Social Media, The Internet and Electronically Stored Information Challenges

Submitted by Prof. Sara Anne Hook
Advanced Issues in Personal Injury Litigation

Authors

Bobby J. Avery-Kimball
Zeigler Cohen & Koch
9465 Counselors Row, Suite 104
Indianapolis, IN

Scott A. Benkie
Benkie & Crawford Attorneys of the Law
156 E Market Street 2 Fl
Indianapolis, IN

Matthew C. Boulton
Boulton Law Group, LLC
405 East Main Street
Brownsburg, IN

David G. Curry
ITC Experts
1020 Airpark Drive
Sugar Grove, IL

Ryan J. Guillory
Hunt Suedhoff Kalamaros LLP
6323 South East Street
Indianapolis, IN

Sara Anne Hook
Indiana University School of Informatics and Computing, IUPUI
535 W. Michigan Street, IT 589
Indianapolis, IN

Willis E. Huiras
Huiras Law
8250 Haverstick Road, Suite 150
Indianapolis, IN

Timothy F. Kelly
Kelly Law Office
5521 W. Lincoln Highway, Suite 101
Crown Point, IN
Scott M. Kyrouac
Wilkinson, Goeller, Modesitt, Wilkinson & Drummy LLP
333 Ohio Street
Terre Haute, IN

John E. Meyer
ITC Experts
1020 Airpark Drive
Sugar Grove, IL

Thomas F. O'Gara
Taft Stettinius & Hollister LLP
One Indiana Square, Suite 3500
Indianapolis, IN

Cari L. Sheehan
Reminger Co., L.P.A.
3925 River Crossing Parkway, Suite 280
Indianapolis, IN

David B. Wilson
David B. Wilson Attorney at Law
4040 South Meridian Street
Indianapolis, IN
applied human performance; and has been awarded four U.S. patents. Dr. Curry is a certified human factors professional, a certified safety professional and a professional member of the American Society of Safety Engineers; with more than 25 years of experience in the design, development and evaluation of user interaction with products and machinery. He is a member of the Society of Automotive Engineers' Safety and Human Factors Committee, the Human Factors and Ergonomics Society and the Association for Psychological Science; and sits on numerous SAE, ANSI and ASTM standards-making committees.

RYAN J. GUILLORY is an attorney in the Indianapolis office of Hunt Suedhoff Kalamaros LLP. His practice is focused primarily in the areas of insurance defense and coverage, and workers' compensation defense. He received his B.S.B.A. and M.A. degrees from Tulane University and his J.D. degree from the Indiana University School of Law - Bloomington. Mr. Guillory is a member of the Indiana State Bar Association, the Indianapolis Bar Association, and the Defense Research Institute; and he is vice chair of the Insurance Section of the Defense Trial Counsel of Indiana.

PROF. SARA ANNE HOOK is professor of Informatics at Indiana University School of Informatics and Computing, IUPUI, where she has developed a suite of courses in the emerging field of legal informatics. She also has served as adjunct professor of law at the Robert H. McKinney School of Law, Indiana University, Indianapolis, where she has taught courses in intellectual property law and professional responsibility. Formerly, Professor Hook was Associate Dean of the Faculties for IUPUI and head librarian at the IU School of Dentistry. She is admitted to practice in Indiana and before the Supreme Court of the United States. During law school, Professor Hook was executive notes editor of the Indiana International & Comparative Law Review, co-chair of the Dean's Tutorial Society, and finished second in the Client Counseling Competition. Her research interests include intellectual property law, the emerging field of legal informatics, and ways to enhance creativity in teaching and learning. Professor Hook is a member of the American Intellectual Property Law Association (AIPLA), the Indiana State Bar Association, the International Legal Technology Association (ILTA) and of the Board of Governors of the Organization for Legal Professionals (OLP). She regularly publishes and gives presentations on intellectual property law, electronic discovery, legal technology, legal research techniques, and issues related to privacy and security. Professor Hook earned her B.A. and M.L.S. degrees from the University of Michigan; her M.B.A. degree from the Kelley School of Business, Indiana University; and her J.D. degree from the Robert H. McKinney School of Law, Indiana University, Indianapolis.

WILLIS E. HUIRAS is the founder of Huiras Law. He has litigated cases in nearly every county in Indiana. Mr. Huiras also regularly appears in federal district and bankruptcy courts, including the Seventh Circuit Court of Appeals. He earned his B.S. degree from Ball State University and his J.D. degree from Indiana University Robert H. McKinney School of Law. While at Ball State University, Mr. Huiras earned the distinction of Dean's List every semester, culminating in the Outstanding Graduate, Department of Economics honor. During law school, he was a Dean's Tutorial Fellow and served on the International and Comparative Law Review. Mr. Huiras had the opportunity to clerk for the Honorable Jerry Barr during law school.
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced Issues in Personal Injury Litigation</td>
<td>1</td>
</tr>
<tr>
<td>Advanced Accident Investigation Strategies</td>
<td>27</td>
</tr>
<tr>
<td>Using Medical Records to Win Your Case</td>
<td>55</td>
</tr>
<tr>
<td>Getting the Most Out of Expert Witnesses</td>
<td>81</td>
</tr>
<tr>
<td>Social Media, The Internet and Electronically Stored Information Challenges</td>
<td>93</td>
</tr>
<tr>
<td>Negotiating Claims With Insurance Companies</td>
<td>119</td>
</tr>
<tr>
<td>Voir Dire And Advanced Jury Selection Strategies</td>
<td>139</td>
</tr>
<tr>
<td>The Art &amp; Science of Modern Jury Selection</td>
<td>151</td>
</tr>
<tr>
<td>Handling Complex Subrogation And Lien Issues</td>
<td>161</td>
</tr>
<tr>
<td>The Affordable Care Act’s Impact on Personal Injury Settlements</td>
<td>185</td>
</tr>
<tr>
<td>Advanced Trial Strategies</td>
<td>203</td>
</tr>
<tr>
<td>Ethical Considerations in Personal Injury Cases</td>
<td>221</td>
</tr>
</tbody>
</table>
V: Social Media, The Internet and Electronically Stored Information Challenges

