



BY  
**WILLIAM HAMILTON**  
AND  
**WENDY K. AKBAR**

# E-Discovery in the Age of

The ethical demands  
for attorney competence

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

*ABA Model Rule of Professional Conduct 1.1; Competence*

**Y**our prospective client arrives at your office. She is obviously agitated and somewhat disheveled. Over the next hour, her story emerges. She has been married for 15 years. The marriage started to suffer three years ago when the husband's business began to fail. The husband, with her assistance, ran a roofing company from their home. Times were good until the real estate bust. Now their business has been scaled back and operates at a loss. They have two children. Both are good students with active online social lives. The son is graduating from high school this year, and the other child, a 14-year-old daughter, is seeing a psychologist for anxiety and depression. The husband has consulted a divorce lawyer and told your client that he is moving out with the kids and "what belongs to him." The husband has scheduled a moving truck to arrive next week. Your client tells you that the husband's relations with the kids are very strained, and that he belongs to some private, online "social" clubs. Your client claims that she is and has been the "brains behind the business."

As counsel, you must quickly assess your client's case, identify the issues, and provide some very immediate, and sometimes emergency, practical advice. In this swirling cacophony of emotional, physical, and economic crises, a fundamental duty to the client may be overlooked—advising the client about the location and preservation of evidence in the family's "digital vault." The location and preservation of this digital evidence to support your client's case requires a new skill set. Family law attorneys must know how to economically and effectively locate, preserve, collect, review, and utilize electronically stored information (ESI) for a number of reasons.

**1. To access a major source of dispositive evidence.** Today's American family is a digital family living in a digital ecosphere that can tell family stories and reveal family secrets better than any after-the-fact human recollection. The volume of a family's household data now rivals that of a small business. Simply put, family members do not just use some digital tools, they live digitally: e-mail, Facebook, Twitter, instant messaging, texting. Young people today were "born digital." Palfrey and Gasser, *Born Digital: Understanding The First Generation of Digital Natives*. For example, few college freshman (members of the graduating class of 2014), who may be clients in divorce cases in a few years, know how to write in cursive and consider e-mail "just too slow" as a means of communication, compared to media such as Facebook and texting. See <http://bits.blogs.nytimes.com/2010/08/17/the-class-of-2014-no-e-mail-or-wrist-watches/?scp=2&sq=cursive&st=cse>.

**2. To adequately collect and preserve evidence.** The typical family law client is not skilled in data

are frequently unfocused, distraught, adversarial, and clueless when it comes to finding and using this evidence. Although "born digital" family members may have certain texting and chatting-on-social-website facilities, few are skilled at collecting and preserving data in a way that meets legal standards and establishes the necessary chain of custody to permit introduction of the data into evidence.

**3. To conduct e-discovery at minimal cost.** Using outside forensic and technical experts is expensive and frequently beyond the case budget. The costs of e-discovery are often painful for even large businesses, and often seem disproportionate to amounts in dispute. In the typical family law case, more modest budgets will make the utilization of experts and e-discovery specialists even more delicate. Thus, the family law attorney must know, not only how to conduct these activities, but how to do so in the most expedient and cost-efficient manner.

**4. To recognize and prevent destruction and alteration.** The emotional cauldron of a family law dispute can create pressures that cloud client judgment, leaving family members feeling that stakes are too high *not* to tamper, alter, and destroy digital evidence. Family law disputes are life-altering events that can bring out the best in people, but all too often, bring out the worst. Data is fragile and easily altered. For example, an original e-mail can be changed and then forwarded to a third-party friend or family member. The altered e-mail can then be produced as evidence of the original forwarded message. The family law attorney must be alert to such pressures and carefully guide the client to minimize the risk of inadvertent and even

# Facebook, Twitter, & the Digital Family

acquisition, preservation, and review and does not generally have the resources to farm it out to experts. Thus, family lawyers work in an environment more challenging than the corporate or business-law litigation attorney. Where the best e-discovery business practices call for creation of internal e-discovery teams composed of management, IT, in-house counsel, and retained counsel who develop in advance e-discovery and litigation-hold protocols, the family lawyer is left to set up his or her own systems while managing clients who

intentional spoliation of data. A working knowledge of how electronic data can be manipulated or destroyed is essential to spotting your client's or an opposing party's attempts to do so. For example, a laptop with a removable hard drive slot may indicate that a spouse has an extra hard drive lying around with useful information. Similarly, while one typically searches for certain types of programs by file extension (.doc for Word files, .xls for Excel, .jpg or .bmp for pictures), those extensions can be changed to hide information.

