



Committee Chairs

Laura McLaughlin
Logan College of Chiropractic
Chesterfield, MO
(636) 230-1734
laura.mclaughlin@logan.edu

Kenneth R. Berman
Nutter McClennen & Fish, LLP
Boston, MA
(617) 439-2532
kberman@nutter.com

Mark S. Davidson
Williams Kastner
Seattle, WA
(206) 628-6648
mdavidson@williamskastner.com

Journal Editors

Gerardo R. Barrios
Baker Donelson
Mandeville, LA
(985) 819-8416
gbarrios@bakerdonelson.com

Peter J. Boyer
Hyland Levin, LLP
Marlton, NJ
(856) 355-2912
boyer@hylandlevin.com

David L. Johnson
Miller & Martin, PLLC
Nashville, TN
(615) 744-8412
dljohnson@millermartin.com

ABA Publishing

Jason Hicks
Associate Editor

Sonya Taylor
Designer

Business Torts Journal (ISSN 1549-2923) is published quarterly by the Committee on Business Torts Litigation, Section of Litigation, American Bar Association, 321 N. Clark Street, Chicago, IL 60654-7598. The views expressed within do not necessarily reflect the views of the American Bar Association, the Section of Litigation, or the Committee on Business Torts Litigation.

© 2011 American Bar Association

apps.americanbar.org/litigation/committees/business_torts



Effectively Accessing Social Media Websites for Use at Trial

By Travis B. Swearingen

In 1999, Judge Samuel B. Cant of the Southern District of Texas, in his decision in *St. Clair v. Johnny's Oyster & Shrimp Inc.*, 76 F.Supp.2d 773, 775 (S.D. Tex. 1999), cautioned against relying on information from the Internet, which he characterized “as one large catalyst for rumor, innuendo, and misinformation” and “voodoo information” that is “adequate for almost nothing.” Ten years later, disciplinary authorities are grappling with the question of how to deal with judges who become Facebook “friends” with attorneys who appear before them. See www.aoc.state.nc.us/www/public/coa/jsc/publicreprimands/jsc08-234.pdf. According to Nielsen’s published stats, the world now spends over 110 billion minutes on social networks and blog sites. This equates to one in every four and a half minutes or 22 percent of all time spent online total. *Social Networks/Blogs Now Account for One in Every Four and a Half Minutes Online*, NielsenWire, June 15, 2010, <http://blog.nielsen.com/nielsenwire/global/social-media-accounts-for-22-percent-of-time-online>. As of July 21, 2010, Facebook boasted over 500 million active users, at least 50 percent of which log in on any given day. Facebook Usage Statistics, www.facebook.com/press/info.php?statistics (last visited January 6, 2011). As of April 2010, Twitter had 105 million registered users with 300,000 new users joining every day. Bianca Bosker, *Twitter User Statistics Revealed*, The Huffington Post, Apr. 30, 2010, www.huffingtonpost.com/2010/04/14/twitter-user-statistics-r_n_537992.html. MySpace has 123 million unique users. Peter Chubb, *Facebook Dethrones MySpace: New 2010 Statistics*, Product Reviews News, Nov. 21, 2010, www.product-reviews.net/2010/11/21/facebook-dethrones-myspace-new-2010-statistics. The average Facebook user adds 90 pieces of “content” every month, be it a status update, photograph, or blog post. Some estimates place the number of Internet blogs at over 150 million. NM Incite, a Nielsen/McKinsey Company, www.blogpulse.com (last visited Jan. 6, 2011). And it’s not just computer savvy kids either; the fastest growing demographic for social networking websites is individuals over the age of 35. Peter Corbett, *Facebook Demographics and Statistics Report 2010—145% Growth in 1 Year*, iStrategyLabs, Jan. 4, 2010, www.istrategylabs.com/2010/01/facebook-demographics-and-statistics-report-2010-145-growth-in-1-year.

Based on these statistics, it is inevitable that an important player in your lawsuit
(Continued on page 20)

Inside This Issue

Message from the Chairs.....	2
Message from the Editors.....	3
Cyber-Defamation: It’s Not Just Business as Usual	4
Avoiding an Electronic Discovery Disaster with Litigation Holds	9
Using Virtual Data Rooms to Your Advantage	13
Achievable Steps to Discovery Cost Management.....	16



Laura McLaughlin



Kenneth R. Berman



Mark S. Davidson

Message from the Chairs

Many of your committee leaders and colleagues attended our joint mid-winter meeting with the Corporate Counsel, Minority Trial Lawyer, and Women Advocate Committees in Naples, Florida, February 17–20, 2011. As always, the CLE programs were outstanding. Our committee business meeting was very productive, and the social events and networking opportunities were casual, successful, and a load of fun. Mark your calendars now for next year's meeting, February 16–19, 2011, in Carlsbad, California. This meeting is always a highlight of committee activity.

The Section of Litigation's Annual Conference is in Miami Beach this year, April 13–15, 2011. Materials from the three programs that our committee is presenting will be available on the committee webpage, <http://apps.americanbar.org/litigation/committees/businesstorts>. Next year's Section Annual Conference will be in Washington, D.C. Our next opportunity to get together will be at the ABA Annual Meeting in Toronto, August 4–6, 2011. We hope to see you there.

We would like to take this opportunity to invite you to submit articles and case notes of interest to business torts practitioners for the committee's webpage. Fresh content is enthusiastically received, and we will provide a link to your bio on your firm's website when the submission is posted. This is one area we would like to improve upon in the months ahead, and we can do it best with submissions from our far-flung members in the trenches and in the know. Submitting material for publication on the webpage is also an excellent way to get more involved in committee activities and to interact with committee colleagues. Submissions should be directed to Betsy Hyatt (ehyatt@starrslaw.com),

Dan Kaufmann (dkaufmann@babco.com), or Jonathan Shapiro (jshapiro@shapirolawofficesct.com).

Please help us grow the committee. If you have friends or colleagues who practice in the area of business litigation, spread the word. There is no longer any limit to the number of committees a member can join in the Section of Litigation, so please encourage existing Section members as well as non-Section members to join the Business Torts Litigation Committee. Anyone interested can join our committee through the Business Torts Litigation home page.

The committee is always looking for new and enthusiastic leaders, and for those of you who would like to participate more actively or serve as subcommittee chairs or editors, please contact our committee and subcommittee chairs. Many of the leaders of our committee and the Section leadership worked their way up through the subcommittee structure. We know from our own experience that actively participating in committee meetings and activities provides excellent opportunities for networking and making lifelong friends around the country.

We invite you to participate in the committee's monthly conference calls. They are conducted on the third Thursday of each month at 1:00 p.m. ET. The call-in number is 866-646-6488, and the pass code is 9968159017#.

We welcome your suggestions on ways in which the Business Torts Litigation Committee can help you—with networking, substantive content, or otherwise. Feel free to drop a line to any or all of us at the email addresses on the front cover.

Finally, the chairs wish to thank both the authors and the committee's journal editors for another informative issue. ■

A
SOUND
ADVICE

for free

now available[^] on iTunes™.

www.americanbar.org/groups/litigation/resources/section_audio.html



Gerardo R. Barrios



Peter J. Boyer



David L. Johnson

Message from the Editors

Advances in technology continue to impact the world and the legal profession. Some of us remember the days when we served requests for the production of documents and received in return bankers' boxes of paper documents, dutifully stamped with "bates" numbers from a mechanical stamp. Now it is difficult to imagine a case in which email, instant messaging, and other forms of electronic evidence are not front and center in discovery and at trial.

Social networking has come of age this year, playing a lead role in Hollywood, in Middle Eastern politics, and in business torts litigation. It is the subject of our lead article, "Effectively Accessing Social Media Websites for Use at Trial," by Travis B. Swearingen. The article examines the rapid expansion of social networking website usage and provides potent examples of how information uploaded onto these websites is shaping the results of litigation across the country. It offers practical tips on discovering and accessing relevant social media information and on how to get the information into evidence in the courtroom.

With an increase in social networking, blogging, and other outlets for posting information, the potential for mischief and abuse also increases. As more businesses use the web for marketing and conducting business, they are also increasingly coming face to face with the darker side of the Internet. Business torts committed and published in cyberspace by sometimes anonymous critics have become an issue to be reckoned with. Zachary G. Newman and Anthony Ellis provide an eye-opening overview of substantive and procedural issues likely to be confronted in both prosecuting and defending cyber-torts claims.

Last year's oil spill in the Gulf of Mexico presented unprecedented challenges to scientists and engineers in capping the well and dealing with the environmental aftermath. Litigation over issues arising from the spill is expected to result in a similarly unprecedented electronic-discovery effort. Elizabeth S. Fenton, Diana Rabeh, and Jonathon M. Shapiro take an updated look at the importance of litigation holds as a crucial first step in preventing a client's unexpected disaster from spawning a secondary electronic-discovery disaster.

Virtual data rooms, commonly referred to as VDRs, are increasingly being used to provide third parties with electronic access to large volumes of information, including confidential information. Amy M. Stewart and Meghan E. Bishop provide an insightful look into the world of VDRs with helpful practice tips on how to analyze and approach claims arising from transactions in which VDRs were used. They also discuss how to structure a VDR site at the outset of the transaction to create an electronic trail that can be authenticated and used, if needed, in subsequent litigation.

The increased proliferation of sources of potential evidence have made the cost of handling, processing, and producing electronic evidence a major line item in any litigation budget. In a topic near and dear to our clients' hearts, Thom Wisinski and Randy Girouard lay out a strategy for controlling costs in processing electronic discovery. Their article stresses the importance of planning, communication, documentation, and standardization of electronic-discovery processes. Diligent adherence to these steps can effectively reduce the cost of compiling, sorting, and producing electronic evidence.

The *Business Torts Litigation Committee* webpage, http://apps.americanbar.org/litigation/committees/business_torts, contains additional articles on technology issues and other business torts litigation topics. The site is updated regularly and has links to other ABA pages with similar resources.

If you are interested in contributing an article to an upcoming issue of the *Business Torts Journal*, we encourage you to contact our substantive subcommittee chairs (who are listed on the committee's website) or to directly contact one of us. We are currently seeking articles on the following topics:

- Unfair Trade Practices
- Fiduciary Duty

We welcome your ideas and your contributions to the *Business Torts Journal*. We also hope to see you at the ABA's Annual Meeting in Toronto, Canada, later this summer. ■

LITIGATION ON THE WEB • www.abanet.org/litigation
Articles • Case Notes • Newsletter Archive • Program Information



Cyber-Defamation: It's Not Just Business as Usual

By Zachary G. Newman and Anthony Ellis

From starting up Facebook pages (Coca Cola has 20 million “fans”) to establishing “Twitter” accounts (Google has 2.6 million “followers”), businesses around the world are embracing the Internet and the many marketing and business opportunities it presents. Yet, businesses are also learning that the same reasons that caused them to flock to the Internet—the ability to reach millions of people in a quick and efficient manner—can also be an Achilles’ heel. To paraphrase an old idiom, the Internet is just a publishing house, and all the men and women are potential publishers. Never before has it been so easy to reach so many with such limited effort, and the simple fact is that many of those publishers are acting with both animus and anonymity.

Anticompetitive and tortious behavior abounds. Competitors are posing as fake customers, spreading false and highly damaging rumors about companies, their personnel, and their products. Consumers are utilizing company Facebook accounts and Twitter postings to levy complaints, both legitimate and illegitimate (a particular problem in our age, where purchasing decisions are increasingly based upon user reviews). In addition to these external hazards, companies are facing internal threats from their own employees. Company employees are starting so-called gripe sites to complain and critique company personnel and policies. *See, e.g., Pietrylo v. Hillstone Restaurant Group*, No. 2:06-cv-5754, 2009 U.S. Dist. LEXIS 88702 (D. N.J. Sept. 25, 2009) (former employees of the Houston’s restaurant sued their former employer when managers fired them after discovering that the employees created a password-protected gripe site to complain about the company. The employees were awarded punitive and compensatory damages based on the managers’ access of the password-protected site, despite the fact that the log-in information used by the managers to access the site was freely given by a fellow employee). The written word on the Internet seems to carry instant credibility, and smart companies are becoming hyper-vigilant in protecting their reputations and defending against illegitimate posts.