Introduction

Whenever I have a question regarding electronic discovery, the first place I start is a review of the Electronic Discovery Reference Model (EDRM). By visualizing the steps in handling a piece of electronically-stored information (ESI) from the left-hand side of the model (which starts with proper information governance) to the presentation of the ESI in court, the EDRM also reminds me of the potential for ethical breaches at each step.

Electronic Discovery Reference Model


Another excellent resource for cases, statutes, guidelines and other materials for electronic discovery is the K&L Gates Electronic Discovery Law website (http://www.ediscoverylaw.com/, accessed 10/21/14). The website contains a very helpful database of over 2000 cases that is searchable by keyword as well as having a number of pre-
determined case attributes (http://www.ediscoverylaw.com/e-discovery-case-database/, accessed 10/21/14). Many of the cases have very short summaries that include the case citation, the nature of the case, the electronic data involved, the electronic discovery issue and searchable attributes. A number of the cases have more robust summaries that also may have links to additional materials.

A quick search of the K&L Gates database for cases involving social media in personal injury yields several interesting and helpful cases, including two cases that have become major cases in the world of electronic discovery, McMillen v. Hummingbird Speedway, Inc. and Romano v. Steelcase, Inc. The following summaries were taken from the K&L Gates database, starting with the McMillen and Romano cases:

- **McMillen v. Hummingbird Speedway, Inc., No. 113-2010 CD (C.P. Jefferson, Sept. 9, 2010).** Court granted defendants' motion to compel production of plaintiff’s user names, log-in names, and passwords to relevant social networking sites, where defendant asserted the likelihood that relevant information would be found based on information available in the public portion of plaintiff’s Facebook account and where the court found the information requested was not confidential or subject to any other evidentiary privilege. [a longer summary, along with copies of the full opinion and order, is available from the K&L Gates website]

- **Romano v. Steelcase, Inc., 907 N.Y.S.2d 650 (N.Y. Sup. Ct. Sept. 2010).** Where defendant sought to discover plaintiff’s “current and historical Facebook and MySpace pages and accounts”, including deleted information, on the belief that information posted there was inconsistent with her injury claims, the court granted the motion, despite plaintiff’s privacy concerns, upon finding the information was material and relevant and that plaintiff had no reasonable expectation of privacy, and because the defendant’s need for access outweighed plaintiff’s privacy concerns. [a longer summary is available from K&L Gates website]

- **Patterson v. Turner Constr. Co., 931 N.Y.S.2d 311 (N.Y. App. Div. Oct. 27, 2011).** Where lower court granted motion to compel authorization for all of plaintiff’s records on an online social networking service, appellate court reversed and remanded “for more specific identification of plaintiff’s Facebook information that is relevant” and noted that if relevant, the content of plaintiff’s account were “not shielded from discovery merely because plaintiff used the service’s privacy settings to restrict access”.

96
• **Richards v. Hertz Corp., ---N.Y.S.2d---, 2012 WL 5503841 (N.Y. App. Div. Nov. 14, 2012).** Where the public contents of one plaintiff's Facebook account established that it was "reasonable to believe" that other relevant information may also be present but where lower court only directed plaintiff to produce certain relevant photographs, appellate court remanded with instruction that the court conduct in camera review of "all status reports, emails, photographs, and videos" to determine which of those materials, if any, were relevant; as to a separate plaintiff where no showing of potential relevance was made, appellate court found lower court properly granted her motion for a protective order.

• **Thompson v. Autoliv ASP, Inc., No. 2:09-cv-01375-PMP-VCF, 2012 WL 2342928 (D. Nev. June 20, 2012).** The court granted (in part) Defendant's motion to compel production of the contents of Plaintiff's Facebook and MySpace accounts from April 2007 through the present and ordered that the contents be uploaded to an external storage device and produced to defense counsel for review and identification of "discoverable" materials; court's analysis included consideration of defendant's assertions that the information was relevant to post-accident social activities, mental state etc. where defendant had previously accessed plaintiff's public Facebook profile before account settings were altered and plaintiff's limited production of information prior to defendant's motion to compel.

• **Pereira v. City of New York, No. 26927/11, 2013 WL 3497615 (N.Y. Sup. Ct. June 19, 2013).** Where Defendant demonstrated that there were probative photos on Plaintiff's Facebook and elsewhere (i.e. "a hockey blog"), the court reasoned that it was "therefore reasonable to believe that other portions of his Facebook account may contain further evidence relevant to the issue of plaintiff’s injuries," and ordered Plaintiff to provide for in camera inspection "all photographs depicting sporting activities posted on the demanded media sites" and "copies of all status reports, emails, photographs, and videos posted on plaintiff's media sites since the date of the subject accident".

