation;
- The applicable jurisdiction's rules and ethics opinions governing the use of internet resources and communications through social media;
- The technological implications of the electronic resources used to investigate and communicate with witnesses;
- The applicable jurisdiction's ethics principles governing honesty and candor in communications with witnesses and jurors, such as the prohibition against the use of deception; and
- The obligation to ethically and appropriately employ technological resources to diligently and competently investigate publicly available information, which will advance her client's case.

Similarly, attorneys should know the applicable jurisdiction's court rules, the judge's preferences and/or standing orders and any precedential ethics opinions that address limitations on communications with the court.

[11] *See* MRPC 4.4(b).

  DDEE ISSN 1941-3882

Just as with traditional means of communications, communications through an electronic medium (*e.g.*, e-mail, text messages, social media, and/or other means of electronic communication) can also raise ethical issues about the propriety of the communication and whether it is an inappropriate *ex parte* communication.

While some jurisdictions might not prevent a judge from being ''friends'' on social media with an attorney that appears before her, a competent attorney will be careful to avoid creating an appearance of impropriety or suggest that the attorney has special access to the judge through their status as ''friends'' on social media.

A competent attorney who is a ''friend'' of a judge on social media will also avoid posting any commentary on matters pending before the judge.

Competence and Technological Issues Associated With Docketing and Filing Documents with the Courts

Filing documents with the court is another method of communication with the court. Competent attorneys should be educated about their court's electronic filing requirements and procedures for filing documents.

Attorneys should also understand their court's requirements for electronic filing and measures to take to protect confidential or privileged information.

RESOURCES

Discovery and Preservation

Cases

Root v. Balfour Beatty Constr. LLC, 2014 BL 30389, 132 So.3d 867 (Fla. Dist. Ct. App. 2014) (unpublished) (on interlocutory appeal, quashing discovery order in part absent showing that postings where relevant and admissible).

Allied Concrete Co. v. Lester, 736 S.E.2d 699 (Va. Sup. Ct. 2013) (improperly authorizing the deletion of Facebook photos).

Ellis v. Toshiba Am. Info. Sys., Inc., 2013 BL 217672, 160 Cal.Rptr.3d 557 (Cal. Ct. App. 2013) (''At the hearing, Sklar's counsel stated: 'I don't even know what ''native format'' means.' The court responded: 'You'll have to find out. I know. Apparently [Toshiba's counsel] knows. You're going to have to get educated in the world of. . .electronic discovery. ESI. . .is here to stay, and these are terms you're just going to have to learn.' '').

State v. Scoles, 69 A.3d 559, 2013 BL 155540, 214 N.J. 236 (N.J. 2013) (demands level of ''ESI competence'' in context of child pornography prosecution).

Giacchetto v. Patchogue-Medford Union Free School Dist., 2013 BL 175080 (E.D.N.Y. 2013) (directing plaintiff counsel to review postings and determine relevance).

Keller v. National Farmers Union Prop. & Cas. Co., 2013 BL 611 (D. Mont. Jan. 2, 2013) (denying access to private portions of social media cite absent threshold showing of need based on content of public portions).

Howell v. Buckeye Ranch Inc., 2012 BL 258589 (S.D. Ohio2012) (directing defendants to serve discovery requests that seek relevant information; plaintiff's counsel may access private portions of social media accounts and provide responses).

Robinson v. Jones Lang LaSalle Americas Inc., 2012 BL 223650 (D. Or. 2012) (allowing discovery of, among other things, plaintiff's e-mail and text messages as well as her ''social media content'').

In re Miles Taylor, 655 F.3d 274 (3d Cir. 2011) (Rule 11 and data generated from automated database).

In re Fannie Mae Sec. Litig., 552 F.3d 814 (D.C. Cir. 2009) (consequences of agreement).

Smith v. Café Asia, 246 F.R.D. 19 (D.D.C. 2007) (plaintiff ordered to produce graphic images stored on mobile phone).

Zubulake v. UBS Warburg (''Zubulake V''), 229 F.R.D. 422 (S.D.N.Y. 2004) (counsel has ongoing duty to monitor preservation and collection efforts).