In this context, we as lawyers are being consulted about cyber-claims, and particularly cyber-defamation claims. You may be approached by a company that simply wants to know what legal recourse is available to stem a smear campaign. In other cases, clients may feel victimized or personally affronted (particularly

in the case of a competitor) and want you to use “all means necessary” to take down the defamer and those that facilitated the defamation. Before treading into the world of cyber-defamation litigation, you should be aware of the complex and unique procedural and statutory rules governing such claims in addition to those already inherent in prosecuting or defending defamation claims. For a plaintiff, these rules may mean that there is no pot of gold at the end of the rainbow; the only pot of gold is the money that your client spent chasing down the alleged defamer without success. For a defendant, there are a number of potential jurisdictional and statutory defenses that could allow your client to escape from such litigation quickly and without significant expense, but to the extent that they are ultimately found liable, there may be significant damage awards for what may appear to your client to be a fairly insignificant statement that is found to be defamatory and actionable.

Does the Claim Satisfy the Basic Elements of Defamation?

At the outset of any potential claim, it is important to understand that the foundation for these cyber-based claims is defamation law. The exact contours of a defamation claim, commonly referred to as libel for published defamation, and the specific causes of action available to a plaintiff will generally depend on the specific law that applies. In general, however, the basic elements of a defamation claim have not changed in the Internet context. A plaintiff generally needs to establish that a false statement of fact published to someone other than the plaintiff is derogatory or otherwise harms the reputation of the plaintiff; the publisher bore fault for the statement, either through negligently publishing it or acting maliciously; and the plaintiff was damaged as a result of the statements. *See, e.g., Harris v. Bornhorst*, 513 F.3d 503, 522 (6th Cir. 2008); *Bustos v. United States*, 257 F.R.D. 617, 621 (D. Colo. 2009); *Singer v. Beach Trading Co.*, 876 A.2d 885, 894 (N.J. Super. Ct. App. Div. 2005). If the statements were made about a public figure, then the plaintiff would also need to establish actual malice. *See New York Times Co. v. Sullivan*, 376 U.S. 254 (1964).

Many states recognize categories of statements that are considered so inherently derogatory that they are per se defamatory, so the plaintiff does not need to establish any special damages. Disparaging statements about a person’s criminal

record, sexual history, and trade or occupation are generally considered defamation per se. *See, e.g., Snyder v. Ag Trucking, Inc.*, 57 F.3d 484, 489 (6th Cir. 1995). Outside of such statements, however, it is critical for the attorney to make at least an initial assessment of whether the statement at issue is a statement of opinion that would likely be considered constitutionally protected speech or an actionable false statement of fact. For many derogatory statements, there may be some court precedent on the type of claim at issue that may provide the lawyer with guidance on how a court would resolve the issue. Without any precedent, however, this is often no easy task. What constitutes an opinion versus a factual statement has been the subject of numerous articles and cases over the years, and court dockets are rife with expensive and time-consuming lawsuits ending with a defense verdict or dismissal.

Moreover, truth is an absolute defense to a defamation claim, and the burden of whether the plaintiff or the defendant is obligated to prove the truth or falsity of the statement depends upon the type of claim brought. As a plaintiff, it is important to discuss and consider whether your client really wants to get into a public trial about whether the claimed defamatory statements are true. In addition, statements made in the context of a lawsuit or litigation, such as affidavits or declarations, are generally immune and privileged from defamation claims (although similar comments made to friends, acquaintances, posted online, or emailed are not). Other defenses are also available in certain jurisdictions.

Even if the potential statement was defamatory, this is merely the tip of the iceberg in determining whether, who, and where to sue, and if such a suit is commenced against your client, how you could get him or her out of the litigation.

Personal Jurisdiction in the Cyber-Defamation Context

Jurisdiction in the cyber-defamation context is not a settled issue, and courts are attempting to come to grips with the various unique issues pertaining to Internet jurisdiction generally, such as “where” something was said and “where” someone was harmed. Because of the global nature of the Internet, this is an issue that is being addressed not only by state and federal courts in the United States, but also in jurisdictions around the world. For example, what is the proper forum for dealing with a case between a Canadian citizen who purportedly spread defamatory statements about an Indiana business to a friend in India through a website owned by a Chinese company using a server based in Vietnam that the Indiana business owners learned about while on a computer in South Africa? The analysis of the proper or available jurisdictions can be dizzying and requires careful research to avoid a costly jurisdictional mistake or fight.

In the United States, jurisdiction prerequisites differ by state. Some states have adopted laws providing for jurisdiction over a cyber-defamer to the extent that the party targets people living in that state. *See Clemens v. McNamee*, 615 F.3d 374, 379 (5th

Cir. 2010) (finding that to exercise jurisdiction in Texas against a nonresident defendant, the forum must be the “focal point” of the story either by making the statements in Texas or directing the statements to Texas residents’ conduct in Texas, thus rejecting Clemens’s attempts to obtain jurisdiction over McNamee in Texas) (citing *Calder v. Jones*, 465 U.S. 783 (1984) (holding that a California court could exercise jurisdiction over a gossip columnist because the publisher expressly aimed its defamatory comments at a California resident)). For example, if a cyber-defamer commented that Bob Smith, who lived in Fort Worth, Texas, was a criminal, courts utilizing the “targeting approach” would likely find a sufficient nexus to exercise personal jurisdiction in Texas. If, however, the cyber-defamer merely criticized Bob Smith, without referencing his residence or otherwise connecting his residence to the post, then Bob Smith may have a more difficult time hauling the cyber-defamer into court in Texas. Other states have adopted entirely different approaches, permitting, for example, a plaintiff to bring suit as long as the defamed party’s reputation was damaged in that particular state. *Kauffman Racing Equipment v. Roberts*, 930 N.E.2d 784 (Ohio 2010). In those states, a cyber-defamer who lives in Maine and has never left Maine could be hauled into court in Ohio if he or she posted information that ultimately caused the plaintiff some reputational harm in Ohio (for example, posting negative comments about an Ohio business from the comfort of the defendant’s Maine living room). *Id.*

In addition to the question of whether a party could be haled into a particular forum as a defendant, there is the independent and equally important consideration of how that particular forum addresses legal issues surrounding the defamation claim, such as the statute of limitations. For example, if the allegedly defamatory statement was initially posted on a public but little-known website three years ago but only made its way onto the *Wall Street Journal*’s website (where your client noticed it) one month ago, how will the potential forum treat that claim? In the context of cyber-defamation, a plaintiff may simply not know when the “first” publication of the defamatory statement was made.

Yet, to date, courts have uniformly adhered to a “single publication” rule, meaning that with the first publication of the statement, the statute of limitations begins to accrue. *Wolk v. Olson*, No. 2:09-cv-4001, 2010 U.S. Dist. LEXIS 77694 (E.D. Pa. Aug. 2, 2010) (“The Court is not aware of any case in which the discovery rule has been applied to postpone the accrual of a cause of action based upon the publication of a defamatory statement contained in a book or newspaper or other mass medium. I reach the same conclusion as my colleagues in the Eastern District of Pennsylvania and other jurisdictions: as a matter of law, the discovery rule does not apply to toll the statute of limitations for mass-media defamation.”) (citing cases). Thus, the statute of limitations for defamation may become a critical issue in choosing where to litigate such a claim. For

a full list of state statutes of limitations for Internet libel and the corresponding citations, see REXXFIELD, LLC, Internet Libel Statute of Limitations, www.rexxfield.com/internet_libel_statute_of_limitations.php.

For a potential plaintiff, there is also the question of whether to sue in state court, federal court, or courts of lower jurisdiction (such as small-claims court, county courts, or town courts). Local courts of limited jurisdiction may offer a fast and efficient way for a client to redress his or her grievances. With respect to equitable relief, however, it is important to remember that some of these courts are not able to award equitable relief, such as ordering the removal of the defaming language from the Internet (although some could potentially condition a specific damages award on some particular action such as removing the defaming statement from the Internet). Simple and streamlined cases in courts that have the capacity to litigate expeditiously could be the perfect formula for redress in these circumstances.

Identifying the speaker is not as easy as it may sound. Many posts are made anonymously or through an untraceable screen name.

Jurisdictional issues are even more complicated when you factor in potential international forums. Internet defamation can easily target and harm a business or corporation throughout the world, and depending upon the source and the size of the defamer, these cases can easily find themselves in foreign courts. Should you consider and discuss with your client the costs, benefits, and potential pitfalls of commencing suit in the United Kingdom, Australia, or even Canada, assuming that they were able to satisfy the jurisdictional prerequisites? If a claim is barred in the United States, could it be pursued abroad? Globally, each country, and perhaps each province, state, or territory within that country, may have its own jurisdictional requirements, and in the context of a global defamation claim, U.S. lawyers practicing in this arena may quickly become familiar with these standards as well. Given that significant libel and defamation awards have been handed down by foreign courts, depending on the specific standards and statute of limitations issues, your client's best or most appropriate opportunity at redress may be in a foreign jurisdiction. *See, e.g., Totalise plc v. Motley Fool Ltd.*, [2001] EWCA Civ 1897 (appeal taken from Q.B.) (U.K.), available at www.bailii.org/ew/cases/EWCA/Civ/2001/1897.html (demanding disclosure of anonymous bloggers and ordering bloggers to

pay the plaintiff's attorney fees); *Black v. Breeden*, [2010] ONCA 547 (Can.), available at www.ontariocourts.on.ca/decisions/2010/august/2010ONCA0547.htm (rejecting jurisdictional challenge and permitting Conrad Black to proceed in a libel suit against Hollinger International in Ontario based on the theory that the republishing of Hollinger International press releases by papers distributed in Canada caused him harm in that province).

Cyber-Defamation Defendants

The Speaker

Although you may think that the defendant in the cyber-defamation context is clearly the speaker (or writer), this is often not the case. In the cyber-world, identifying the speaker is not as easy as it may sound. Many posts are made anonymously or through an untraceable screen name.

To identify anonymous speakers, parties, depending on the applicable procedural rules, can commence suits against John or Jane Doe and begin using subpoena power on the service providers and host sites. *See, e.g., Doe I and Doe II v. Individuals*, 561 F. Supp.2d 249 (D. Conn. 2008). Pre-action discovery could also be available, depending on the jurisdiction. *See* John P. McCahey and Anting Wang, Hahn & Hessen, LLP, *Pre-Action Discovery in the Digital Age*, 2009 LexisNexis Emerging Issues 4554 (Nov. 2009). But be warned, this is not a simple assignment. Courts have recognized that, as in the traditional speech context, the First Amendment protections afforded to anonymous speech extend to the Internet arena. Because the Supreme Court simply has not addressed the proper standard for balancing the free speech rights of the anonymous speaker against the right of the defamed plaintiff to redress, courts have developed a wide variety of standards for addressing the issue. Some courts, for instance, have created a set of enumerated factors. *See Enterline v. Pocono Medical Center*, No. 3:08-cv-1934, 2008 U.S. Dist. LEXIS 100033 (M.D. Pa. 2008) (applying a four-part test); *Doe I*, 561 F. Supp. 2d at 254–55 (setting forth a six-factor test). Other courts have adopted a fairly strict test, requiring the party to establish that he or she would be able to prevail on a motion for summary judgment for all elements of their defamation claim based upon evidence within its control—i.e., “not dependent on knowing the identity of the poster.” *See, e.g., Ecommerce Innovations, LLC v. Doe*, No. MC-08-93-PHX-DGC, 2008 U.S. Dist. LEXIS 99325 (D. Ariz. Nov. 25, 2008).