## What makes “digital” different

Electronic data discovery has burst into the mainstream of American commercial litigation. See, e.g., Ralph C. Losey, *Electronic Discovery: New Ideas, Case Law, Trends and Practices* (West Publishing 2010). New federal rules of civil procedure specifically pertaining to the discovery of ESI were promulgated and became effective on December 1, 2006. Many federal district courts also have adopted local rules specifically addressing e-discovery. For example, forty-one state courts have promulgated civil procedure rules pertaining to e-discovery, *available at* <http://www.ediscoverylaw.com/articles/resources/>.

Data, however, is mysterious. No one sees or holds these electronic impulses. What appears on the computer screen (an “output” device) is only a partial rendition of the ESI ultimately available. ESI is (i) voluminous, (ii) fragile, (iii) dispersed, (iv) disorganized, (v) recoverable, (vi) searchable, and (vii) persistent. The Sedona Principles; 2d. edition (2007), pp 1-5, <http://www.thesedonaconference.org/>.

Add to all the mystery the element of constant change. E-mail is now almost old-fashioned among hip professionals and college students, supplemented if not supplanted by texting, tweeting, “instant messaging,” and communications within social networks such as Facebook, MySpace, Friendster, Bebo, and others. Data is stored in massive databases holding unimaginable amounts of information. Facebook now has more than 350 million worldwide members, 100 million in the United States. Charles Petersen, “In the World of Facebook,” *The New York Review of Books*, <http://www.nybooks.com/articles/23651>. Most laptop computers have storage space of more than 200 gigabytes. Each gigabyte of pure text data will produce approximately 50 banker boxes of paper, or nearly 3,000 sheets—enough paper to fill the back of a small pick-up truck. Ralph Losey, E-Discovery Team Blog, “How Much Data Do You Have?” It would take a lawyer reviewing 100 documents an hour, approximately a month to get through this single gigabyte of text-based information. A single e-discovery review project in a modest litigation can require rooms of attorneys working for weeks or months.

## Accessing the family vault

Let’s take a brief look at the digital environment of a typical American family, and then at our hypothetical family. The typical family household will have multiple desktop and laptop computers and multiple e-mail accounts. Home networks with computers acting as “servers” are not uncommon. Texting and instant messaging is the coin of the realm. Family members are involved in social networking sites like Facebook, MySpace, Flickr, and Twitter. Much of the family’s digital vault will be stored in the Internet “cloud”—electronic storage facilities and databases outside the home. The most common e-mail providers are web-based: Google, Hotmail, and others, whose offerings, along with e-mail include a host

of online software applications, social sites, and gadgets. Wikipedia lists more than 100 major active social websites. See [http://en.wikipedia.org/wiki/List\\_of\\_social\\_networking\\_websites](http://en.wikipedia.org/wiki/List_of_social_networking_websites).

It is this emergence of what has been called “Web 2.0” that has brought e-discovery to the front burner for family lawyers. “The term ‘Web 2.0’ (2004–present) is commonly associated with web applications that facilitate interactive information sharing, interoperability, user-centered design, and collaboration on the World Wide Web. (Examples of Web 2.0 include web-based communities, hosted services, web applications, social-networking sites, video-sharing sites, wikis, blogs, mashups, and folksonomies. A Web 2.0 site allows its users to interact with other users or to change website content, in contrast to noninteractive websites where users are limited to the passive viewing of information that is provided to them. See also [http://en.wikipedia.org/wiki/Web\\_2.0](http://en.wikipedia.org/wiki/Web_2.0)).

## The family footprint

The family’s financial records will be stored electronically. Banking, investments, retirement accounts, and profit-sharing plans will likely be managed electronically from the home computers. E-mails abound from the PTA, high school, and college networks, neighborhood associations, and sports

## The Digital Family Preservation and Collection Checklist



### Financial

- Home business
- Mortgage
- Credit cards
- Bank statements
- Purchase accounts—no one uses cash

### Educational

- School
- Online grades
- Testing
- Home delivered school software

### Social websites

- Clubs
- Associations
- Religious
- Political

### Online digital

- Facebook
- eBay
- Twitter
- LinkedIn
- Internet favorites and browsing history
- Amazon account
- Store accounts

teams. Employer-owned laptops brought home for work in the evenings also may contain these personal records. The typical American family now has its own data information ecosphere that reflects and captures the life of the family.