Ethics Opinions

California State Bar Standing Committee on Professional Responsibility and Conduct, Formal Opinion No. 2015-193 (June 30, 2015) (answering the question about ''What are an attorney's ethical duties in the handling of discovery of electronically stored information?'').

Kenneth Paul Reisman, Public Reprimand No. 2013-21 (Mass. Bd. of Bar Overseers Oct. 9, 2013) (attorney ordered to attend e-discovery and ethics CLEs for failure to put client on notice of preservation obligations, for permitting client to delete non-relevant files, and for being inexperienced in e-discovery).

NYCLA Ethics Op. 745 (July 2, 2013) (''Advising a Client Regarding Posts on Social Media Sites'').

Secondary Sources

Robert Ambrogi, ''Add Two More States To Those That Have Adopted Duty of Technology Competence,'' Law Sites Blog (Dec. 23, 2015) (noting that Iowa and Utah adopted the duty of technology competence rule).

Robert Ambrogi, ''Two More States Adopt Duty of Technology Competence,'' Law Sites Blog (Nov. 11, 2015) (noting that New York and New Hampshire adopted the duty of technology competence rule).

The Florida Bar Best Practices for Effective Electronic Communication (Aug. 7, 2015).

General Recommendation 5 for Judges, *The Sedona Conference® Cooperation Proclamation Resources for the Judiciary* 9 (Feb. 2014 ed.) (''. . . at a minimum, an attorney should understand how to reasonably ensure client confidences when using e-mail. Moreover, an attorney should understand when she needs the assistance of an eDiscovery consultant.'')

J. Poje, ''What Matters? Knowing What To Know About Technology,'' *Your ABA* (ABA Legal Tech. Resource Ctr. May 2013).

B. Deitch, ''How to Access Data from a Party's Facebook Profile,'' *ABA Section of Litigation, Technology for the Litigator* (Oct. 23, 2012).

''The Sedona Conference® 'Jumpstart Outline': Questions to Ask Your Client & Adversary to Prepare for

Preservation, Rule 26 Obligations, Court Conferences & Requests for Production'' (Mar. 2011).

Duty to Supervise

Cases

Lawlor v. North American Corp. of Illinois, 983 N.E.2d 414 (Ill.2012) (corporation was vicariously liable for the tort of intrusion upon seclusion as the principal of the investigator).

Ethics Opinions

District of Columbia Bar Ethics Opinion No. 362 (June 30, 2012) (final staffing selections and the supervision of document review attorneys' work must be performed by an attorney).

District of Columbia Ct. of App. Comm. on the Unauthorized Practice of Law Op. 21-12 (Jan. 12, 2012) (''Applicability of Rule 49 to Discovery Service Companies'').

ABA Standing Comm. on Ethics and Prof. Resp. Formal Op. 08-451 (Aug. 5, 2008) (''The challenge for an outsourcing lawyer is . . . to ensure that tasks are delegated to individuals who are competent to perform them, and then to oversee the execution of the project adequately and appropriately).

Secondary Sources

Robert Hilson, ''Five Ways to Avoid Getting Sued for Discovery Malpractice,'' The Florida Bar Journal (Jan. 2016).

Charles R. Ragan and Eric P. Mandel, ''Ostriches Beware: E-Discovery Ethics In Social Media,'' Law360 (July 13, 2015) (''the attorney responsible for the litigation cannot simply lateral the e-discovery responsibility off to others.'').

Data Mining

Cases

Stengart v. Loving Care Agency, Inc., 201 N.J. 300 (2010) (addressing an employer's use of e-mails obtained through a forensic analysis of a former employee's hard drive on a company laptop).

Liebeskind v. Rutgers Univ., 2015 BL 65262 (N.J. Super. App. Div. Jan. 22, 2015) (public employer utilized software to create a report of plaintiff's internet browsing history to demonstrate time spent on non-work-related internet sites, which the court factually distinguished from *Stengart v. Loving Care Agency*).

Ethics Opinions

''*Metadata Ethics Opinions Around the U.S.*,'' ABA Legal Technology Resource Center.