Another consideration is that while some courts have ordered the disclosure of otherwise anonymous posters, pursuing the name of the speaker through litigation could be very expensive and time-consuming. *In re Anonymous Online Speakers, Anonymous Online Speakers v. United States District Court for the District of Nevada Reno*, 611 F.3d 653 (9th Cir. 2010) (affirming a district court order requiring an online content manager to disclose the identities of certain comment posters based on allegations by a business that its competitors were engaging in an anonymous smear campaign to injure its reputation); *In re*

Subpoena Duces Tecum to Am. Online, Inc., 52 Va. Cir. 26 (Va. Cir. Ct. 2000) (ordering the disclosure of identities from the ISP of parties that allegedly disclosed confidential trade secrets and defamed the business), rev'd on other grounds by *America Online, Inc. v. Anonymous Publicly Traded Co.*, 542 S.E.2d 377 (Va. 2001).

As counsel, you should discuss with your client whether, from an economic standpoint, it makes financial sense to initiate a lawsuit. For example, if the defamer is someone who is likely to be judgment-proof, obtaining a monetary judgment against him or her may have little benefit for your client. Given the costs associated with such discovery, you also need to determine whether your investigation should include efforts to identify potential defendants that may have facilitated or republished the defamatory statements. You will likely have to justify your actions to your client, particularly if your efforts fail to uncover the perpetrator, so you should make sure up front that both you and your client are comfortable with and confident in the discovery plan to be followed. From a defense perspective, if you find yourself in receipt of one of these subpoenas, your client may or may not be compelled to divulge information about its customers, as the law differs from jurisdiction to jurisdiction.

Best practices mandate that the lawyer conduct a thorough review of the law pertaining to these types of disclosures, understand recent decisions that can impact strategy, and fully explain to the client the legal risks, benefits, and projected costs.

One potential avenue that could avoid the costs and expenses of litigation is retaining a third-party consultant or investigator to assist in identifying the speakers. Dozens of firms are sprouting up as these suits become more and more common, and many of them boast of significant success in identifying the perpetrators. *See, e.g.*, REXXfield, LLC, Digital Forensics, Investigations & Litigation Support, www.rexxfield.com/libel_law_suit.php (noting that “in most Doe cases (unidentified defendants) we can positively identify the offenders using proprietary investigative techniques as well as carefully crafted subpoenas and orders, and noting an 80–90% success rate”).

The Internet Service Provider

In addition to the speaker or poster of the information, there could be a claim available against web hosting services and Internet Service Providers (ISPs) for the websites where the comments were posted on the theory that they republished the incriminating statements. Initially, it may seem like an easy decision to sue the ISP—financial recovery may seem more likely from an ISP than from the creator of the post—but there are in fact significant statutory defenses available to such service providers in the context of cyber-defamation claims.

Section 230 of the Federal Communication Decency Act of 1996 (CDA) explicitly provides that “no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider” (CDA, 47 U.S.C. § 230(c)(1) (1996)), and

further that “no cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section.” § 230(e)(3). Based on this language, courts have regularly dismissed claims against websites that post third-party comments and information that were allegedly defamatory. *See, e.g., Reit v. Yelp!, Inc.*, 907 N.Y.S.2d 411 (N.Y. Sup. Ct. 2010) (dismissing a defamation claim against Yelp! for allegedly defamatory negative comments about the plaintiff’s dental practice). A highly regarded Internet defamation lawyer and author, Aaron Morris, has used the very apt analogy that “naming an Internet Service Provider in an Internet defamation action is akin to naming Microsoft as a defendant because the defamer used Word to type the defamatory statements.” *See* <http://internetdefamationblog.com>.

Whether the website host is ultimately immune from a defamation suit will likely depend on the level of involvement it has or had with the speech and speakers who post on its site and whether the website arguably was involved in encouraging illegal conduct. In one noteworthy recent case from the Ninth Circuit, *Fair Housing Council of San Fernando Valley v. Roommate.com, LLC*, 521 F.3d 1157 (9th Cir. 2008), the court held that because Roommate.com’s website was structured in such a way that users submitted information that was then posted by Roommate.com, the website crossed over from being merely an interactive computer service (with no liability for the statements) to being an information content provider that could potentially be liable for defamatory posts on its site. Yet, even getting to the position where you can tell the type of information service provider with which you are dealing may itself require significant amounts of time and the retention of an expert who can navigate the technical details and nuances of the posting technology.

Anti-SLAPP Laws

Another aspect of potential defamation claims is what are commonly referred to as anti-SLAPP laws. Strategic lawsuits against public participation (SLAPP) are designed to silence people from making otherwise protected but unwanted speech, such as legitimate consumer opinions or complaints. California led the United States with anti-SLAPP litigation, offering potential defendants an allegedly quick and efficient means of dismissing such complaints. Cal. Civ. Pro. § 425.16. If the alleged defamation fell within a specific category of protected statements, defendants could file a short motion establishing that the speech was protected and effectively stay all discovery pending resolution of the motion. If the motion is denied, the order is immediately appealable. If the defendant prevailed, then the plaintiff is obligated to pay for the defendant’s attorney fees. Ultimately, faced with what many people considered abuse of anti-SLAPP legislation, California carved out from the procedure suits involving commercial issues and made other changes to the anti-SLAPP legislation, but this provision

remains an important potential consideration for anyone considering filing a defamation suit. Cal. Civ. Pro. § 425.17.

Twenty-six states, including Arizona, Arkansas, Delaware, Florida, Georgia, Hawaii, Illinois, Indiana, Louisiana, Maine, Maryland, Massachusetts, Minnesota, Missouri, Nebraska, Nevada, New Mexico, New York, Oklahoma, Oregon, Pennsylvania, Rhode Island, Tennessee, Utah, Vermont, and Washington, have enacted their own anti-SLAPP legislation, and Colorado and West Virginia have adopted non-statutory protections against SLAPP lawsuits. Similar legislation has been introduced at the federal level. *See* The Citizen Participation Act, H.R. 4364, 111th Cong. (2009). In any case, in determining where and whether to file suit, counsel should consider the relevant anti-SLAPP legislation and its potential applicability to the client's case.

Conclusion

The question of whether a client should initiate a lawsuit for Internet defamation is one that requires careful consideration of the costs and risks. It is often extremely difficult to determine what a court will conclude is actionable "defamation" and what is protected "opinion." For example, a customer's opinions about his or her experience with a particular product, such as "this product is awful" are likely protected First Amendment speech that is not actionable. As we noted above, there are also serious potential costs to pursuing a potential defamation suit with significant risks to obtaining any meaningful recovery. Finally, the litigant must weigh the potential for reputational damage in the community tied to pursuing litigation, such as having to republish the harmful statements in court and in pleadings. *See* www.

internetdefamationblog.com/category/case-results.

Faced with these significant barriers to suit, it is perhaps the best approach for counsel to first explore constructive pre-suit measures to resolve the dispute. In some cases, the client may be able to have the offensive commentary removed by sending a traditional cease-and-desist letter. Sending such a letter before initiating litigation may also have an added benefit of lending credibility to a claim that the defendant was acting in bad faith by refusing to remove the defaming commentary. *See Northern Light Tech., Inc. v. Northern Lights Club*, 236 F.3d 57, 65 (1st Cir. 2001) (affirming the district court's consideration of failure to remove content after receiving a cease-and-desist letter as a factor in the bad-faith determination). Of course, sending an inappropriate and over-the-top cease and desist letter could have the opposite effect. *See Green v. Fornario*, 486 F.3d 100 (3d Cir. 2007) (noting that an attorney who sent a cease-and-desist letter threatening criminal conduct for civil violations acted unwisely).

Nonetheless, if the client finds itself in the courthouse (whether to prosecute or defend), counsel is well advised to ensure that the client fully understands the risks as well as the potential rewards, the costs, and the potential for additional reputational damage so that the client's decision to litigate the issues is an informed one. ■

Zachary G. Newman is a partner and Anthony Ellis is an associate with Hahn & Hessen, LLP, in New York, New York. Both are members of the firm's Litigation Practice Group. The authors thank Aaron Morris for providing some of the background material used to prepare this article.

WE'RE GOING DIGITAL!

By Fall 2011, the ABA Section of Litigation will distribute all newsletters via email only.



Visit americanbar.org/myaba to:

- ➔ Join up to 37 Committees to receive practice-specific e-newsletters
- ➔ Add or update your email address



Avoiding an Electronic Discovery Disaster with Litigation Holds

By Elizabeth S. Fenton, Diana Rabeh,
and Jonathan M. Shapiro

The U.S. government estimates 206,000,000 barrels of oil flowed from the explosion of BP's rig into the Gulf of Mexico. Dina Cappiello, "New BP Challenge to Spill Size Could Affect Fine," *Associated Press*, Dec. 3, 2010, available at <http://abcnews.go.com/Business/wireStory?id=12306686>. BP has confirmed that the cost of the Deepwater Horizon oil spill is \$1.6 billion as of December 1, 2010. There are 1 trillion bytes of data in the form of documents, emails, voice mails, text messages, and instant messages expected to be retrieved from BP's electronic discovery. William W. Belt Jr., *Electronic Discovery Challenges in BP Oil Spill Cases*, The e-Discovery 4-1-1, Aug. 2010, <http://marketing.leclairryan.com/files/Uploads/Documents/e-Discovery%204-1-1%20August%202010.pdf>. The sheer volume of electronic data will cause the Deepwater Horizon oil spill to become one of the largest electronic discovery events in history.

In the wake of events like an oil spill, natural disaster, or other catastrophic event, clients find themselves confronting urgent duties regarding the maintenance and preservation of electronic evidence, duties that may possibly burden their ability to conduct operations going forward. As litigators, especially as business torts litigators, it is imperative that we provide effective guidance to clients both before and during litigation to ensure that these duties are met and to minimize—to the degree possible—the burden on their business so that a disaster does not become an e-discovery disaster as well.

Although the explosion of electronic discovery over the years alone warrants heavy emphasis on having a proper system in place to respond to pending or anticipated litigation, a disaster such as the Deepwater Horizon oil spill reminds us that work done before a crisis will pay off when the inevitable crisis comes. In the face of an overwhelming amount of daily electronic communication and the relative ease of spoliation, we must advise our business clients of the triggers for the common-law duty to preserve evidence and assist them in developing policies and practices to ensure that the duty is met when it arises. We must also advise them that the high costs associated with electronic discovery coupled with the risks of sanctions in the event of data destruction, even inadvertent destruction, make ignoring such a duty perilous.

The Law Governing Litigation Holds

A litigation hold is simply a communication within a company that requires that all information—whether paper or electronic—relating to the subject of a current or an impending litigation be preserved for possible production in the litigation. The 2003 landmark case, *Zubulake v. UBS Warburg, LLC*, popularized the use of the litigation hold to satisfy preservation obligations imposed on parties. The court explained that “[o]nce a party reasonably anticipates litigation, it must suspend its routine document retention/destruction policy and put in place a ‘litigation hold’” to safeguard all relevant data. *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212, 218 (S.D.N.Y. 2003); see also *ACORN (N.Y. Ass’n of Cmty. Org. for Reform Now) v. County of Nassau*, No. 05-2301, 2009 WL 605859, at *2 (E.D.N.Y. Mar. 9, 2009) (explaining that once the duty to preserve arises, “a litigant is expected, at the very least, to suspend its routine document and retention/destruction and to put in place a litigation hold” (internal citation omitted)).