• **Fawcett v. Altieri, ---N.Y.S.2d---, 2013 WL 150247 (N.Y. Sup. Ct. Jan. 11, 2013).** Court acknowledged the discoverability of social media content but reasoned that "[i]n order to obtain a closed or private social media account by a court order for the subscriber to execute an authorization for their release, the adversary must show with some credible facts that the adversary subscriber has posted information or photographs that are relevant to the facts of the case at hand," and thus denied defendants motion to compel.

A second excellent resource for materials on electronic discovery is the Kroll Ontrack ([http://www.krollontrack.com/](http://www.krollontrack.com/), accessed 10/21/14) This website includes blogs on electronic discovery and data recovery, white papers, case studies and industry news. It also offers a searchable database of electronic discovery cases that complements what is provided by K&L.
Gates and is searchable by keyword as well as by e-discovery-related topics and jurisdiction (http://www.ediscovery.com/pulse/case-law/, accessed 10/21/14). I find it comforting when both of these databases provide summaries of the same case, but also they may cover different cases, which broadens my collection of cases. A quick search of the Kroll Ontrack database reveals three more recent cases on social media and personal injury with helpful summaries provided.

- **Zimmerman v. Weis Markets, Inc.**, No. CV-09-1535 (C.P. Northumberland May 19, 2011). In this personal injury litigation, the defendant requested preservation and disclosure of the non-public portions of the plaintiff's Facebook and MySpace pages. Noting that recent photographs and comments on the public portions of the plaintiff's pages appeared to contradict claims of physical and emotional distress, the defendant argued it should have access to relevant information in areas designated as private. The plaintiff countered that allowing access to shielded information would violate his reasonable expectation of privacy. Rejecting the plaintiff's argument, the court noted that no privilege exists in Pennsylvania for non-public social website information and the "paramount ideal" of pursuing truth favors liberal discovery. Further, the court agreed with the rationale in *McMillen v. Hummingbird Speedway Inc.* and cited *Romano v. Steelcase, Inc.*, which held that an individual who voluntarily posts pictures and information on social websites does so with the intention of sharing, and thus cannot later claim any expectation of privacy, especially because the privacy policies of Facebook and MySpace disclose that any information posted may become publicly available at the user's own risk. Finding a reasonable likelihood that additional relevant information existed on the non-public portions, the court ordered the plaintiff to provide all passwords and user names to the defendant, and preserve all existing information.

- **Offenback v. L.M Bowman, Inc.**, 2011 WL 2491371 (M.D. Pa. June 22, 2011). In this personal injury case, the defendants requested an in camera review of the plaintiff's Facebook and MySpace accounts, arguing the plaintiff's claims of physical and psychological impairment made relevant any evidence that documented the plaintiff's social life, physical capabilities and emotional state of mind. To the extent that such information was relevant under Fed.R.Civ.P. 26, the plaintiff agreed that limited public information on his Facebook account was discoverable and provided the password to the court (the plaintiff claimed he could no longer access his MySpace account). Upon review, the court agreed to the relevance of a limited amount of photographs and postings that reflected the plaintiff continued to ride motorcycles, went hunting and rode a mule, and ordered production of this information. In a closing footnote, the court stated it was confused as to why intervention was necessary since the parties agreed that at least some of the information was relevant. The court further noted the plaintiff should have reviewed his own Facebook account for potentially responsive information, only soliciting the court's assistance if a dispute remained.
• **Gatto v. United Air Lines, Inc.,** 2013 WL 1285285 (D.N.J. Mar. 25, 2013). In this personal injury dispute, the defendants sought spoliation sanctions arising out of the plaintiff's destruction of relevant social media evidence. Despite complying with a court order mandating the plaintiff to change his Facebook password to allow the defendants counsel to access the plaintiff's social media account, the plaintiff deactivated his Facebook account after receiving an alert from Facebook that his account was being accessed by an unfamiliar IP address in New Jersey. The parties disputed over exactly how the information on the account was permanently deleted ("as noted by the defendants, the procedures for deactivating versus permanently deleting a Facebook account are not identical"), however, the court found it sufficient that any "scenario involves the withholding or destruction of evidence." The court stated that spoliation occurs wherever a party fails to "preserve property for another's use in pending or reasonably foreseeable litigation." Assessing whether an adverse inference instruction was appropriate, the court found three of the four factors clearly favored the defendants: the plaintiff was in control of the social media account, the evidence was potentially relevant to damages and it was reasonably foreseeable that the evidence would be discoverable. Regarding the second factor, which requires "actual suppression or withholding of evidence," the court found that plaintiff's deactivation of the account was sufficient. The court granted the defendants' request for an adverse inference instruction.

An additional search of both databases for social media cases in 2014 resulted in several other interesting cases. These cases further illuminate a wide spectrum of issues with collecting, preserving and presenting this type of ESI as part of litigation.


• **Stallings v. City of Johnston City,** 2014 WL 2061669 (S.D. Ill. May 19, 2014).