Mississippi Bar, Ethics Op. No. 259 (Nov. 22, 2012) (Lawyer cannot actively search for confidential metadata received from another attorney).

Maryland State Bar Ass'n Comm. on Ethics, No. 2007-09 (2007) (MD has no analogue to Rule 4.4(b) and concluded that their RPCs do not require the receiving attorney to notify the sending attorney of an inadvertent transmittal of information).

Pennsylvania Bar Ass'n Comm. on Leg. Ethics and Prof'l Resp., Formal Op. 2007-500 (identified a list of factors an attorney should consider before using metadata contained in an adversary's document).

Florida Bar Prof. Ethics, Op. 06-2 (Sept. 2006) (avoid mining non-discovery documents and notify adversary upon discovery of inadvertently sent metadata).

ABA Formal Op. 06-442 (Aug. 5, 2006) (duty to notify sender of inadvertent transmittal of information, but no ethical restriction on mining and using embedded data).

New York State Bar Ass'n Comm. on Prof. Ethics, Op. No. 749 (Dec. 2001) and Op. No. 782 (Dec. 2004) (reasonable care required to prevent disclosure of metadata).

Secondary Sources

''The Sedona Conference® Commentary on Ethics & Metadata,'' 14 *Sedona Conf. J.* 169 (2012).

Protecting Work Product and Privilege

Cases

Stinson v. City of N.Y., 2014 BL 284883 (S.D.N.Y.2014) (requiring the return of the documents, but permitting the receiving party to rely on material learned to challenge privilege claims in a case without a claw-back type agreement).

Lund v. Myers, 232 Ariz. 309 (Sup. Ct. 2013) (*en banc*) (establishing procedure for *in camera* review of contested documents).

Massachusetts Mut. Life Ins. Co. v. Merrill Lynch, Pierce, Fenner & Smith, Inc., Civil Action No. 2011-30285-PBS (D. Mass. Sept. 23, 2013) (addressing when undisclosed communications must be turned over under FRE 502(a)).

BNP Paribas Mortg. Corp. v. Bank of America, N.A., 2013 BL 290891 (S.D.N.Y. May 21, 2013) (enforcing the clawback procedure set forth in the parties' Protective Order and finding privilege had not been waived in the large document production).

Brookfield Asset Mgmt. v. AIG Fin. Prod. Corp., No. 1:09-CV-08285 (S.D.N.Y. Jan. 7, 2013) (Rule 502(d) order means what it says if document inadvertently produced).

Potomac Elec. Power Co. v. United States, 107 Fed. Cl. 725 (Ct. Fed. Cl. 2012) (a 502(d) order cannot ''protect'' intentional disclosures).

Smith v. Allstate Ins. Co., Civil Action No. 3:11-CV-165 (W.D. Pa. Nov. 8, 2012).

Clark County v. Jacobs Facilities, Inc., 2:10-cv-00194-LRH-PAL (D. Nev. Oct. 1, 2012) (concluding that the parties' claw-back agreement precluded the waiver of privilege and noting that with large ESI productions it is cost prohibitive to expect record-by-record preproduction privilege review).

Blythe v. Bell, 2012 NCBC 42 (Sup. Ct. Div. July 26, 2012) (finding waiver after utter failure of defense counsel to take precautions to avoid inadvertent production; noting that a ''litigant may make a considered choice to relax efforts to avoid that [preproduction review] expense. While such choices may be informed and reasonable ones, those choices must at the same time absorb the risk of a privilege waiver'').

Thorncreek Apartments III LLC v. Village of Park Forest, 1:08-cv-01225 (N.D. Ill.Aug, 9, 2011) (applying FRE 502(b) and finding that inadequacies in defendant's review process led to waiver of privilege).

Datel Holdings Ltd. v. Microsoft Corp., No. C-09-05535 EDL (N.D. Cal. Mar. 11, 2011) (addressing automated searches and their reasonableness).

  DDEE ISSN 1941-3882

Castellano v. Winthrop, 27 So. 3d 134 (Fla. Dist. Ct. App. 2010) (discussing attorney behavior that goes beyond inadvertence).