The family's digit vault is not merely composed of text and financial ESI. It may well have hours upon hours of electronically stored movies and music. Internet browsers will track the family's Web-based activity, storing information about websites visited and the favorites of each family member. Parents or anyone in the home with access to the family computers may have installed "ghosting" software to tracks the surfing, texting, and messaging activities. Presumably, to protect music, movies, e-mail, and other data, the family will have periodic computer back-ups stored locally on drives separate from the computers or online. See, e.g., [www.carbonitepro.com](http://www.carbonitepro.com).

The family's ESI will be vital to the issues of any family law case and critical evidence in any contested matter. For example, significant components of a parent's relationship with the children should jump out of the family's digital record. Moreover, the digital vault is a shared family asset of immense value to each family member. In some respects, the digital record is each family member's diary. Issues relating to the ownership of and access to the family's data will loom large in any family dissolution.

More than 80 percent of lawyers surveyed by the *American Academy of Matrimonial Lawyers* said Facebook is showing up in more divorce cases. Sixty-six percent called Facebook the unrivaled leader for online divorce evidence, followed by MySpace (15 percent) and Twitter (5 percent). <http://www2.tbo.com/content/2010/feb/21/na-facebook-adds-fuel-to-flames-of-divorce/>.

What kind of evidence can be gathered from the trivial postings on Facebook, MySpace, Twitter or others of their ilk? More than one might think. People often believe that virtual actions do not carry the same consequences as real-life actions—that e-flirting does not equate to flirting in a bar, and that details shared on social networks will not intrude into off-line lives. In reality, the

written trail can haunt an individual far more readily than an oral conversation in a noisy and crowded room. For example, the following could have major repercussions in a divorce or custody battle:

**1. Personal habits:** A spouse posts a Facebook picture of him or herself in a drunken pose, beer in one hand and a bong in another. Or perhaps the spouse is smart enough not to do this—but a friend from the party posts it on his own page and "tags" the spouse in the photo, causing the photograph to show up on the spouse's site as well.

**2. Employment and money issues:** A spouse posts comments on a MySpace page worrying about losing a high-paying job and becoming unemployed. Or maybe a post simply says something along the lines of, "Using the money from my secret off-shore account to buy a BMW" or "Just bought a villa in Italy."

**3. Whereabouts:** A spouse tweets a Twitter along the lines of "Partying with friends in Vegas" when he or she was supposed to be on a business trip.

**4. Infidelity:** A spouse chats with a lover on Google Talk about a rendezvous, not knowing that every single Google Chat is archived and can be accessed through the spouse's Gmail account—such as during discovery in a divorce case. Or perhaps the spouse has a Match.com page that says "single and looking for love."

### Who, what, when, and where

**1. Who is your best source?** In our hypothetical, the first stop should be everyone in the family home, particularly the husband and, based on their active online presence, possibly the children, as they might have vented online about what the husband said or did. Also consider contacting the couple's employees. Their e-mails could contain information on who really is the "brains" behind the business, who they consider to be the real boss, and their perceptions as to the division of hard work between the couple. Investment firms and other financial advisors may have important information on both personal and business fronts, as may friends' and relatives' computers.

This is a broad list, however. It is not cost-effective to obtain ESI from anyone in the couple's circle of acquaintance, so the trick is to limit overlap and repetition. For example, direct correspondence between the husband and investment firms, employees, and others should all be on the couple's hard drive or the husband's laptop. There may be no need to obtain it from multiple sources, such as the investment firm as well. Absent suspicion that the husband has altered his hard drive or intentionally deleted information in a way that may not be retrievable, it is more cost-effective to start with ESI in the home, and then consider what blanks need filling in.

#### Cloud computing

- iMobile
- iPhone applications
- Google applications
- Hotmail
- Yahoo accounts and clubs

#### PDA

- iPhones
- Blackberries
- Etc.