“[W]hile a litigant is under no duty to keep or retain every document in its possession, it is under a duty to preserve what it knows, or reasonably should know, is relevant in the action, is reasonably calculated to lead to the discovery of admissible evidence, is reasonably likely to be requested during discovery and/or is the subject of a pending discovery request.” *Wm. T. Thompson Co. v. General Nutrition Corp.*, 593 F. Supp. 1443, 1455 (C.D. Cal. 1984). The purpose of a litigation hold is to prevent the automatic destruction of potentially relevant or discoverable documents and information pursuant to a document retention policy.

Amendments to the Federal Rules of Civil Procedure that took effect on December 1, 2006, codified the evolving obligation for companies to preserve, collect, and produce “electronically stored information.” Except for a Note to Rule 37(f), which references the use of a “litigation hold” as a method of implementation, the Federal Rules do not define the scope of the preservation obligation under a litigation hold per se and do not expressly require litigants to adopt a “litigation hold.” Similarly, although the Delaware Court of Chancery recently issued guidelines regarding the preservation of electronically stored information, few other courts have done so. See Court of Chancery Guidelines for Preservation of Electronically

Stored Information, available at <http://courts.delaware.gov/forms/download.aspx?id=50988>. Nonetheless, many district courts have determined that the “utter failure to establish any form of litigation hold at the outset of litigation is grossly negligent” and subject to sanctions. *Heng Chan v. Triple 8 Palace, Inc.*, No. 03-CIV-6048, 2005 WL 1925579, at *7 (S.D.N.Y. Aug. 11, 2005). As one judge recently explained, “By now, it should be abundantly clear that the duty to preserve means what it says and that a failure to preserve records—paper or electronic—and to search in the right places for those records, will inevitably result in the spoliation of evidence.” *Pension Comm. of Univ. of Montreal Pension Plan v. Bank of Am. Secs., LLC*, 685 F. Supp. 2d 456, 462 (S.D.N.Y. 2010).

When Is the Duty to Preserve Triggered?

Because the duty to preserve is not necessarily triggered at the commencement of litigation, it is imperative that a company be aware of when the duty to preserve documents and issue a litigation hold arises. “The duty to preserve material evidence arises not only during litigation but also extends to the period before the litigation when a party reasonably should know that the evidence may be relevant to anticipated litigation.” *Silvestri v. General Motors Corp.*, 271 F.3d 583, 591 (4th Cir. 2001); see also *Jacob v. City of New York*, No. 07-cv-04141, 2009 WL 383752, at *1 (E.D.N.Y. Feb. 6, 2009) (“[The] obligation to preserve evidence arises when the party has notice that the evidence is relevant to litigation or when a party should have known that the evidence may be relevant to future litigation.”). When the duty to preserve is triggered, a party must take reasonable steps to preserve relevant and/or discoverable information, which includes “what it knows, or reasonably should know, is relevant in the action, is reasonably calculated to lead to the discovery of admissible evidence, is reasonably likely to be requested during discovery and/or is the subject of a pending discovery request.” See *Wm. T. Thompson*, 593 F. Supp. at 1455. A party who fails to preserve and produce information as required may be subject to a range of sanctions. *Id.* (“Sanctions may be imposed against a litigant who is on notice that documents and information in its possession are relevant to litigation, or potential litigation, or are reasonably calculated to lead to the discovery of admissible evidence, and destroys such documents and information.”).

Although this rule may appear straightforward, its application can be hard to pin down in some situations. For example, when an unexpected disaster strikes, many would argue that the duty to preserve arises almost immediately at the outset of the disaster. At least one commentator has speculated that the duty to preserve arguably arises before disaster strikes, particularly where the disaster is “man-made” or the result of ongoing negligence. Maribeth L. Minella, *BP Oil Spill Demonstrates Why Litigation Hold Instructions Are Invaluable*, Delaware Employment Blog, June 16, 2010, www.delawareemploymentlawblog.com/2010/06/bp_oil_spill_demonstrates_why.html. Suffice it to say that

“[d]etermining whether a duty to preserve is triggered is fact-intensive and is not amenable to a one-size-fits all or a checklist approach.” The Sedona Conference, “The Sedona Conference Commentary on Legal Holds: The Trigger & the Process,” 11 *Sedona Conf. J.* 265, 271 (2010).

The Sedona Conference, recognizing that determining when the duty to preserve is triggered can be difficult, has provided a number of guidelines to practitioners. *Id.* First, the Sedona Conference defines “reasonable anticipation of litigation” as arising “when an organization is on notice of a credible probability that it will become involved in litigation, seriously contemplates initiating litigation, or when it takes specific action to commence litigation.” *Id.* at 269. This determination “should be based on a good faith and reasonable evaluation of relevant facts and circumstances.” *Id.* at 270. Important reasonable facts and circumstances for a company to consider include:

- The nature and specificity of the complaint or threat;
- The party making the claim;
- The business relationship between the accused and accusing parties;
- Whether the threat is direct, implied or inferred;
- Whether the party making the claim is known to be aggressive or litigious;
- Whether a party who could assert a claim is aware of the claim;
- The strength, scope, or value of the known or reasonably anticipated claim;
- Whether the company has learned of similar claims;
- The experience of the industry, and
- Reputable press and/or industry coverage of the issue either directly pertaining to the client or of complaints brought against someone similarly situated in the industry.

Id. at 276.

Accordingly, because the duty to preserve documents may arise well before a complaint has been filed or a subpoena is served, a company must be cognizant of the factors outlined above and must consider the necessity of a litigation hold whenever a claim or threat of a claim first comes to light.

Best Practices for Implementing Litigation Holds

Companies should not wait until disaster strikes or litigation is commenced to start thinking about how best to manage and protect their electronic data. The following practice tips are designed to assist companies in managing, storing, and protecting electronically stored information and implementing a proper litigation hold.

Be Prepared

Before drafting a litigation-hold policy, a company should set forth a “policy or practice setting forth a process for determining

whether the duty to preserve information has attached.” *Id.* at 274. As the Sedona Conference explained, “[A]dopting and consistently following a policy or practice governing an organization’s preservation obligations is one fact that may demonstrate reasonableness and good faith.” *Id.* In addition, a company must know how its electronic data is stored, backed up, and archived so that it can draft a proper litigation-hold policy. Specifically, companies should be aware of potential “evidence destroyers” and problem areas such as the automatic deletion of email, the recycling of backup tapes, the upgrading and reformatting of systems, laptop computers, home computers, portable storage devices such as flash drives, and personal email accounts.

Be Proactive

Businesses should periodically review and monitor their document-retention policies before a situation necessitates the implementation of a litigation hold. By being proactive, a company can determine if there are any holes or deficiencies in the policy or its implementation and whether the policy needs to be updated. This step is also critical to a later showing of good faith, as Rule 37(e) provides that “[a]bsent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system.” Fed. R. Civ. P. 37(e). The protection of this provision may be lost, however, if—after the duty to preserve is triggered—the retention policies are not suspended or modified.

Set Up an Electronic Discovery Team

For larger companies and/or legal departments, the time and resources dedicated to putting together an e-discovery team are well worth it. This team should consist of not only legal personnel but technology personnel as well. Technology personnel will be particularly important for ensuring the suspension of the automatic deletion of email, the recycling of backup tapes, and the upgrading and reformatting of systems. It is also important to designate and train a member of the electronic discovery team to handle inquiries from employees about claims or threats of litigation, the duty to preserve, and other questions regarding the litigation hold.

Identify Key Players

When litigation is reasonably anticipated, a business must quickly implement an effective litigation hold and make sure all sources of potentially relevant information are identified and placed on hold. To do so, a company must identify and interview the key players in the litigation as quickly as possible. It is important to note that it may be necessary to extend the litigation hold beyond the key players to “appropriate date stewards, records management personal, information technology (IT) and other potentially knowledgeable personnel.” Sedona Conference, *supra* p. 10, at 283.

Issue Effective Litigation-Hold Policy Promptly

When a company issues a hold notice, the company should disseminate it to its employees both electronically and via interoffice mail. The litigation hold should also include the following information:

- A description of the case in laymen’s terms;
- Instruction on which documents should be preserved and how such documents should be preserved;
- Instruction that any automatic deletion of email or other electronic media should be suspended;
- Instruction for recipients to search all information for anything relevant or potentially relevant to the claim and to err on the side of preserving;
- An explanation to recipients about the risk to the company and its employee for failing to heed the litigation-hold request; and
- Contact information for the designated person from the e-discovery team, or an in-house or outside lawyer.

A company must know how its electronic data is stored, backed up, and archived so that it can draft a proper litigation-hold policy.

The widespread use of electronic discovery makes it vital for litigants to employ litigation holds as soon as a claim or potential claim is reasonably anticipated. The failure to timely implement a litigation hold may not only result in spoliation but may also be costly to a party in the form of court-ordered sanctions, including the entry of a default judgment. One court even went so far as to suggest the imposition of jail time for spoliation. *See* Sean T. Carnathan, “Jail Time for Spoliation?” 36-2, *Litigation News*, Winter 2011, at 17. In *Victor Stanley, Inc. v. Creative Pipe, Inc.*, 269 F.R.D. 497 (D. Md. 2010), Magistrate Judge Paul W. Grimm of the U.S. District Court for the District of Maryland determined that the defendant’s willful acts of spoliation warranted not only partial default judgment in favor of the plaintiff but also constituted civil contempt. *Id.* at 500. The court ordered the culpable individual defendant to be “imprisoned for a period not to exceed two years unless and until he pays to Plaintiff the attorney’s fees and costs” allocable to spoliation. *Id.* (internal citations omitted). In later proceedings, U.S. District Judge Marvin J. Garbis modified the sanctions to eliminate the potential for

jail time, reasoning that it was not appropriate to order the individual “[d]efendant incarcerated for future possible failure to comply. . . .” See *Victor Stanley, Inc. v. Creative Pipe, Inc.*, D.C. Md., C.A. No. MJG-06-2662, Garbis, J., at *3 (Nov. 1, 2010) (Memorandum and Order). Businesses cannot afford to take the requirement that they issue litigation holds lightly.

Be Over-Inclusive

It doesn’t hurt to be over-inclusive in determining which documents should be placed in the litigation hold, and employees should always err on the side of caution. Although preserving and collecting massive quantities of data can be expensive, this cost must be weighed against the very real threat of spoliation and the issuance of sanctions. Thus, until a company is aware of what discovery requests it will face in the future, it is recommended that companies preserve their data very broadly.

Be in Control

It is necessary not only to implement a litigation hold but also to continually take affirmative steps to monitor compliance. The monitoring and testing of a litigation-hold policy ensures that employees are following the policy and that its data has been safeguarded. In *Zubulake*, the court explained that litigation-hold responsibilities do not end with the issuance of the litigation hold: “Counsel must oversee compliance with the litigation hold, monitoring the party’s efforts to retain and produce the relevant documents.” *Zubulake*, 229 F.R.D. at 432. This is especially true where a company may face criminal charges and employees may be tempted to delete or alter information that might get them in trouble. Throughout the process,

counsel should document the steps taken to both ensure compliance and prevent the destruction of potentially relevant electronically stored information.

Keep Communications Open

A company should communicate with its employees to ensure that the litigation hold has been effectively implemented, while counsel is, at the same time, having ongoing conversations with opposing counsel and the court on the status and progress of electronic data. This is especially true where discovery may involve particular areas of sensitivity.