It is interesting to review the nature of these cases, which illustrate how social media has permeated every facet of our work and daily lives. For example, these cases include breach of
settlement, trademark infringement and unfair competition, sexual harassment, violations of Title VII and the Family Medical Leave Act, bullying and harassment and wrongful termination.

Among the disputes and mistakes outlined in these cases are data preservation, lack of cooperation in the discovery process, inadequacy of search, identification or collection processes, motions to compel, motions for sanctions, adverse inference instructions and undue burden.

Also of note is that many of the cases from 2014 concern text messages, indicating the continued evolution of the technology that people use to communicate with each other.

Other resources are available to advise lawyers on the proper handling of social media as ESI throughout the electronic discovery process. For example, the American Bar Association has published Social Media as Evidence: Cases, Practice Pointers and Techniques (Anahit Tagvoryan and Joshua M. Briones. Social Media as Evidence: Cases, Practice Pointers and Techniques. Chicago: American Bar Association, 2013, ISBN: 978-1-61438-629-2). Another helpful resource is Social Media Evidence – How to Find It and How to Use It, which was presented by the ABA Section of Litigation at the 2013 ABA Annual Meeting (http://www.americanbar.org/content/dam/aba/administrative/litigation/materials/aba-annual-2013/written_materials/15_1_social_media_evidence.authcheckdam.pdf, accessed 10/21/14).

This free resource includes sample interrogatories and document requests, advice for jury instructions (because the temptation for jury members to conduct their own investigations via Google and social media is an increasing problem in litigation), complaints, requests for discovery and other documents.


**Jurisdiction Over Websites**

As stated on page 8 of *Social Media Evidence – How to Find It and How to Use It*, “[a]lways check the Terms of Service for the social media website as they may have an impact on your approach to obtaining the information or even the target of your discovery demands. For example, Twitter’s Terms of Service clearly state that a Twitter user provides Twitter a license to distribute to anyone at any time whatever the user tweets.”


This advice continues with a discussion of *People v. Harris*, a summary of which is provided by the K&L Gates database:

- **People v. Harris**, ---N.Y.S.2d---, 2012 WL 1381238 (N.Y. Crim. Ct. Apr. 20, 2012). In this case, the court held that the criminal defendant did not have standing to move to quash a subpoena (issued pursuant to the Stored Communications Act) seeking production of his Tweets and the user information associated with his Twitter account because the defendant “had no proprietary interests” in the information sought and because his claimed privacy interest was “understandable” but “without merit”; court's analysis turned largely on Twitter's terms of service. [a longer summary is also available through the K&L Gates website]

In Socializing Over State Lines, Wasson reviews the “minimum contacts” standard for personal jurisdiction, which he notes the Internet has made the test more difficult to apply (Brian Wasson. *Socializing Over State Lines: Social Media as a Basis for Personal Jurisdiction.* Wassom.com: Discussion of Law of Social & Emerging Media, April 25, 2012, http://www.wassom.com/socializing-over-state-lines-social-media-as-a-basis-for-personal-jurisdiction.html, accessed 10/21/14). He then describes three cases to illustrate that even relatively minor faculty details can make a significant difference in whether a person will be subject to jurisdiction in a foreign state. He notes that social media cases do not always fit the
mold of “old” Internet case law (Id. at 2) and risks when using Twitter to solicit business (Id. at 2-3).

Social Media – Complying with the Stored Communications Act

One of the earliest cases to address the application of the Stored Communications Act to requests for ESI from social media was Crispin v. Christian Audigier, Inc. A summary of this case is provided by the K&L Gates database.

- **Crispin v. Christian Audigier, Inc., 717 F.Supp.2d 965 (C.D. Cal. 2010).** Upon holding that the social networking sites at issue (Facebook, MySpace, Media Temple) were subject to the Stored Communications Act, court quashed subpoenas seeking private messages but, as to subpoenas seeking messages posted to plaintiff’s Facebook wall and MySpace comments, remanded for further investigation of plaintiff’s privacy settings as to those messages because the Stored Communications Act is not applicable to information readily available to the general public. [a longer summary is available from the K&L Gates website]

More recent cases have been decided, including:

- **Optiver Australia Pty, Ltd. & Anor v. Tibra Trading Pty. Ltd. & Ors, No. C 12-80242 EJD (PSG), 2013 WL 256771 (N.D. Cal. Jan. 23, 2013).** Court quashed portion of subpoena seeking identification of documents containing certain search terms upon concluding that such terms “constitute content, or information concerning the ‘substance purport, or meaning’ of the communication” and was the sort of information protected by the Stored Communications Act (“SCA”); court quashed portion of subpoena seeking the subject lines of email communications and Google talk messages upon finding that such information was “content” and thus protected by the SCA; court declined to quash portion of subpoena seeking non-content metadata. (K&L Gates database) [a longer summary is also available through the K&L Gates website – see also Does the Stored Communications Act Protect an Email’s Subject Line From Disclosure? Information Law Group, January 31, 2-13, http://www.infolawgroup.com/2013/01/articles/privacy-law/does-the-stored-communications-act-protect-an-emails-subject-line-from-disclosure/, accessed 10/21/14]