#### Backup

- Online archives
- Home backups

#### Home network

- Server configuration and residual data



**2. What sources are worthwhile?** The possibilities seem endless. Certainly cell-phone records (both calls and texts), home and business computers and laptops, along with any removable hard drives or backup disks, portable devices, such as Blackberries and iPhones, e-mail accounts, and records, including deleted e-mails and website search history.

Of course, social network and related materials will be important, as the husband supposedly belongs to several online social “clubs.” A search of the home computer will likely reveal from the website history, which clubs these are. How accessible information from these websites is will depend on facts, such as whether the husband’s profile is open to everyone, or just to accepted “friends,” as is the case with Facebook. If the page is open to everyone, it is certainly fair game. If not, it is possible to go to the source. Twitter archives all tweets ever tweeted, and Facebook archives user pages. What’s more, social networking sites have been taking steps to make sure their content is accessible in legal situations.

Social media companies also are zealous about protecting the privacy of their users, making them reluctant to provide user information to lawyers without permission from the account holder, even when confronted with a subpoena. Internet service providers (ISPs), which also temporarily store user information, also are reluctant to provide access absent consent. Thus, any subpoena is likely to end in a courtroom, with both the husband and the ISP/social network fighting access. In the end, unless a court order is granted, the fact is that family lawyers must rely on opposing parties to contact a social networking site, collect, and produce the data. While this obviously raises questions about whether everything is being handed over, it also saves the wife the expense of fighting a subpoena in court. Thus, one way to be cost-effective is to limit the need for litigation to recover online social pages. Determine at the beginning of the case whether such sites should be obtained and preserved. If both sides agree, determine the scope of what will be produced.

If the husband refuses to produce any social networking materials, or if financial issues make issuing and fighting a subpoena impractical, other avenues remain. Many aspects of the husband’s Internet activity will be on the family and even business computers and laptops—which may be fair game in a situation like this where both spouses claim an equal interest in the business and its equipment. Because Facebook notifies a person by e-mail when someone comments on a post, the husband’s e-mail account may contain the content and the date and time of Facebook messages, even those that have been deleted from his page. What’s more, unless his hard drive is wiped clean, it should store a copy of the deleted and other social networking information, which can then be retrieved.

Social networking and e-mails, however, only scratch the surface. Office calendars, such as those set up through

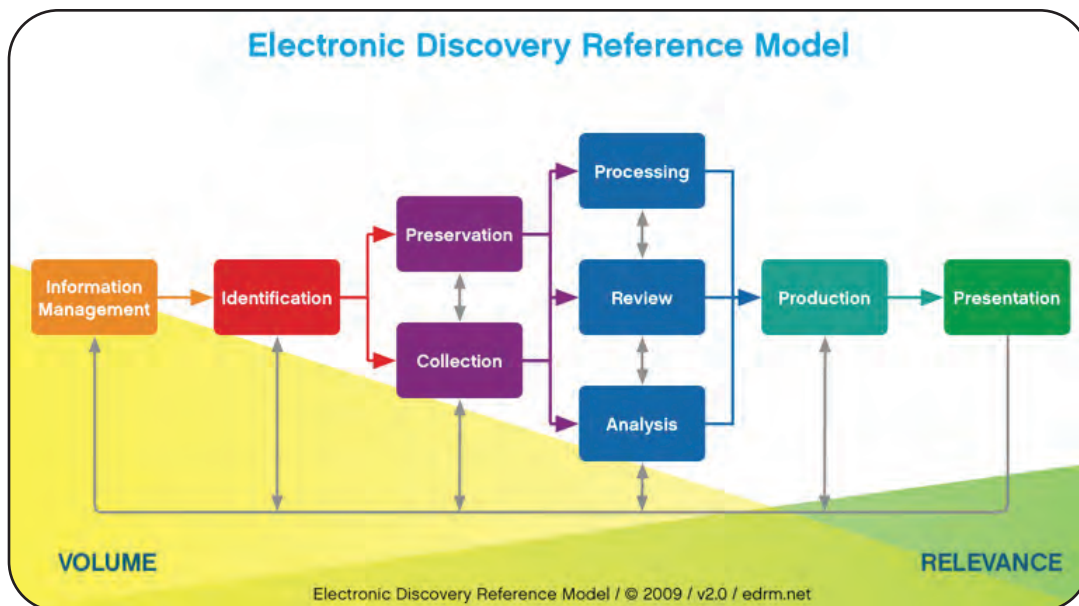
Google and Microsoft Outlook, will contain detailed information about the husband’s calendar and where he was in relation to where he was supposed to be. The browser history files on his computer and laptop can show what websites he visited and what graphics he viewed. This could include real estate listings in Key West, repeated visits to off-shore banking websites, or other revealing information about his personal habits. Additionally, to gain an adequate sense of the husband’s financial resources (and what he considers to “belong to him”), computer hard drives should be examined for materials such as word processing files that have to do with asset transfers, business activities, and stock option agreements; spreadsheet files with asset lists, financial plans, budgets and expenses; and database files with contact lists, financial data and assets.