Conclusion

No one can predict when disaster will strike, but a company can and should prepare itself for disasters that might arise and take steps to minimize the risk of secondary electronic discovery disaster. As litigators, we play an instrumental part in ensuring that our business clients are prepared if disaster strikes. To adequately prepare our clients and provide effective guidance, we must follow the best practices outlined above for implementing an effective litigation-hold policy. The high costs of electronic discovery, as well as the risk of sanctions in the event of spoliation, even inadvertent, make it imperative that we assist our clients in proactively implementing policies and practices to ensure that the common-law duty to preserve is met. ■

Elizabeth S. Fenton is a partner and Diana Rabe is an associate at Reed Smith, LLP, in Wilmington, Delaware. Jonathan M. Shapiro is a partner with Shapiro Law Offices, LLC, in Middletown, Connecticut.

Find Us on Twitter and Facebook.

Find timely articles and news updates,
CLE program information, and recent podcasts for litigators.



Follow @ABALitigation
on Twitter



“Like” The ABA Section
of Litigation on Facebook





Using Virtual Data Rooms to Your Advantage

By Amy M. Stewart and Meghan E. Bishop

Virtual data rooms (VDRs) have in some respects replaced the traditional “brick and mortar” data rooms traditionally used by businesses to share large volumes of confidential information with third parties. While VDRs are most commonly used to allow potential buyers or investors to perform “due diligence” reviews of assets in the context of debt or equity financing, mergers and acquisitions (M&A), or in bankruptcy sales and/or liquidation, VDRs are also increasingly utilized to store and manage discovery materials in document-intensive litigation. There are important issues that the hosting party should consider prior to a VDR going “live,” such as the sensitivity of documents that will be available, whether access to certain information will be limited or restricted based on the stage of the sale or other process necessitating the review, clearly communicating the VDR “rules” to reviewers, and drafting and having executed appropriate confidentiality or disclosure agreements, to name a few.

In the litigation context, VDRs typically come into play in one of two scenarios—either as a tool for assembling and/or producing electronic evidence or as a substantive source of evidence in the dispute. When hosts employ a VDR provider that cannot provide auditing features, or choose not to employ the preventative, defensive-minded measures that are available in current VDR technology, such neglect can complicate future litigation, including efforts to hold reviewers accountable for their misuse of the information disclosed in the VDR. Furthermore, not employing these measures can expose the host to litigation stemming from the information that was or was not provided in the VDR. *In re Topps Co. Shareholders Litigation*, 926 A.2d 58, 81 (Del. Ch., 2007).

The Governing Documents Define the Rules of Play

By the time a lawsuit actually ensues, the governing documents are usually already in place, leaving the litigator to deal with the advantages or disadvantages of the underlying contract language previously negotiated by the parties. Key provisions for litigators to consider and evaluate in transactions involving VDRs include the terms and scope of the confidentiality and/or nondisclosure agreement, the terms and scope of the noncompete provisions, and warranty and representation provisions.

When Was the Confidentiality Agreement in Effect?

Most confidentiality agreements limit the time period during which information must remain confidential. While there is no “usual” term for a confidentiality agreement, it is rare for the term to be less than one year. Normally, the term is a function of the nature of the business and the specific assets that are part of the potential deal. If information related to the transaction is particularly time-sensitive—meaning that the significance of data has a short life span—then it would not be unlikely to encounter a one- to three-year term. If the information could reveal significant technical or business advantages to endure for an extended period of time, then a longer time frame was probably negotiated and agreed to by the parties. In either event, to be actionable, any alleged breach of the confidentiality agreement must occur within the span of time prescribed under the confidentiality agreement.

What Is the Scope of the Confidentiality Agreement?

Assuming the confidentiality agreement was in effect at the time of the alleged wrongdoing, the litigator must next determine what information disclosed in the VDR, and possibly during the underlying transaction, is considered confidential. Defining what is and what is not confidential is often the most important part of the confidentiality agreement, and the most litigated. An initial determination should be made as to how the confidentiality agreement defines that which is confidential—that is, whether it is limited to that information disclosed by the seller to the reviewer or whether it is defined by the *nature* of the information, rather than the means by which it was communicated. In other words, does the definition focus on the manner in which the information is conveyed (i.e., provided by the seller or host in the VDR or otherwise) or the inherent confidential character (due to particular sensitivity) of the information, without regard to how or by whom such information is communicated. This latter approach is arguably better from the seller’s standpoint, as it “follows” the information, rather than the means by which the information is communicated.

For example, suppose a host wants to file breach of contract or trademark infringement claims against a VDR reviewer who has used information disclosed during the

review in a manner the host believes to be outside the scope of that intended by the parties. It will be important to determine whether the confidentiality agreement covers only information that was disclosed in the VDR or if it is broad enough to cover information that was provided in the course of the transaction by employees or third-party agents of the host, or even outside the transaction by rogue employees or third parties acting outside the scope of any agency relationship. This could be a critical determination in the context of litigation based on the actions of a reviewer given access to the host's confidential data but with whom a deal ultimately was not finalized. It is not uncommon for potential purchasers or other reviewers to feign interest in the underlying transaction solely to gain access to the information uploaded into the VDR and to which it would otherwise not have access. It is important to determine whether the "veil" of confidentiality remains in place under these circumstances.

Do the Governing Documents Include "Noncompete" Clauses?

After determining the scope of the confidentiality clause, the next determination is whether or not a noncompete provision or other restrictive covenant was included in the governing documents. From the host's perspective, these clauses help to further safeguard against third parties wrongly using information obtained through a VDR or otherwise exchanged during a sale or other due-diligence process. Several of the considerations described earlier should again be evaluated in the context of restrictive covenants included in the governing documents—i.e., was it still in effect at the time of the alleged breach, who is bound and under what circumstances are those persons bound by the restrictive covenant.

Defining who knew what, when, and how is the essence of a knowledge qualifier.

Other considerations include whether a "noncompete" penalty clause was included in the governing documents. Instead of an outright prohibition on competition, such a clause typically provides that in the event of a competitive use of the information, the reviewer will be obligated to pay a specified amount of damages to the host of the VDR providing the confidential information that served as a basis for the transaction. For example, in the context of an oil and gas transaction, some exploration and production (E&P) companies trying to sell assets will require a potential purchaser that views confidential data during the sales process and who later purchases assets

from a different entity in the same geographical region to pay the E&P company a specified percentage interest in the assets purchased. Other restrictive covenants often encountered and of which a litigator should be aware are non-solicitation provisions restricting a party from soliciting employees, vendors, or customers and, if the disclosing party is publicly traded, "standstill" provisions that prohibit a reviewer from acquiring any stock of the disclosing party (to prevent a possible hostile takeover) and clauses reminding the reviewer of its duties under applicable insider-trading laws.

What Warranties and Representations Were Made in the Governing Documents?

Breach of warranty and/or misrepresentation claims can arise under circumstances when the invitee alleges that the host failed to provide or misrepresented certain vital information in the VDR prior to his or her purchase of an asset. In analyzing the viability of the claims, the litigator needs to evaluate the warranty and representation section contained in the governing documents to determine what representations and warranties were made relating to the host's responsibility to disclose material information in the VDR for the reviewers to review. Specifically, the litigator should determine, under the terms of the governing documents and possibly as required by law, what material information must be disclosed, whether the representations or warranties were "clean" or "qualified," and whether the governing documents provided a disclosure schedule of when and under what circumstances the host would provide material information to the reviewers.

If a "knowledge" qualifier has been used (e.g., "To the seller's knowledge, no claims are asserted against it or the assets. . ."), VDRs can be especially important because defining who knew what, when, and how is the essence of a knowledge qualifier. Furthermore, a potential purchaser having viewed a document (this can be traced through the use of a VDR) and therefore having knowledge of a certain key piece of information can prove critical for defending a lawsuit based on the breach of a representation or warranty. Likewise, if a potential purchaser did not have access to certain information (either by being blocked in that section of the VDR or otherwise) and can show such, then this information could prove useful in prosecuting a breach of representation or warranty claim. *See In re Topps*, 926 A.2d 58, 81.

A VDR's Security Features

Any claim based on information contained in a VDR will generally involve at least two questions. First, what documents were uploaded to the VDR (and which ones were not), and second, what documents were actually reviewed? The first question is easily answered, regardless of the VDR provider; however, proof of the second question is dependent upon the inherent capabilities of the VDR service provider. Nicholas Renter, a regional sales director for the Greater Texas Region for Merrill DataSite,

a VDR provider, believes that when initially analyzing the potential of future litigation, a litigator should request the following information to determine how helpful the auditing features of the particular VDR site purchased will be in developing evidence to either support or defend against future litigation.

It is important to determine whether the VDR provider allows an invitee to search all page-based file types included in the VDR on a page level. This will enable users to realistically review tens of thousands of pages. Alternatively, it will allow the host to analyze what information his invitees have searched based on each invitee's specific search criteria. In addition, it is important to determine whether your VDR provider can provide a report on which documents were reviewed and printed down to the individual page level. Further, it may be important to determine when, down to 1/100 of a minute, a document page was reviewed by an invitee. When initially setting up the VDR, some consider these features unnecessary. However, should litigation arise, they are absolutely critical.

Track Documents Reviewed

Viewer tracking is a must-have security feature that can diffuse potential "failure to disclose" litigation or substantiate your client's claims that the not-so-well-intentioned third party used confidential information provided in the VDR in a manner not contemplated by the host. For example, in a trade secrets case, a first line of defense often raised is that the alleged misappropriator did not use the "trade secrets," but instead based its business decisions on information legitimately obtained from other sources. A VDR can help in this case by easily showing not only that the alleged misappropriator viewed confidential information, but also when, for how long, and whether such information was flagged or printed and removed off-site. This could prove crucial for proving that the reviewer accessed the information in the VDR, when it was accessed, and the extent to which it was printed or otherwise downloaded. This evidence, when combined with other evidence or what was publicly or otherwise available, can be compelling in proving the trade secret claim.

Track a Viewer's Activity in the VDR

Another line of defense is to have your VDR service provider supply reports on a viewer's activity while inside the VDR. Activity reporting can provide up-to-the-minute information regarding how long a viewer was in the system, what documents were reviewed, how many times they were viewed, how much time was spent reviewing those documents, and whether the documents were printed. In the alternative, activity reporting may show that a reviewer had a practice of logging into the VDR but not actually viewing documents.

One risk that is inherent in any sales process and especially in an auction scenario is "data mining." This is the practice of a potential purchaser presenting itself under the guise of being interested in pursuing a transaction when it is actually interested

only in learning its competitor's business information, much of which is likely sensitive and confidential, for its own competitive advantage. A VDR feature allowing a host to track the type of information being viewed arms a seller with knowledge that may send signals as to a potential purchaser's true intent. For example, assume a potential purchaser and the seller are rivals in highly competitive oil and gas play. If the potential purchaser spends the bulk of its time reviewing well data, without reviewing other information that would give a broader picture of the company as a whole, this could be one indicator that the potential purchaser has no intention of making an offer and, instead, is focused on data mining for improper purposes.

Roll Out Information on a Need-to-Know Basis

One way to protect your client's confidential information from not-so-well-intentioned viewers is to roll out the confidential materials on a staggered or need-to-know basis. This is particularly helpful in an auction context, where bidders are narrowed down from a large pool of initial bidders. The idea is that basic company information on general corporate matters, organization information, capital stock, basic financial information, and tax matters will be initially available to all users. As the pool of serious bidders is narrowed, access can then be given to more sensitive information regarding the assets, contracts, employees, etc. Users should be made aware at each stage of the "unveiling" what type of information will be available.

Require the User to Reaffirm the Confidentiality Agreement

A final security measure to consider, in addition to requiring a VDR user to reaffirm the confidentiality agreement upon log-in, is to require a user to reaffirm the agreement at various stages of review. To do so upon each page may be overly cumbersome, but a periodic reaffirmation upon moving into a new category of information (e.g., general corporate matters and contracts) will reinforce that the material contained therein is subject to a confidentiality agreement and helps overcome a potential argument that a user did not understand what material was and was not covered by the confidentiality provisions.