Jeanes-Kemp, LLC v. Johnson Controls, Inc., 09-cv-00723 (S.D. Miss. Sept. 1, 2010) (addressing the interplay of Rule 26(b)(5)(B), Evidence Rule 502(b), and ethical duties).

Rajala v. McGuire Woods LLP, No. 2:08-cv-02638 (D. Kan.July 22, 2010) and subsequent ''Order Determining Privilege Waiver and Clawback,'' 2013 BL 1445(D. Kan. Jan. 3, 2013).

Lawson v. Sun Microsystems, 2010 BL 260034 (S.D. Ind. Feb. 8, 2010) (addressing sanctions for the plaintiff improperly accessing privileged, password-protected documents produced on a hard drive by defendant).

United States v. Sensient Colors, Inc., Civ. No. 07-1275 (D.N.J. Sept. 9, 2009) (waiver of privilege and work product objections where there was a failure to take reasonable precautions to correct the inadvertent disclosure).

In re eBay Seller Antitrust Litigation, Case No. C-07-01882-JF, (N.D. Cal. Oct. 2, 2007) (document retention notice).

Maldonado v. State, 225 F.R.D. 120 (D.N.J. 2004) (involving an ''involuntary'' disclosure that was not inadvertent and finding no waiver of the privilege).

Kinsella v. NYT Television, 370 N.J. Super. 311 (App. Div. 2004) (holding that New Jersey courts might look to a test modeled on Federal Rules that permits a finding of waiver where there was gross negligence).

Ciba-Geigy Corp. v. Sandoz Ltd., 916 F. Supp. 404, 406 (D.N.J. 1995) (''Establishing that a disclosure was unintentional . . . does not go far in establishing the absence of waiver. Rather, the party resisting a waiver argument must demonstrate that it undertook reasonable precautions to avoid inadvertent disclosures of privileged documents.'').

Ethics Opinions

American Bar Association, Cloud Ethics Opinions Around the U.S. (compilation of ethics opinions related to cloud computing by state available at: https://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/cloud-ethics-chart.html).

Iowa Ethics Op. 15-01 (Jan. 28, 2015) (''A lawyer sending or receiving substantive communications with a client via e-mail or other electronic means ordinarily must warn the client about the risk of interception including the use of a computer or other device, or e-mail account, to which a third party may gain access.'').

Iowa Ethics Op. 15-02 (Jan. 28, 2015) (''Interception of confidential or attorney-client communication: the duty to stop, notify, return and, in the case of wrongful interception, to withdraw representation.'').

Philadelphia Bar Ass'n Prof. Guidance Comm. Op. 2013-4 (Sept. 2013) (firm's handling of former partner's e-mail account).

North Carolina State Bar 2012 Formal Ethics Op. 5 (Oct. 26, 2012) (''a lawyer representing an employer must evaluate whether e-mail messages an employee sent to and received from the employee's lawyer using the employer's business e-mail system are protected by the attorney-client privilege and, if so, decline to review or use the messages . . . .'').

ABA Formal Op. 11-460 (Aug. 4, 2011) (''Duty When Lawyer Receives Copies of a Third Party's E-mail Communications with Counsel'').

ABA Formal Op. 11-459 (Aug. 4, 2011) (''Duty to Protect Confidentiality of E-mail Communications with One's Client'').

California State Bar Standing Committee on Professional Responsibility and Conduct, Formal Opinion No. 2010-179 (answering the question about ''Does an attorney violate the duties of confidentiality and competence he or she owes to a client by using technology to transmit or store confidential client information when the technology may be susceptible to unauthorized access by third parties?'').

State Bar of Arizona Ethics Opinion, Op. 07-03 (Nov. 2007) (''Confidentiality; Electronic Communications; Inadvertent Disclosure'').

Secondary Sources

Joanna Stern, ''The Future of Public Wi-Fi: What to Do Before Using Free, Fast Hot Spots,'' The Wall Street Journal (Jan. 19, 2016).

Adriana Linares, ''Information Management Skills Every Attorney Should Know,'' The Florida Bar Journal (Jan. 2016).

Amy Walker Wagner, ''Maintaining Competence in Your Legal Practice in the Face of Technological Advancement,'' The Bencher (Nov./Dec. 2015).