- **Doe v. City of San Diego, No. 12-cv-0689-MMA (DHB), 2013 WL 2338713 (S.D. Cal. May 28, 2013).** Court found plaintiff had standing to challenge city’s subpoena to Verizon Wireless seeking “any and all records” for Plaintiff’s cellular phone, including texts, instant messages, etc. and found that Verizon was prohibited from disclosing such content by the Federal Stored Communications Act; Verizon was also prohibited from disclosing non-content records where such disclosure to a “governmental agency” is prohibited; court noted that alternative methods for discovery were available and
specifically noted the availability of a Rule 34 request for production. (K&L Gates database)


### Predictive Coding and Other Data Mining Procedures

Not very long ago, the concept of using predictive coding and other technologies to assist with the electronic discovery process seemed revolutionary. In just a few short years, using technology for review of ESI is not only considered mainstream, but is almost expected. Two cases stand as the first cases where judges clearly approved the use of predictive coding procedures, *Da Silva Moore (Da Silva Moore v. Publicis Groupe & MSL Group*, No. 11 Civ. 1279, 2012 WL 607412 (ALC) (AJP) (S.D.N.Y. Feb. 24, 2012)) and *Global Aerospace v. Landow Aviation (Global Aerospace, Inc. v. Landow Aviation, L.P.*, No. CL 61040 (Vir. Cir. Ct. Apr. 23, 2012)).
It is not difficult to appreciate the advantages of predictive coding and other technologies at various stages of electronic discovery. First, the costs of electronic discovery can be significant, depending on the size of the case, the number of parties, the complexity of the issues and the variety of ESI formats that may need to be collected, preserved, analyzed, reviewed and produced. Second, the Federal Rules of Civil Procedure and other court rules are designed to expedite and streamline the discovery process as much as possible, so the timeframe for electronic discovery is short. Third, without some sort of technology filtering at the beginning of the process, there is a risk that relevant ESI will be overlooked and not produced to the opposing party or that ESI that could have and should have been protected by privilege or another doctrine of confidentiality is inadvertently produced to the opposing party, with a range of options for the court, including granting a waiver of the privilege that lets the opposing party keep and use the ESI. The risks of spoliation are high, with substantial sanctions for both the parties and their attorneys.

Commentators have noted that in the future, failure to use predictive coding or other technology-assisted review may be grounds for disciplinary action, especially with Comment 8 ABA Model Rule 1.1 on Competence making it clear that competence includes the benefits and risks associated with relevant technology. Thus, it makes sense to understand the options for predictive coding and other technology-assisted review processes. This may be especially true when handling ESI from social media in a personal injury case, where the attorney is likely gleaning material in a variety of traditional (accident reports, medical records, witness testimony) and 21st century formats (Facebook, YouTube, Twitter, text
messages, iPhones, etc.) Also, the massive amounts of ESI mean that we need to look at electronic discovery from the vantage point of data mining because this is all about "big data".

In terms of predictive coding, an article in the April 2013 *ABA Journal* noted the following statistics (Computerized Review on Trial: Predictive Coding on The Rise in Courts, *ABA Journal*, April 2013, p. 30):

- 9% of cases studied discussed predictive coding or technology-assisted review
- 14% discussed cost considerations
- 16% addressed discoverability and admissibility
- 29% addressed procedural issues
- 32% addressed sanctions

Fortunately, there are many excellent articles available that discuss the spectrum of predictive coding:


Among the recent cases where the use of predictive coding was at issue, there is an interesting case from Indiana. The court addressed proportionality, given the substantial data
universe of 2.5 million documents, and the costs for ordering predictive coding versus the likelihood that this search process would be superior to the approach already being used by the defendants (summary from the Kroll Ontrack database – but see also the longer summary available from the K&L Gates database).

- *In re Biomet*, 2013 WL 1729682 (N.D. Ind. Apr. 18, 2013). In this behemoth multidistrict litigation, the defendants used key word search to cull 19.5 million documents prior to leveraging predictive coding. Pointing to commentary questioning the efficacy of key word search, the Plaintiffs’ Steering Committee alleged that the defendants “tainted the [search] process” by sharply reducing the data universe to 2.5 million documents primarily with key words. Instead, the plaintiffs argued that the defendants should go back to square one with predictive coding. The defendants countered by evoking the proportionality principle at Fed.R.Civ.P. 26(b)(2)(C), stating that the benefits of starting over with predictive coding would be outweighed by the burden of doing so. The court framed the relative positions of the parties succinctly: “It might be well that predictive coding, instead of a keyword search... would unearth additional relevant documents. But it would cost Biomet a million, or millions, of dollars to test the Steering Committee’s theory that predictive coding would produce a significantly greater number of relevant documents.” The court found that the defendants were allowed to carry on with their chosen search approach and encouraged both parties to continue to confer over future discovery.

Other 2014 cases specifically addressing predictive coding were located through the K&L Gates database.


- *Dynamo Holdings Ltd. P’ship v. Comm’r of Internal Revenue*, Nos. 2685-11, 8393-12 (T.C. Sept. 17, 2014) [with longer summary available from the K&L Gates website].


Admissibility/Authentication/Identifying Who Made That Post

The admissibility of social media as evidence is well-established, provided that it meets the criteria required under the rules of evidence, such as relevance and probative value, and that it can overcome any exceptions or objections that might be raised by the opposing party. This is true even in criminal cases, which was demonstrated in Indiana in 2009 by the murder case of Clark v. State (Clark v. State, 915 N.E.2d 126 (2009)). The following are some 2014 cases, with summaries from the K&L Gates database, that deal with the admissibility of social media and ESI that may be helpful.