Conclusion

VDRs are changing the landscape of how corporate transactions are structured and, in turn, are changing the game for deal-related litigation. They can be a powerful tool for managing data and tracking the review of information. With careful thought and planning at the outset, VDR technology can be a powerful tool to protect your client's interest not only in the underlying transaction for which it is employed, but also in any litigation that may arise out of that transaction. ■

Amy M. Stewart is an associate with Cox Smith Matthews Inc. in Dallas, Texas. Meghan E. Bishop is an associate with Cox Smith Matthews Inc. in San Antonio, Texas.



Achievable Steps to Discovery Cost Management

By Thom Wisinski and Randy Girouard

Cost, cost, cost. The client doesn't want to spend any money. Why am I paying to process electronic documents? If they're electronic, shouldn't a machine just be able to do it? Why don't we just produce everything in native format? These are just a few of the many anecdotal comments we hear when we mention discovery costs. The fact of the matter (no pun intended) is that there is a tug of war between processing electronic discovery the proper, defensible way and managing discovery costs. Managing discovery costs does not mean cutting corners and taking on risk—it is about making informed decisions and documenting them in a way that captures the spirit of the choice in context to the event.

Our intent is not to reiterate horror stories of electronic discovery mishaps and sanctions, but rather to provide practical and achievable suggestions and identify key factors that play a role in the outcome of the cost of discovery. After all, the Federal Rules of Civil Procedure begin with Rule 1 stating that the rules shall be “administered to secure the just, speedy and inexpensive determination of every action,” although “inexpensive” is a relative term in the context of electronic discovery.

Formation of the Case Team

As project management is being infused into the law-firm environment, working as a team (or core team) becomes more important, especially since the days of the “free-billing” case are all but gone. Identifying key people is essential to building a case team that covers most aspects of the work to be done. Below are various roles that need to be established and can be divided or combined as necessary depending on competencies and volume.

Team Leader

The team leader does not need to know all the nuances of electronic discovery, but he or she does need to know and be confident that there are others on the team with that knowledge and be able to manage them. The Sedona Conference, Commentary on Achieving Quality in the E-Discovery Process, May 2009, at 6, available at www.thesedonaconference.org/dltForm?did=Achieving_Quality.pdf. The team leader is typically in charge of coordinating the litigation schedule with opposing counsel and the team, assigning the various litigation

tasks, and coordinating with the other team members to meet the litigation schedule.

Discovery Manager

This position is essentially in charge of gathering what is relevant to a document request for review and production. The person that fills this role needs to be competent in all aspects of electronic discovery to ensure a complete and thorough gathering and production of documents. This role works with the team leader or other senior attorney, who will eventually sign the Rule 26(g)(1) certification (or state law equivalent) that requires certification of accuracy and good faith in requesting and responding to discovery. This is often a role that is performed by either an e-discovery attorney, a competent internal consultant, or an outside consultant working closely with the legal team.

Shortly after the December 1, 2006, amendments to the Federal Rules went into effect, some jurisdictions began strongly suggesting or requiring that parties use a form “report to the court” e-discovery plan and that it be filed with the court. Some of these reports to the court require a person from each party to be identified by name and include a phone number. Careful thought should be given in the identification of the person for the report in that it could be a client's IT person, in-house counsel or the discovery manager.

Review/Production Manager

This role can be split, but if so, it is important that there be constant communication, because decisions made during the review process will affect how documents are annotated. These annotations are commonly used for production queries, and if groups of documents are annotated as exceptions to be or not to be produced, they may be omitted from production or, worse, produced to the detriment of the attorney-client privilege. The person(s) filling this role must be detail-oriented and must document decisions.

Planning to Plan

As the old saying goes, “If you fail to plan, you plan to fail!” With team players and roles defined, what is the next logical step? Everyone is ready to begin the task(s) at hand. It is far too easy to fall into the same old “full steam ahead” trap. It seems to make

sense—we have all participated in discovery dozens of times and are familiar with the routine, so taking time to plan is viewed as inefficient. Stay the urge to push forward. The organization of a team is a critical first step towards success; don't miss the mark now by marginalizing devotion to crafting a sound plan.

Complete team participation for initial planning sessions is essential to thoroughly account for the important components of the upcoming discovery project. Many details may be unknown at this point; this realization does not negate the need to meet before any work begins. The amount of unknown details to this exercise can equal the known. The following are some agenda discussion topics for the initial planning meeting.

Define Objectives

It is crucial to discuss not only what should be done, but also what should not be done to meet client satisfaction. Internal investigations seldom require formal document production; therefore, the entire team should be privy to these details. This approach could prevent wasted preparation or even the execution of unnecessary work. Furthermore, do not attempt to disseminate information to team members on a need-to-know basis. It is not effective or conducive to quality team performance. The focused performance of all participants toward universally understood objectives with no one working in a vacuum will prevent errors and duplicated work due to lack of communication or miscommunication.

Discuss Timelines

Present all timelines to the entire group and make them available throughout the duration of the project for everyone to see and understand. Generate a paper timeline calendar displayed in an open area or maintain a synchronized calendar in a computer program such as Microsoft Outlook. No one succeeds if team members are playing by different schedules.

Talk About the Budget

Don't just state that the client does not want to spend any money on the project and believe the discussion is implicitly closed. The result will undoubtedly require uncomfortable client discussions about excessive budgets. Break down the various phases and determine the costs of each segment, but also put together a comprehensive project to conclude the feasibility of meeting the predetermined budget. Are plan changes or discussions with the client necessary? A conversation is easier now than it will be after the fact. Trust your team members. When they provide a budget plan, they are doing so from practical and historical experience. Don't move forward with your own budget based on distrust of what the team is telling you. This could be a critical mistake with severe future consequences.

Develop the Communication Protocols

Most of the problems with electronic discovery cost overruns can be traced to poor communication. Good communication is

a two-way street. Institute communication expectations on day one and enforce them religiously. Accept what may seem to be over-communication, because the opposite is destructive. Furthermore, beware of creating communication "roadblocks." This is the restriction of communications from one person or group on a team toward the senior-level members. This is typically accomplished by placing one team member in the middle of the two groups as a "filter." This is not only a poor communication mechanism that almost always fails, but it instills dissension and infighting. There is nothing more corrosive to successful teamwork.

Once the project has commenced, it is usually not necessary to broadcast every single matter detail to the entire team, but don't leave team members guessing when and who they should inform and when they shouldn't. Be detailed in determining communication protocol. Establish the list of people who need to be "in the loop" for certain events and those who do not.

Continued team meeting expectations should be a part of the communication planning protocols. Depending on the size and complexity of the discovery project, weekly or even daily meetings may be necessary to keep a project on track. Full team meetings are not required with such frequency, but fully attended meetings should be regularly scheduled to assure everyone is on the same page. The meetings do not have to last forever. Even if there is nothing to report, keep the meeting for no other reason than there is a schedule placeholder and all team members understand there is nothing to report. Be effective; use your project detail correspondence to establish an agenda and remain true to it for the meeting proper. Use subsequent meetings for off-agenda topics for only those members required. This will keep everyone engaged in critical team meetings.

Finally, discuss the discovery specifications to be used for the project. How and when will collection be identified and performed? What type of production is mandated? How will review be accomplished? Resolution for every detail is not required at this point; however, task-completion methodologies should be discussed if there is confusion. Perplexity about technique is not helpful and can lead to bad decisions based on misunderstandings. Once you get agreement and comprehension from all team members regarding project viability, sufficient comfort will carry over to the next steps, including dealing with opposing counsel(s).

Negotiate, but Cooperate

If you spend your effort on task completion, you out-manuever by speed and knowledge—not by shenanigans and gamesmanship with opposing counsel.

With great effort, some key factors contributing to project failure have been eliminated by forming a team and developing a plan. Don't go astray now by employing antiquated, unproductive gamesmanship with opposing counsel. Remember, the team has a solid plan. The unknowns are limited, and the selected team is prepared to execute successfully. Understanding one's

position is the first step toward positive negotiation. Because this was accomplished by teamwork and planning, any consequences that arise from agreements made with opposing counsel will be understood.

The next step consists of a shift in stance toward negotiation, upholding cooperative intentions with opposing parties. Team-building and planning appear effortless compared to resisting the routine obstinacy conveyed in pretrial discovery conferences. Fortunately, scrutiny for this obstacle is providing an arena for transformation. According to Sedona Conference writings, “Cooperation does not conflict with the advancement of their clients’ interests—it enhances it.” The Sedona Conference, Cooperation Proclamation 2008, Jul. 2008, at 1, available at www.thosedonaconference.org/content/tsc_cooperation_proclamation/proclamation.pdf.

There are numerous documentation points to consider within a matter, and every one conceivably impacts current or future project costs.

The conference is preparing a road map to collaboration with its 2008 published Cooperation Proclamation. It is constructing a three-part course of action based on “Awareness, Commitment and Tools” where “the legal profession can engage in a comprehensive effort to promote pre-trial discovery cooperation.”

When negotiating, if finer technical points are still vague, invite team experts to attend the conference. Additional assurance that “technically” inaccurate agreements or statements never come to pass save the need for embarrassing renegotiation later.

Stick to your plan. Only a compelling reason should warrant deviation from the plan based on the opposing counsel’s request. Determining the root of the request may reveal misunderstanding as opposed to an inadequate plan. It is often possible to meet requirements without completely altering your own arrangements.

If all else fails and agreement can’t be reached with good-faith attempts to satisfy opposing party requests, it may be time to let the court decide. Remember, conceding to opposing counsels’ potentially unreasonable request will likely cost your client at the end of the day.

Documentation of the Process

This will often be a tough battle, but documentation has too many benefits to weigh against the perceived inconvenience of capturing historical information during the heat of a fast-moving discovery project. Each unique matter requires differing actions to finish tasks during discovery, and all decisions are supported with valid reasoning. If these points are not documented contemporaneously, those reasons may be forgotten. If forgotten, facts needed to prevent a costly redo or a lost motion may be sorely missed. Also, documentation has often been requested in discovery mishaps to show the court that there was at least thought given to a process as part of a “reasonability” test.

There are numerous documentation points to consider within a matter, and every one conceivably impacts current or future project costs. Document procedural data for the tasks performed or to be performed with appropriate specificity. The gain of maintaining consistency across repetitive assignments is a given, but a historical accounting of actions will be preserved should these events be challenged. Future matters or projects will also benefit greatly from this practice, as will be discussed later. This documentation, as well as other forms, can be systematized throughout matter management with templates containing predetermined, common points of data capture. This will provide dependable documentation over the long haul.

Memorialize any project cost and time budgets prepared from planning through completion. Don’t overwrite budgets as they change. Create a new, updated version. This allows the manager to monitor and control expectations by sharing budget progression with all stakeholders, thereby keeping everyone accountable to the goals of the project. How many times have initial project budgets been referenced even though requirements have increased threefold? Good budget records eliminate disconnection between project fantasy and reality. Creating budget templates for utilization on all projects will provide routine reliability and conformity.

Document and centralize correspondence for every project to build a record supporting key strategy adjustments and other decision points during the project. Just finished a phone conversation that altered the review strategy? Provide a follow-up email to relevant team members, outlining the conversation, assuring collective concurrence and perception.

Many short-term rewards are realized through comprehensive documentation practices. Many hours have been saved on an individual matter when details about a communication or completed task are produced without endless hours of searching, or when someone is using a quality-control template to assure a task is complete to expectations instead of missing one final step due to forgetfulness. Documentation can bear extraordinary fruit over the long-term analysis of budget stats and reuse of recorded procedural facts.

Standardization

The logical step of standardization follows practical documentation habits. The result is a foundation for building a uniform records process, repeatable methods for performing tasks, consistent quality-control expectations and effective communication protocols as today's task and project information is gathered.