David G. Ries, ''Encryption: Basic Security You Should Be Using Now,'' Trends (July/Aug. 2015).

Samson Habte, ''Lawyers May Need to Encrypt E-Mail in Especially Risky or Sensitive Scenarios,'' 15 *DDEE* 226 (May 28, 2015).

Use of Social Media and Technology

Cases

Congregation Rabbinical Coll. of Tartikov, Inc. v. Vill. of Pomona, No. 07-CV-6304 (S.D.N.Y. Sep. 29, 2015) (permitting adverse inference ''[b]ecause Defendants concealed—and failed to disclose—the relevant Facebook post and potentially a portion of the accompanying text messages'').

United States v. Ganias, 755 F.3d 125 (2d Cir. 2014) (finding after the court's inquiry that a juror's postings about his jury service on a social networking site and ''friending'' another juror during the trial and jury deliberations did not, under the particular facts, violate the defendant's right to an impartial jury).

Baird v. Owczarek, 2014 BL 147920 (Del.2014) (reversing a medical malpractice judgment where a juror's internet research constituted an improper extraneous influence that was an egregious circumstance raising a presumption of prejudice).

Chace v. Loisel, 2014 BL 18583 (Fla. Dist. Ct. App. 5th Dist. Jan. 24, 2014) (finding that the trial judge's efforts to initiate *ex parte* contact with a litigant was prohibited and warranted disqualification because it has the ability to undermine confidence in the judge's neutrality).

J.T. v. Anbari, No. SD32562 (Mo. Ct. App. Jan. 23, 2014) (affirming defense verdict in medical malpractice action and rejecting argument that juror engaged in misconduct).

Lacy v. Lacy, 320 Ga. App. 739 (Ga. Ct. App. 2013) (despite mother boasting on Facebook about a meeting

with the judge in advance of a custody hearing, evidence supported the award of custody).

Ehling v. Monmouth-Ocean Hosp. Serv. Corp., 961 F.Supp. 2d 659 (D.N.J. 2013) (since the plaintiff's privacy settings permitted a coworker friend to see a post, it was permissible for that friend to, without coercion, share the post with management).

In re Collie, 406 S.C. 181 (S.C. 2013) (suspended an attorney for failing to comply with their rule requiring that attorneys admitted to practice law in South Carolina must have, among other things, an e-mail address).

State of Tenn. v. Smith, 418 S.W.3d 38 (Tenn. 2013) (finding the trial court should have held an evidentiary hearing to identify all facts surrounding the extrajudicial Facebook communication between a juror and a State's witness to determine if the misconduct was harmless or prejudicial).

State v. Polk, No. ED98946 (Mo. Ct. App. Dec. 17, 2013) (stating that ''[w]e doubt that using social media to highlight the evidence . . . and publicly dramatize the plight of the victim serves any legitimate law enforcement purpose or is necessary to inform the public . . .'', but there was no evidence that jury knew of or was influenced by the prosecutor's tweets).

Clore v. Clore, No. 2110967 (Ala. Civ. App. June 28, 2013) (finding that in a small town the fact that the judge was friends on Facebook with the adult daughter of the parents getting divorced did not justify recusal).

Juror No. One v. Superior Court, 142 Cal. Rptr. 3d 151 (Ct. App. 2012) (concluding that even if a juror had a privacy interest in his posts, that interest was not absolute and had to be balanced against the criminal defendants' rights to a fair trial).

Domville v. State, 103 So. 3d 184 (Fla. Dist. Ct. App. 4th Dist. 2012) (a judge's friendship on Facebook with a prosecutor conveys the lawyer friend is in a special position to influence judge).

Sluss v. Commonwealth, 381 S.W.3d 215 (Ky. Sup. Ct. 2012) (the status of two jurors that were ''friends'' of a minor victim's mother on a social-networking website was not, standing alone, a ground for a new trial based on juror bias).

United States v. Daugerdas, 867 F.Supp. 2d 445 (S.D.N.Y. 2012) (failure to disclose that juror lied about suspension from practice of law and criminal background resulted in convicted defendant's waiver of his right to challenge partiality of the juror).