- Chewning v. Commonwealth of Virginia, No. 2204-12-4, 2014 WL 931053 (Va. Ct. App. Mar. 11, 2014) (unpublished)(Cell phone records, text messages). Trial court did not err in admitting cell phone records or the content of text messages exchanged between Chewning and girlfriend (who pleaded guilty to murdering her mother) on the day of murder, as records were admissible as computer-generated records not requiring hearsay analysis, and, alternatively, as hearsay admissible under business records exception, text messages were admissible under exception for party and adoptive admissions, and authentication of records and texts was achieved through testimony of Verizon Wireless records custodian; further, court did not err in permitting prosecutor and detective to read aloud certain portions of texts during trial or in permitting the limited interpretation of abbreviations and misspellings provided by the readers.

- Commonwealth v. Gelfgatt, 11 N.E.3d 605 (Mass. 2014)(ESI; encryption key). Where the facts that would be conveyed by a criminal defendant through his act of decryption of computer files -- i.e., his ownership and control of the computers and their contents, knowledge of the act of encryption, and knowledge of the encryption key -- are already known to the government and are thus a "foregone conclusion," compelling the defendant to enter his encryption key does not violate the defendant's rights under the Fifth Amendment because the defendant is only telling the government what it already knows; accordingly, court reversed trial judge's denial of government's motion to compel decryption and remanded the case to the trial court for further proceedings.

them into evidence as they were properly authenticated by direct or circumstantial evidence; nor did court err when it accepted detective as an expert in digital forensic examination.

- United States v. Vayner, ---F.3d---, No. 13-803-cr, 2014 WL 4942227 (2d Cir. Oct. 3, 2014) Printout from internet ("Russian Facebook"). District Court reversed conviction where printout of profile page from VK.com (the "Russian Facebook") was not properly authenticated by witness who discovered the page but admitted he did not know who created it and where no extrinsic evidence was presented linking the defendant to the page; because error was not harmless, conviction was reversed.

In their article, Holt and San Pedro provide a practical approach to using social media as evidence. (Michael R. Holt and Victoria San Pedro. Social Media Evidence: What You Can’t Use Won’t Help You – Practical Considerations for Using Evidence Gathered on the Internet. The Florida Bar Journal, Vol. 88, No. 1, January 2104, pp. 8). After acknowledging the problems with trying to obtain social media information from Facebook, they recommend using the Wayback Machine (but note the requirements for authentication). They then turn their attention to the issues with presenting social media evidence, including authentication, especially because of concerns that the party or witness is not the same person who posted or transmitted the message. Their suggestions for authenticating social media content are personal knowledge (through the testimony of witnesses), distinctive characteristics (including appearance, contents, substance internal patterns, barcodes, serial numbers, or signatures), self-authenticating documents, expert witness testimony or Internet consultants. Other issues with the admissibility of social media as evidence discussed in the article are relevance, witness bias and hearsay. In terms of the authentication of social media content, Whaley provides the following comments (Alan Whaley. Whaley: Adventures in E-Discovery and Social Media, The Indiana Lawyer, July 30, 2014):
If a party has obtained social media content and needs to get it into evidence, authenticating that evidence may become an issue. One approach is to preserve and print a static image from a social media account – that can easily be done with a party’s public social media posts, for example. But the personal testimony of an authenticating witness, like the person who collected and printed the image, will probably be necessary. And with some kinds of content, like video or audio materials, special software and the assistance of a forensic computer consultant may be needed.

Seibert and Seibert also discuss the need to authenticate information from social media sites (Kimberly K. Seibert and Robert J. Seibert. Social Networking Sites and the Requirement of Authentication. *Michigan Bar Journal*, July 2014, pp. 32-35). Among the rules that are most likely to apply to social networking sites are:

- Rule 901(b)(1): Testimony of a Witness with Knowledge
- Rule 901(b)(3): Comparison by Trier or Expert Witness
- Rule 901(b)(4): Distinctive Characteristics and the Like
- Rule 901(b)(7): Public Records or Reproductions
- Rule 901(b)(9): Process or System

In their practice pointers, the authors state that “[t]he potential for fabricating or tampering with electronically stored information on social networking sites poses significant challenges from the standpoint of printouts of the site. The current trend is to require more evidence than just a distinctive profile page to authenticate a specific posting or message on the social networking site.” (*Id.* at 34). The authors suggest that some or even all of the following forms of authentication should be used for social media sites:

- Testimony from the creator of the profile and relevant postings
- Testimony from the person who received the message
- Testimony about the distinctive aspects in the messages revealing the identity of the sender
- Testimony regarding the account holder’s exclusive access to the account
- Testimony from the social networking website connecting the post to the person who created it (*Id.* at 35)
Obtaining Posted Content