Standardization of the processes will begin to provide a sustainable method for consistently meeting cost and time budgets, providing a quality work product the first time around and providing more support to a defensible electronic discovery process.

A standardized process for assignment completion permits the accurate measurement of task duration and total cost when a specific job is repeated in subsequent matters. With increasing cost and time estimate precision, a fixed price can be attached to that task if desired.

As the process is defined and the results are documented, measurement is being captured to allow optimization. People and process are requirements for the optimal exploitation of technology. New software and other tools to automate discovery are entering the market at a dizzying pace, all promising to cut costs. However, you can't experience the cost savings, and will actually spend more without first planning, documenting, and establishing standards.

Quality-control standards provide calculated evidence of continued success. Measuring too many errors for a certain task probably means the standards need addressing and optimizing for better performance.

Finally, standardization is designed for repetitive tasks performed on the majority of matters. The requirement that the tactics and expected outcome be consistent renders standards a logical course to maximize performance. Regulating the process frees a case team to concentrate its effort on nonstandard jobs while enabling creativity to rule in those solutions. Many people fear standardization, believing the opposite is true and thwarting movement in this direction.

Cost of Collection

A number of technologies and methodologies exist today to provide a sound and cost-effective document collection. An important step sometimes left out of witness interviews is questioning the witness about potential locations of data of which IT personnel may not be aware. This is a helpful step in that it can identify unknown sources that have been omitted by others. This avoids situations where, upon questioning, a witness might say, "I know everyone else does X but I found that the way I store my documents on an external hard drive is easier." Although this may add additional data to review, it saves time and money from having to go back and re-collect and potentially re-interview everyone.

Evaluate what type of collection needs to be done. For example, rather than sending a collection professional, consider whether you can use a remote collection device instead.

Avoid collecting documents and data by having the client send it through email. This typically increases cost by requiring the manual removal of the header email for review and production. If a custodian or IT person exports the emails as a PST and sends the PST as an attachment, the end user's email system can quarantine the email because of the attachment format—possibly without notice to the receiver. The main reason to avoid this, though, is the lack of trackability.

Cost of Review

Much has been discussed about the cost benefits of outsourcing review to contract reviewers. However, there are a number of offerings in the market to reduce review time and costs even further that use both process and technology or a combination of both. These offerings typically allow potentially responsive documents to bubble to the top in various groupings that can then be reviewed and produced. Originally shied away from as black-box voodoo, these systems are starting to come into the mainstream as both counsel and the judiciary become more comfortable with their use. As with any device or system for reviewing electronic records, while they can be very useful, they can be dangerous when they are not used properly. It is best to take heed from the vendor sponsoring these tools rather than assume omniscience.

As stated above, a plan for review is necessary. This review plan may also contain a workflow diagram that shows the flow of the review as well as what entity is performing what task should a third party shoulder some of the review. A typical review strategy might be that documents are reviewed first for responsiveness. That group of responsive documents are then reviewed for privilege and segregated if necessary. Some additional factors to consider in the review are items like nonviewable files and how to annotate them to segregate them from production while allowing them to be reviewed in their native format for responsiveness. How will redactions be handled? Can documents be redacted to produce if they are partially privileged? Will emails and attachments be reviewed together for responsiveness, or is there a possibility they will be produced separately should either the email or attachment be privileged?

Conclusion

Although there are some who look at the above and see it as just additional work, these ideas most often prevent reinventing the wheel on several levels—from trying to figure out what was gathered all the way to what was actually produced and why. If a routine is followed from case to case, it becomes a matter of habit and can always be tweaked and modified as needed. ■

Thom Wisinski is the chief knowledge officer and Randy Girouard is manager of automated legal services at Haynes and Boone, LLP.

SOCIAL MEDIA WEBSITES

(Continued from page 1)

will have potentially relevant and thus discoverable information located online. To harvest this information, it is now common practice for trial lawyers to conduct online research on their own clients, opposing parties, witnesses, experts, and even jurors.

Social Media Data Can Make or Break Your Case

The average online social networking profile contains a wealth of potentially discoverable knowledge. Profiles can include a person's hometown, date of birth, address, occupation, ethnicity, height, relationship status, income, education, and a limitless array of comments, messages, photographs, and videos. While all of this information may be helpful, it is usually the messages and photographs that are the focus of a litigation search. Although not scientifically verifiable, anecdotal evidence suggests that a user's social filter—the buffer that tells us what not to say and do at a dinner party—stops working the moment a person sits down in front of a computer screen. During recent political races, Facebook photographs emerged of candidates or their influential staff performing sexually suggestive acts while dressed up like Santa Claus (Kashmir Hill, *Krystal Ball Offers Glimpse into the Future of Politicking for the Facebook Generation*, The Not-So Private Parts, Oct. 10, 2010, <http://blogs.forbes.com/kashmirhill/2010/10/13/krystal-ball-offers-glimpse-into-the-future-of-politicking-for-the-facebook-generation>), groping cardboard cutouts of their candidate's opponent (*Facebook: Obama Speechwriter Parties with Clinton Cut-Out*, The Huffington Post, Dec. 5, 2008, www.huffingtonpost.com/2008/12/05/facebook-obama-speechwrit_n_148774.html), and violently vomiting after over-indulging on adult beverages (Eli Sanders, *GOP Party-Boy Scandal!*, The Stranger, Oct. 10, 2006, www.thestranger.com/seattle/Content?oid=87882).

With increasing frequency, courts are holding that what you do and say on Facebook can and will be held against you in a court of law. Information exchanged via social networks has assumed prominent roles in a variety of litigation contexts and has taken on particular importance in family law, personal injury, criminal law, business torts, and employment matters. Recently, a local matrimonial lawyer commented to this author that the first step in any divorce proceeding was to try and seize the other party's computer hard drive and the incriminating treasure trove it may contain.

The importance of social media has been evidenced in several recent decisions. In an Ohio family law case, a divorcing husband and wife were contesting custody of their five-year-old daughter. The trial court found that its primary concern was a determination of what would be in the “best interests of the

child.” *Dexter v. Dexter*, No. 2006-P-0051, 2007 WL 1532084, at *1–2 (Ohio Ct. App. May 25, 2007). During the proceedings, the husband's counsel located the wife's online blogs, where she admitted that she practices sadomasochism, that she was on a hiatus from using illicit drugs during the pendency of the proceedings, and that she planned to use drugs in the future. The wife further admitted in her online blogs that she would use drugs in her home while the child was sleeping. Unsurprisingly, the court found that the wife's lifestyle choices would have a detrimental effect on the child and awarded full custody to the husband. *Id.*

In another family law case, a husband was recently charged with criminal contempt for violating a domestic relations order of protection by sending multiple communications to his wife's MySpace account. *Dockery v. Dockery*, No. E2009-01059-COA-R3-CV, 2009 WL 3486662 (Tenn. Ct. App., Oct. 29, 2009). Elsewhere, a Texas court declined to award custody of a couple's two children to the father after he posted on his MySpace account “I don't want kids” two weeks before trial. *In re T.T.*, 228 S.W.3d 312, 322 (Tex. App. 2007). In the U.S. District Court for the Northern District of Ohio, a judge overseeing multi-district litigation related to welding injuries recently dismissed a plaintiff's claims of permanent and severe disability after defense lawyers uncovered photographs of the plaintiff on Facebook, racing motor boats. *In re Welding Fume Products Liability Litigation*, MDL 1535, No. 03-17000, N.D. Ohio.

Social Media Information Used as Evidence

Courts are increasingly willing to allow your opposing counsel access to your client's Facebook and MySpace accounts, regardless of privacy settings. In the recent case of *Romano v. Steelcase Inc.*, 907 N.Y.S.2d 650 (N.Y.Sup. Ct. 2010), the New York Supreme Court ordered the plaintiff to grant the defendants access to current and historical Facebook and MySpace pages and accounts on the basis that information on the social networking sites was inconsistent with the plaintiff's claims in that action concerning the extent and nature of her injuries, especially her claims for loss of enjoyment of life. To convince the court to grant its motion, the defendants produced public portions of the plaintiff's MySpace and Facebook pages that revealed an active lifestyle that included travel to Florida and Pennsylvania during the time period in which she claimed her injuries precluded such activity. The court was particularly intrigued by the plaintiff's public profile page on Facebook, showing her smiling happily in a photograph outside the confines of her home in a case in which the plaintiff had claimed significant permanent injuries that had kept her bedridden. The court found that the information sought by the defendants was

“material and necessary to the defense of this action and/or could lead to admissible evidence.” *Id.* at 654.

In *Ledbetter v. WalMart Stores, Inc.*, No. 06-cv-01958-WYD-MJW, 2009 WL 1067018, *1 (D.Colo. Apr. 21, 2009), the U.S. District Court for Colorado ordered the defendants in a personal injury suit to produce Facebook, MySpace, and Meetup .com account information. The court found that because the plaintiffs had called into question their physical condition as well as their relationships with their spouses, they had waived any privileges related to that type of information and that the subpoenas to Facebook and MySpace were reasonably calculated to lead to the discovery of admissible evidence. *Id.*

Similarly, the Superior Court of Justice for Ontario in a recent decision in *Murphy v. Perger*, [2007] 67 C.P.C. (6th) 245 (Can.), held that a defendant was entitled to the production of the plaintiff’s Facebook page. The plaintiff had claimed damages for pain and suffering and loss of enjoyment of life arising out of a motor vehicle accident. The defendant had successfully accessed another website that contained a photograph of the plaintiff engaging in various social activities and suspected additional photographs were contained on her Facebook site. The court, in finding that the plaintiff did not have a right to privacy that extended to protecting Facebook photographs, held that “a party who maintains a private, or limited access, Facebook profile stands in no different position than one who sets up a publicly available profile” and that “any invasion of privacy is minimal and is outweighed by the defendant’s need to have the photographs in order to assess the case.” The judge further found that the plaintiff could not have a “serious expectation of privacy,” as her “private” profile still granted access to 366 people. *Id.*

Gaining Access to Social Media Information

As it appears courts are becoming more apt to allow social media data into a case, the next question is how to go about accessing the information. However you decide to go about it, I would advise against setting up a fake user name to “friend” the opposing party or asking your paralegal to do so. Such actions are frowned upon. See www.philadelphiabar.org/WebObjects/PBAREadOnly.woa/Contents/WebServerResources/CMSResources/Opinion_2009-2.pdf.

In the world of electronic discovery and electronically stored information, when a case first lands on your desk, it is common practice to prepare and submit a spoliation letter to the opposing counsel. In preparing such a letter, be sure to specifically mention social networking sites, online blogs, and any other accounts that the opposing party may have. Individuals who have potentially damaging information stored on their social media website may be quick to alter or destroy that information after becoming party to a lawsuit, and Facebook has asserted that once that information is deleted, they have no way of recovering it. Facebook Frequently Asked Questions, www.facebook.com/help/?faq=17158 (last visited Jan. 6, 2011).

If you are able catch someone in the act of spoliation, it may be enough to win your case. In *Torres v. Lexington Ins. Co.*, 237 F.R.D. 533 (D.P.R. 2006), a plaintiff sued a hotel chain, alleging that sexual assault at the hotel caused her to become socially isolated and that she suffered intense humiliation and mental anguish. The defense counsel located the plaintiff’s online account, which contained photographs “depicting an active social life, and an aspiring singing and modeling career.” *Id.* at 533–534. The defense counsel was able to download and print much of the information and subsequently sent the plaintiff’s counsel a spoliation notice and requested that the remaining data be produced. Two days later, the plaintiff had deleted the account in its entirety. The court sanctioned the plaintiff’s spoliation by dismissing her claims for mental anguish. *Id.*

As it appears courts are becoming more apt to allow social media data into a case, the next question is how to go about accessing the information.