Johnson v. McCullough, 306 S.W.3d 551 (Mo. Sup. Ct. 2010) (en banc) (''in light of advances in technology allowing greater access to information that can inform a trial court about the past litigation history of venire members, it is appropriate to place a greater burden on the parties to bring such matters [nondisclosure by a juror] to the court's attention at an earlier stage. Litigants should not be allowed to wait until a verdict has been rendered to perform a Case.net search for jurors' prior litigation history . . . .''

Ethics Opinions

National Center for State Courts, Social Media and the Courts (compilation of state ethics opinions on social media use available at: http://www.ncsc.org/Topics/Media/Social-Media-and-the-Courts/State-Links.aspx?cat=Judicial%20Ethics%20Advisory%20Opinions%20on%20Social%20Media).

West Virginia Lawyer Disciplinary Board, Social Media and Attorneys, L.E.O. No. 2015-02 (Sept. 22, 2015) (providing an overview of social media ethics issues).

In re Hon. Michelle Slaughter, etc., Docket No. 15-0001 (Special Court of Review of Texas Sept. 30, 2015) (dismissing admonition for Facebook posts by judge during trial).

Colorado Bar Association Ethics Committee, Use of Social Media for Investigative Purposes, Op. 127 (Sept. 2015) (''This opinion addresses ethical issues that arise when lawyers, either directly or indirectly, use social media to obtain information regarding witnesses, jurors, opposing parties, opposing counsel, and judges. The opinion also addresses circumstances in which lawyers seek to access restricted portions of a person's social media profile or website that ordinarily may be viewed only by permission.'').

Professional Ethics of the Florida Bar, Op. 14-1 (June 25, 2015, approved by The Florida Bar Board of Governors on Oct. 16, 2015) (''A personal injury lawyer may advise a client pre-litigation to change privacy settings on the client's social media pages so that they are not publicly accessible. Provided that there is no violation of the rules or substantive law pertaining to the preservation and/or spoliation of evidence, the lawyer also may advise that a client remove information relevant to the foreseeable proceeding from social media pages as long as the social media information or data is preserved.'').

Pennsylvania Bar Ass'n Formal Op. 2014-300 (Sept. 2014) (''Ethical Obligations for Attorneys Using Social Media'').

Massachusetts Bar Ass'n Ethics Op. 2014-5 (May 8, 2014) (using social media to ''friend'' an unrepresented adversary).

ABA Formal Op. 466 (April 24, 2014) (''Lawyer Reviewing Jurors' Internet Presence'').

Oregon State Bar Legal Ethics Comm. Formal Op. 2013-189 (Feb. 2013) (''Accessing Information about Third Parties Through a Social Networking Site'').

ABA Formal Op. 462 (Feb. 21, 2013) (''Judge's Use of Electronic Social Networking Media''— when used with proper care it does not compromise their judicial duties under the Model Code any more than traditional forms of communication).

New Hampshire Ethics Comm. Advisory Op. 2012-13/05 (June 20, 2013) (''Social Media Contact with Witnesses in the Course of Litigation'').

San Diego Cty. Bar Ass'n Legal Ethics Op. 2011-2 (May 24, 2011) (''friending'').

NYCLA Comm. on Prof. Ethics, Formal Op. No. 743 (May 18, 2011) (''Lawyer investigation of juror internet and social networking postings during conduct of trial'').

Association of the Bar of the City of New York Comm. on Prof. Ethics Formal Op. 2010-2 (Sept. 2010) (''Obtaining Evidence from Social Networking Websites'').

Philadelphia Bar Ass'n Prof. Guidance Comm. Op. 2009-02 (using a third party to ''friend'' a witness and, by so doing, obtain access to witness' social media postings).

Secondary Sources

Arianne Fuchsberger, ''Social Media Searches: Go Beyond the Google,'' Lexology (Dec. 26, 2015) (provid-

   ISSN 1941-3882

ing tips on locating a complete picture of a person's online presence).

Debra Cassens Weiss, ''BigLaw Partner is Ordered to Donate $5,000 for Tweeting Photos During Federal Trial,'' ABA Journal (Dec. 15, 2015).