Many resources provide practical information on social media as evidence, including how to request and preserve it, the duty to preserve, the consequences of failing to preserve and warning clients not to delete, preservation in a BYOD (Bring Your Own Device) world and methods of access to social media (See Ed Finkel. Evidence/Social Media: Building Your Case with Social Media Evidence, Illinois Bar Journal, vol. 102, no. 6, June 2014, p. 276, http://www.isba.org/ibj/2014/06/buildingyourcasewithsocialmediaevid, accessed 10/21/14; Margaret (Molly) DiBianca. Discovery and Preservation of Social Media Evidence., Business Law Today (BLT), January 2014, http://www.americanbar.org/publications/blt/2014/01/02_dibianca.html, accessed 10/21/14). In terms of obtaining posted content, DiBianca identifies several methods in her article and discusses the advantages and difficulties with each method: direct access to social media accounts (see Gatto v. United Air Lines, Inc.), in camera review (see Offenback v. L.M. Bowman, Inc.), attorney’s eyes only (see Thompson v. Autoliv ASP, Inc.) and third-party subpoenas (but beware of issues with the Stored Communications Act, see Crispin v. Christian Audigier, Inc., 717 F.Supp.2d 965 (C.D. Cal. 2010)). Likewise, Social Media Evidence – How to Find It and How to Use It offers the following principles and trends for involving the discovery of social media evidence on pages 15-19 ((http://www.americanbar.org/content/dam/aba/administrative/litigation/materials/aba-annual-2013/written_materials/15_1_social_media_evidence.authcheckdam.pdf, accessed 10/21/14):

- Discovery requests/subpoenas for social media evidence should be drawn narrowly.
- Tie your discovery requests to information already in hand that shows the request is seeking evidence that likely exists and, therefore, not a fishing expedition.
- Compulsion efforts are better targeted at the users of the social media, not at the social media providers.
If you have evidence that the producing party has improperly withheld evidence, go to the court for sanctions and/or for more social media discovery.

Consider who “owns” the social media link. You may have more than one potential discovery target.

In camera review by the court may be needed.

If the request is too broad, the court may limit it or deny it altogether.

In terms of obtaining posted content, we can look at the summaries of some cases from the K&L Gates database related to motions to compel technology-enabled content from a variety of sources (email, text messages, social media such as Facebook, Flickr, Twitter, etc.)

- **D.O.H. ex rel. Haddad v. Lake Cent. Sch. Corp.,** No. 2:11-CV-430, 2014 WL 174675 (N.D. Ind. Jan. 15, 2014). Following the rule set out in E.E.O.C. v. Simply Storage Mgmt., LLC, 270 F.R.D. 430 (S.D. Ind. 2010), court ordered plaintiff to produce social media postings, messages, status updates, wall comments (etc.) for the relevant time period “that reveal, refer, or relate to any emotion, feeling, or mental state, as well as communications that reveal, refer, or relate to events that could reasonably be expected to produce a significant emotion, feeling, or mental state.”


- **Giacchetto v. Patchogue-Medford Union Free School Dist.,** No. CV 11-6323(ADS)(AKT), 2013 WL 2897054 (E.D.N.Y. May 6, 2013). In this case, the court conducted a “traditional relevance analysis” to assess Defendant’s request for broad access to Plaintiff’s social networking accounts and concluded that only limited discovery was appropriate. Specifically, the court concluded that “unfettered access to Plaintiff’s social networking history will not be permitted simply because Plaintiff has a claim for emotional distress damages.” Thus, the court ordered Plaintiff’s counsel to review Plaintiff’s postings and to produce those determined to be relevant, “keeping in mind the broad scope of discovery contemplated under Rule 26.” [a longer summary is available from the K&L Gates website]

- **In re Christus Health S.E. Texas,** 399 S.W.3d 343 (Tex. Ct. App. 2013). Denial of motion to compel documents reflecting deceased patient’s children’s purchases and calls on the day the patient underwent his at-issue procedure was no abuse of discretion where the request for production was not sufficiently limited in time and was therefore overly broad; request for all posting to social media regarding the patient or his death was also not limited in time and thus “overly broad on its face” and trial court did not abuse discretion in denying the motion to compel.

- **Johnson v. PPI Tech. Servs., L.P.,** No. 11-2773, 2013 WL 4508128 (E.D. La. Aug. 22, 2013) Court sustained objections to requests for social media content reasoning that
although such content was potentially discoverable, Defendant had not made a sufficient showing that the material sought was “reasonably calculated to lead to the discovery of admissible evidence,” and went on to reason that: “Simply placing their mental and physical conditions at issue is not sufficient to allow PPI to rummage through Johnson's or Croke's social media sites. Almost every plaintiff places his or her mental or physical condition at issue, and this Court is reticent to create a bright-line rule that such conditions allow defendants unfettered access to a plaintiff’s social networking sites that he or she has limited from public view.”

• Keller v. Nat'l Farmers Union Prop. & Cas. Co., No. CV 12-72-m-DLC-JCL, 2013 WL 27731 (D. Mont. Jan. 2, 2013). Court denied defendant’s motion to compel plaintiffs’ production of printouts of all social media content where the court recognized that discovery of social network content has been allowed by other courts upon a showing that publically available information on those sites undermines the plaintiff’s claims and where no such showing was made in the present case.