Finally, consider investing in Web-page preservation, which runs a cost-effective \$200 or so. This provides a way to preserve, or take a “snapshot” of, a specific page on a specific date. (On a Mac, use command, shift, 4, and your mouse to frame and capture the page.) Take “snapshots” of any public Web page that may be useful in the case, and that the husband may alter once he becomes aware that he is in for a court battle. For example, perhaps the business website currently credits both spouses as having founded the business or as co-owners, or perhaps it lists the wife as the business contact for certain areas. The husband may change the page to take all mentions of her off the website; with a snapshot of what the page looked like before this happened, the evidence remains.

Alternatively, there are sites that archive earlier versions of Web pages, and are accessible for free—for example, Wayback Machine at <http://www.waybackmachine.org>. There is a risk, however, in relying on these sites alone: they may not have archived the page as it existed in the particular timeframe you are interested in.

**3. When and where to collect materials.** In this case (as in most), the extent to which a family lawyer requests and collects ESI depends, in part, on the scope of what it is expected to yield and what kind of budget is on the table. Requesting all ESI ever created will be expensive and time-consuming, so focus on (a) the most relevant places to look; and (b) the most relevant time period to focus on.

As to the first issue, discuss with the wife at the initial meeting, exactly where she believes her husband’s most important materials are, both business and personal. There is usually no question about the relevance of the hard drive in the husband’s computer and laptops, any disks, network storage, remote Internet storage, handheld devices, and backup disks. Get a sense of how computer savvy the husband is: Ask how often he uses the computer. A business laptop? How socially active is he online? Does he spend a lot of free time on the computer? How many portable devices does he have? Be creative when drawing up ESI



Incorporate these EDRM phases into your family law practice.

requests, and make sure that they are broad enough to hit all of these items. Consider hiring investigators with digital forensic tools to engage in some limited, targeted electronic snooping on the hard drive. Do some of the investigation yourself, such as by using Wayback Machine or checking common social websites like Match.com to see if the husband has a profile there. Do a basic Google search for the husband's name and see what pops up.

Second, the time it takes to obtain and go through every single file from the beginning of time will be inordinate. Set out a reasonable, limited period on which to focus your requests. For example, if the joint business was started seven years ago, searching computer files created over the entire fifteen-year marriage will probably yield thousands of useless and irrelevant documents. Similarly, since the marriage started to suffer only three years ago, there may not be much reason to look through electronic data from ten years ago.

### Set boundaries

In the end, although you want to impress upon the wife how important obtaining relevant ESI is, she must be informed about boundaries. The first step is to take stock in what she has that may be discoverable and determine what she believes the husband may have. Nowadays, these questions should be asked during the initial interview in *any* family case. Ask the wife to preserve all electronic information, and based on what she tells you is out there, provide a list of what is possible to include. Draft a letter, along similar lines, to send to the husband's attorney, laying out what he should preserve. That way, the husband is on notice not to destroy or alter any ESI and can be sanctioned if he does.

At the same time, caution the client to stop posting on her own social networks and to be careful of her texts and IMs, while making sure she knows not to delete or alter anything negative that may already be on her pages. It is much easier to spin a bad picture or comment, than to explain why

it was deleted. Destroying evidence can lead to court-imposed sanctions. Moreover, be aware of reality and the dangers of temptation for your client. ESI gathering must be done in a way that does not run afoul of federal or state privacy laws. Chances are, the wife has easy access to much of her husband's relevant ESI. She may be tempted to log onto their home computer and copy all files, especially because he is about to move out. She may snoop in her husband's business laptop for financial information and try and log onto his social networks. (If he's the only one who uses that computer, it may automatically input his password and sign him in.) If she can't access the sites, a mutual friend may provide inside knowledge or "snapshots" of what is on the site. Or she may enlist a mutual acquaintance to "friend" him and pass along juicy information.