NYSBA Social Media Jury Instructions Report (Dec. 8, 2015) (''To reduce the potential impact of improper social media communications on jury trials, the Section recommends that courts, as discussed above, should: (1) consult with counsel prior to jury selection concerning the potential review and/or monitoring of 'public' juror social media communications during jury selection, trial and/or deliberations; (2) consider the Section's revised model New York's Pattern Jury Instructions; and (3) consider displaying in the jury deliberation room a social media usage poster warning of the consequences of improper social media communications.'').

Amy B. Alderfer and Abby L. Sacunas, ''A Step by Step Guide To Maximizing The Use of Social Media In Defending Product Liability Claims,'' Lexology (Dec. 4, 2015).

Samson Habte, ''Lawyers' Intensive Social Media Investigations Carry Risks,'' 15 *DDEE* 534 (Dec. 10, 2015).

Kevin W. Turbert, ''Discoverability of Social Media Profiles in New York,'' NYSBA Journal (Oct. 2015).

NYSBA Social Media Ethics Guidelines (June 9, 2015) (''A lawyer may review the contents of the restricted portion of the social media profile of a represented person that was provided to the lawyer by her client, as long as the lawyer did not cause or assist the client to: (i) inappropriately obtain confidential information from the represented person; (ii) invite the represented person to take action without the advice of his or her lawyer; or (iii) otherwise overreach with respect to the represented person.'').

Jurors' Use of Social Media During Trials and Deliberations, Federal Judicial Center (Nov. 22, 2011) (*available at*: http://www.fjc.gov/public/pdf.nsf/lookup/dunnjuror.pdf/$file/dunnjuror.pdf) (Surveyed over 500 judges and determined that they infrequently detected juror use of social media.).

Use of Court Filing Technology

Cases

Franklin v. McHugh, 804 *F.3d* 627 (2d Cir. 2015) (dismissing appeal as untimely for failing to follow the e-filing of the notice of appeal process to completion).

Two-Way Media, LLC v. AT&T Operations, Inc., No. 09-CA-00476 (W.D. Tex. Feb. 6, 2014) (aff'd, 782 F.3d 1311 (Fed. Cir. 2015) (denying extension of time to file appeal where defense counsel failed to check docket activity for over 52 days, improperly relied upon NEF docket text, and failing to read the orders they downloaded from the NEF e-mail).

Kanoff v. Better Life Renting Corp., 2008 BL 242871 (D.N.J. Oct. 22, 2008), aff'd 350 Fed. Appx. 655 (3d Cir. 2009) (paper mailing of notice of appeal was delayed due to address problems and the notice was received late because the attorney did not e-file it — the Third Circuit stated: ''Put simply, this was not a case where 'as the result of some minor neglect, compliance was not achieved.' . . . Compliance was not achieved because counsel failed to educate himself about a sea change in filing requirements that had taken place more than three years before the relevant events of the instant case.'').

2015 Amendments to the Federal Rules of Civil Procedure

Secondary Sources

R.J. Hedges & M. Nelson, ''Status Quo or Game Changer? New Federal Rules Go Into Effect on December 1,'' 15 *DDEE* 444 (2015).

T.Y. Allman, ''The 2015 Civil Rules Package as Transmitted to Congress,'' 16 Sedona Conf. J. ___ (2015).

T.Y. Allman, ''Thoughts on the 2015 Amendments to Federal Rule of Civil Procedure 37(e),'' 15 *DDEE* 245 (2015).

T.E. Brostoff, ''eDiscovery Experts Discuss How Proposed Amendments Will Possibly Shake Out in Court,'' 14 *DDEE* 329 (2014).

T.E. Brostoff, ''Webinar Panel Discusses FRCP Proposals, Public Comments and Key Controversies,'' 14 *DDEE* 108 (2014).

T.E. Brostoff, ''Amending the Federal eDiscovery Rules: Tackling the Comments on 26(b) and 37(e),'' 13 *DDEE* 593 (2013).

T.E. Brostoff, ''The State of Sanctions in 2013: Recent Developments, Rule Amendments,'' 13 *DDEE* 530 (2013).