After sending a spoliation letter, you can pursue social media information through traditional discovery. Interrogatories should ask the respondent to identify all the websites that he or she uses to communicate with other individuals, the name, account, or username information associated with that website, the names of all individuals who have access to that account, the last time the account was accessed, and the individual’s email addresses, phone number, address and other normal biographical information. The requests for production can seek printouts evidencing each account and copies or screenshots of all photographs and messages included within the account.

Finally, you should submit an authorization to be signed by the respondent that specifically includes the above account information. Information contained on Facebook, MySpace, and any other social media website is protected from subpoena under the Stored Communications Act, 18 U.S.C. § 2701 *et. seq.* As a result, the most that Facebook or MySpace can produce absent an authorization from the user is basic subscriber information from a particular account. Facebook Frequently Asked Questions, www.facebook.com/help/?faq=17158 (last visited Jan. 6, 2011). To access photographs, messages, and other account content stored on Facebook or Myspace, you

will need an authorization from the user to the social media website, authorizing it to release the specified account information. The authorization should include the user's account and pertinent biographical information. Undoubtedly, as with most avenues of discovery, the opposing party may refuse to sign the authorization based on privacy or relevancy grounds. With the liberal discovery breadth afforded by the Federal Rules of Civil Procedure and the recent trends toward disclosure discussed above, you should be in a strong position to convince the court to order access to the information.

Counsel is required under Rule 901 to make a prima facie showing of authenticity. However, Rule 901 does not address how to authenticate electronically stored evidence.

Once you have the signed authorization and pertinent account information, you can prepare a subpoena to the social media entity. Any Facebook request should be sent to Facebook, 1601 S. California Ave., Palo Alto, CA 94304, Attention: Security Department, or fax 650-644-3229. While Facebook will accept service by fax or mail, MySpace requires personal service on its registered agent at 2121 Avenue of the Stars, Suite 700, Los Angeles, CA 90067. All subpoenas should be addressed to the custodian of records for MySpace.com. The subpoena should include the user's full name, the full URL to the Facebook or Myspace profile, the school or network in which the person is included, the person's birth date, known email addresses, the account ID number, phone numbers, the address, and the expected period of activity. Both MySpace and Facebook will accept subpoenas from out-of-state civil litigants only if they have been properly domesticated through a California court. While Facebook and MySpace cannot provide content that has been previously deleted, if a Facebook or MySpace user has terminated his or her account, the entities can restore access to allow the user to collect and produce information to the extent possible. *Id.*

Admitting Social Media Information into Evidence

Now that you have the information, the next step is to get it admitted into evidence in court. Information gathered from the Internet is usually opposed on authenticity grounds. Federal Rule of Evidence 901(a) requires a party attempting to admit

evidence to be able to authenticate it by showing that the evidence is what it is purported to be. Federal Rule 901(b) provides a non-exhaustive list of 10 methods available to the party to make this authenticity showing. While the opposing party can always raise preliminary questions about the evidence under Rule 104, as well as relevancy questions under Rule 401, the most likely hurdle for a party attempting to introduce social networking information is under Rule 901.

Counsel is required under Rule 901 to make a prima facie showing of authenticity. However, Rule 901 does not address how to authenticate electronically stored evidence. Using a conglomerate of the 10 methods under 901(b)(1), however, counsel can piece together a method of authenticating social media data. First, under 901(b)(1), counsel can provide an authenticating witness who can provide factual specificity about the process by which the electronically stored information was created, acquired, maintained, and preserved without alteration or change or the process by which it is produced as a result of the system or process that does so. If you have used a legal assistant or paralegal to print screenshots from someone's Facebook account, then that person can submit an affidavit or otherwise testify about the method in which he or she produced the information. The affidavit or testimony of the person who made the copy of the website should include the Internet address of the website, the date the content was printed, the method of printing, and the method in which the printing has since been stored.

Second, as set forth in *United States v. Siddiqui*, 235 F.3d 1318, 1322-23 (11th Cir. 2000), courts will often allow electronic information to be authenticated by the content itself under Rule 901(b)(4). If a Facebook account contains the contact information, name, date of birth, and other personal information about a particular witness, that information itself may be used to authenticate the ownership of the account, as well as the individual using it. Often, the documents can be self-authenticating by providing distinctive characteristics of the website that address that a particular party authored it if you can prove the person was one of few or the only individual who knew the information at the time that it was submitted to the Internet or the only individual who had access to the account on which the content was published.

Next, a party can take advantage of Rule 902(11), which allows electronic information to be self-authenticated when it complies with the business record exception. If you have successfully subpoenaed information from Facebook, it will be accompanied by an affidavit of the custodian of records. Facebook Frequently Asked Questions, www.facebook.com/help/?faq=17161 (last visited Jan. 6, 2011). Facebook will refuse to appear in person as a witness. However, use of the affidavit should be enough to overcome any objections to the business record exception.

Concerns with authenticity become even more nuanced when dealing with jurors who may not be technologically savvy enough

to understand the intricacies of social media websites. Jurors will undoubtedly have heard of hacking, and opposing counsel may pray on these fears by suggesting that someone other than the alleged author may have accessed the social media account and posted a particular message or status update. In the case of *In re K. W.*, 666 S.E.2d 490, 494 (N.C. Ct. App. 2008), a plaintiff admitted that the proffered MySpace page was hers but claimed that her friend posted the answers to the survey questions that the defendant sought to introduce as impeachment evidence with respect to her claims of rape. Accordingly, when evaluating what method to use in introducing and authenticating social media evidence, you should be cognizant of additional potential hurdles in gaining acceptance with the jury. Questioning the opposing witness and forcing him or her to authenticate a pseudonymous social networking profile, based on admission, may be the most convincing method.

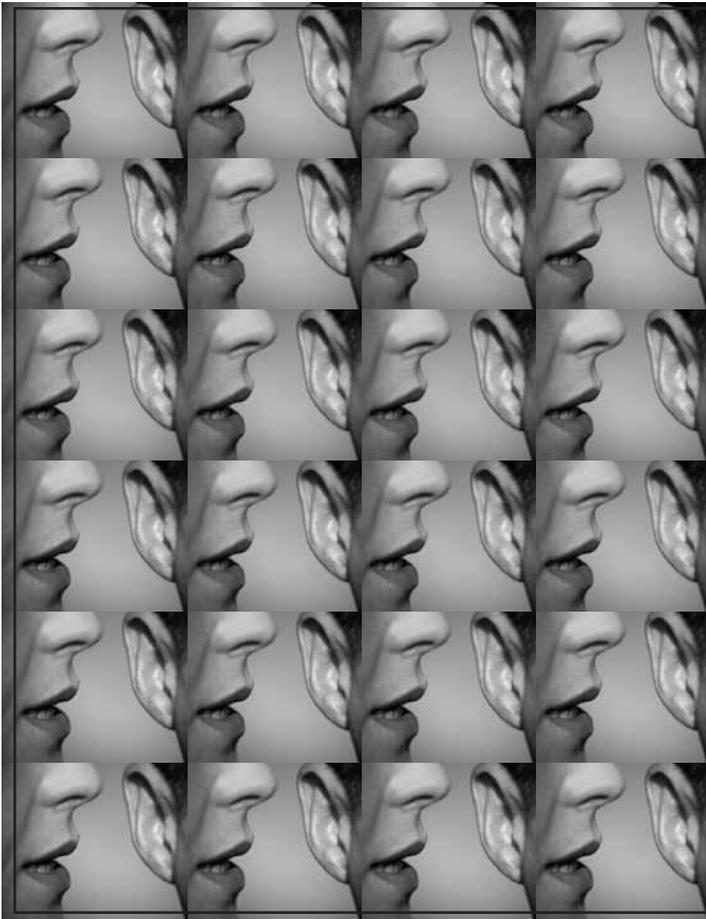
Finally, once the information has been found to be relevant and authentic, the electronic social media information must overcome any potential hearsay objections. In particular, any messages that have been sent between users of Facebook or MySpace, postings on a blog, or other postings on a website will have to overcome typical hearsay objections. This article

will not delve into the various facets of the hearsay rule and its application to these statements except to note that under Rule 801(d)(2), most often, the messages that are being made by opposing parties on their Facebook, MySpace, Twitter, or blog pages can be considered admissions by a party opponent.

Conclusion

As soon as a new file hits your desk, you should be researching your own client, opposing parties, witnesses, experts, and even jurors to find all leads and information that they have deposited on the Internet. With the high number of individuals routinely posting information to these social media websites, it is inevitable that someone in your case is going to be directly or indirectly involved. The question is: How do you go about getting that information, and how do you use it to your best advantage? Rest assured, the opposing counsel is going to be taking these same steps to investigate all of the players on your side of the table. You do not want to be caught one step behind. ■

Travis B. Swearingen is an associate in the General Litigation and Commercial Department of Miller & Martin, PLLC, in Nashville, Tennessee.



THE BENEFITS OF MEMBERSHIP

Spread the Word

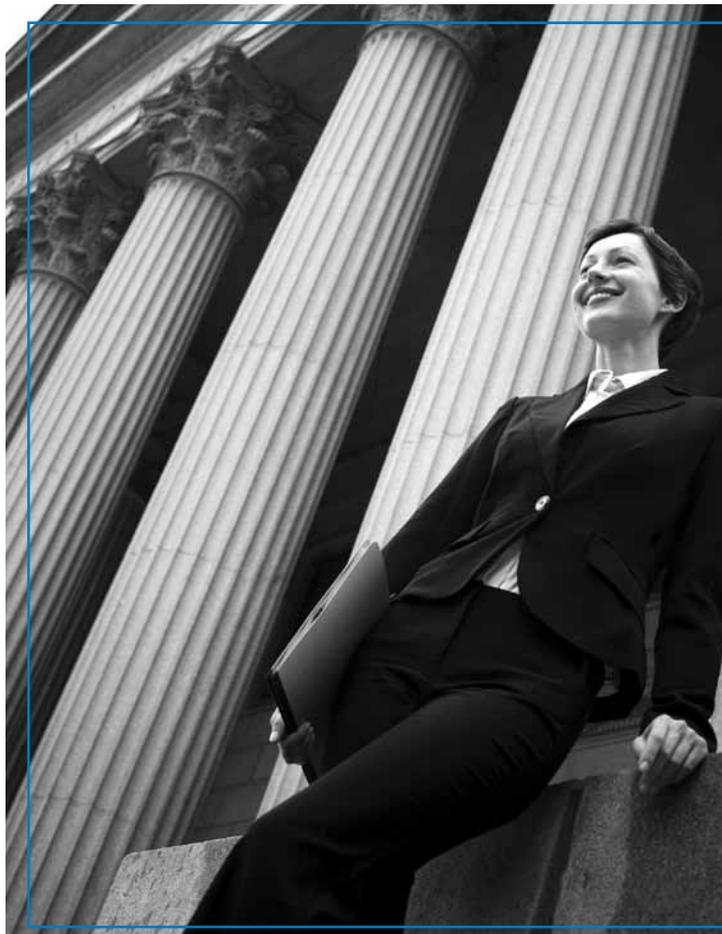
Have you told your friends and colleagues about the benefits of Section membership?

Fill them in. Don't keep this secret all to yourself.

To join go to:

www.americanbar.org/groups/litigation/membership

ABA Section of Litigation
AMERICAN BAR ASSOCIATION



THE BENEFITS OF MEMBERSHIP

Reach Your Potential

- *Litigation News* Website and Monthly Emails
- *Litigation Magazine*
- Litigation Podcast
- Meetings & CLE Calendar
- Cutting-Edge News and Analysis
- Newsletter Archive back to 2002

Go to www.americanbar.org/groups/litigation