Although the wife may well have a right to snoop and copy anything on the home computer, some of these other self-investigative activities are questionable and can lead to monetary sanctions or to a finding that the materials—even smoking e-guns—are inadmissible in a divorce or custody action. For example, in *Byrne v. Byrne*, 168 Misc. 2d 321, 650 N.Y.S.2d 499 (Sup. Ct. 1996), the husband had a laptop owned by his employer, who permitted him to use it for personal matters as well. It was in the marital residence when confiscated by his wife and given to her attorney. Uncertain about the ethics of poring through the computer, the attorney wisely turned it over to the court. It was only after a hearing that the court ruled that the laptop was fair game since the husband (a) used it at home; (b) allowed their children to use it for homework; and (c) often used it for personal matters, including family finances. The court reasoned that the computer was analogous to a "file cabinet" in the house and, therefore, accessible to the wife as well as the husband. Not all cases turn out like this, however, and who knows if the outcome would have been as favorable if the wife or attorney rifled through the laptop right away.

## Your ESI ethical duties

In summary, to meet the ethical demands of competent representation, the family lawyer must now adroitly and expertly handle all phases of the e-discovery process: organization, preservation, collection, review, and production of electronic data. The various phases in e-discovery have been popularized in the EDRM model. See [www.edrm.net](http://www.edrm.net).

How many family law litigators are familiar with this now well-established e-discovery model and systematically

### At the beginning of a case, issue to clients clear and understandable written data preservation instructions and monitor the client's compliance

incorporate these e-discovery phases into standard practices? Percentage-wise, the number is likely low. Family law attorneys must learn to think digitally and to understand the implications of how these new forms and containers of information have altered the character of the litigation process. From the inception of the case, the lawyer must work with clients to identify, locate, and preserve relevant data. At the very least:

- At the beginning of a case, issue to clients clear and understandable written data preservation instructions and monitor the client's compliance. Failure to do so may be deemed *per se* negligence. (*The Pension Committee of the University of Montreal Pension Plan v. Banc of America Securities, LLC*, 2101 WL 184312 (S.D.N.Y.) (Judge Shira A. Scheindlin.)

- Put parties holding electronic information on notice that they must preserve relevant data, and then immediately subpoena the data.

- Become adroit at negotiating with opposing counsel regarding the location and search of ESI, paying close attention to the principles of the Sedona Cooperation Proclamation, which are widely endorsed by judges across the nation. See [www.thesedonaconference.org](http://www.thesedonaconference.org).

- Become familiar with search tools

and technology, which can be critical to finding pertinent text, pictures, and video in the family's digital vault.

- Be alert to the potential for alteration and spoliation of ESI, as well as the dangers of seeking and obtaining ESI through improper means, which may render it inadmissible.

- Make it a routine, during intake meetings with new clients, to find out what ESI both spouses may have, where it resides, and to what extent it is relevant. Consider talking with opposing counsel before going on the defensive. If both sides agree ESI is relevant, it may be a matter of determining what to preserve, rather than saving an entire hard drive or retrieving every piece of ESI in the digital vault. **FA**



**William Hamilton** is a partner with Quarles & Brady in Tampa, Florida. He is Board Certified in Business Litigation and Intellectual Property by

The Florida Bar. His work includes complex business litigation in the areas of contract, software and technology disputes, intellectual property (copyright, trademark, patent and trade secrets law), e-commerce, data security, telecommunications, trade regulation, and unfair trade practices. He teaches Electronic Discovery and Digital Evidence as an adjunct professor at the University of Florida's College of Law, and his full professional biography is available at [http://www.quarles.com/william\\_hamilton/](http://www.quarles.com/william_hamilton/).



**Wendy K. Akbar** is an associate with the firm. She represents clients in all aspects of complex commercial litigation with a focus on intellectual

property litigation, particularly patent litigation, trademark, trade dress and copyright litigation, trade secret, false advertising and licensing disputes. She serves as chair of the firm's records retention and electronic discovery team and is editor-in-chief and a writer for E-discovery Bytes, Quarles' e-discovery blawg, located at <http://ediscovery.quarles.com/>.