Social Media Preservation

Two of my favorite authors are Sharon Nelson and John Simek, who have been on the cutting edge of security, digital forensics, electronic discovery and legal technology for many years through their company, Sensei Enterprises. (Sensei Enterprises, Inc., http://www.senseient.com/, accessed 10/22/14). I use their materials extensively in several of the courses I teach at the School of Informatics and Computing (Indiana University). One suggestion is that all lawyers register for Sensei’s free article distribution service. A recent article by Nelson and Simek covers the preservation and harvesting of social media evidence as well as authentication, which is available from the Sensei Enterprises website (Sharon D. Nelson and John W. Simek. Social Media: Preservation, Harvesting and Authentication. Sensei Enterprises, 2014). In this article, they discuss the benefits and risks of outsourcing the preservation process versus trying to handle it in-house, with special concerns raised about the danger of spoliation which often results in significant sanctions (Id. at 1-2). They also provide practical suggestions for how to harvest the information without going through the social media
vendor, who are only allowed to provide basic subscriber information, but not content, because of the Stored Communications Act (Id. at 3).

In terms of the preservation of social media content, Whaley provides the following suggestions (Alan Whaley. Whaley: Adventures in E-Discovery and Social Media, The Indiana Lawyer, July 30, 2014):

One significant aspect of electronic data is that it frequently changes, and that is especially true of social media content. Therefore, at the beginning of a case it may be particularly important to try to preserve the status of another party’s social media information. You can do this with a preservation notice to that party, or if you think additional measures are needed, consider a preservation request to the service provider or even a “preservation subpoena” and motion filed with a court. (Id.)

An especially helpful resource is provided by Ball, which discusses the importance of a comprehensive preservation letter that covers all types of ESI, including how to handle back-up tapes, drive cloning and imaging and metadata. (Craig Ball. The Perfect Preservation Letter. http://www.craigball.com/perfect%20preservation%20letter.pdf, accessed 10/22/14). The Appendix to his article is an exemplar of a preservation demand letter to an opposing party.

The duty to preserve ESI in all formats is covered by the Federal Rules of Civil Procedure as well as a whole chain of cases, starting with the Zubulake v. UBS Warburg decisions from the early 2000s. This duty extends to social media of kinds. An important point to keep in mind is that this ESI may reside on a wide variety of devices and may also be found on personal devices with the increasing number of companies that are using a BYOD (Bring Your Own Device) strategy as a way to manage their technology.

Some recent cases located through the K&L Gates database, along with their summaries, include:
• *Ogden v. All-State Career School*, No. 2:13cv406, 2014 WL 1646934 (W.D. Pa. Apr. 23, 2014) (Electronic communications made or affirmatively acknowledged by plaintiff on any social networking website (e.g., Twitter, Facebook, MySpace) during the period of alleged harassment). Court observed that ordering plaintiff to permit access to or produce complete copies of his social networking accounts would permit defendant to cast too wide a net and sanction an inquiry into scores of quasi-personal information that would be irrelevant and non-discoverable, and stated: “Defendant is no more entitled to such unfettered access to plaintiff’s personal email and social networking communications than it is to rummage through the desk drawers and closets in plaintiff’s home”; court ruled that defendant was only entitled to limited discovery of plaintiff’s communications, and set out particular steps that plaintiff must take to comply with defendant’s requests.

• *Painter v. Atwood*, No. 2:12-cv-01215-JCM-RJJ, 2014 WL 1089694 (D. Nev. Mar. 18, 2014) Text messages and social media posts (Facebook comments and photographs). Court granted defendants’ motion for sanctions in the form of an adverse inference instruction where, after she contemplated filing a lawsuit and retained counsel, plaintiff intentionally deleted Facebook comments that stated she enjoyed working for defendants; however, no sanctions were warranted for plaintiff’s deletion of text messages, as she was not on notice to preserve the texts at the time she deleted them (prior to leaving defendants’ employ).

• *Petition of John W. Danforth Group, Inc*, No. 13-MC033S, 2013 WL 3324017 (W.D.N.Y. July 1, 2013)(Anticipated witness's mobile device). Where petitioner sought to perpetuate evidence and an order of preservation pursuant to Rule 27 in light of an anticipated witness’s untruthfulness about his use of social media and refusal to turn over his personal mobile phone or to allow for a backup to be made absent a court order, the court declined to issue such an order where Rule 27 relief should be granted “only in special circumstances to preserve evidence that would otherwise be lost” and where the petitioner’s “generalized statements of concern” were insufficient to warrant pre-complaint intervention.

**Hearsay and Electronically Stored Information**

As stated on page 21 of *Social Media Evidence – How to Find It and How to Use It* (http://www.americanbar.org/content/dam/aba/administrative/litigation/materials/aba-annual-2013/written_materials/15_1_social_media_evidence.authcheckdam.pdf, accessed 10/21/14),

Of course, hearsay objections may arise when using electronic evidence. See *Miles v. Raycom Media, Inc.*, 2010 WL 4791764 *3 n.1 (S.D.Miss. Nov. 18, 2010), (unsworn statements made on Facebook page by nonparties were inadmissible under FRE 801). You may have multiple layers of hearsay involved and have to rely upon several hearsay
exceptions. Judge Grimm provides an extensive discussion in Lorraine of hearsay in the context of electronically stored information. The procedural posture may affect how the court treats the information. In granting defendant’s motion for summary judgment in *Witt v. Franklin County Board of Education*, 2011 WL 3438090 *2-4* (E.D.Pa. Aug. 4, 2013), the court considered three Facebook messages from nonparties offered by plaintiff because plaintiff could have reduced them to admissible form at trial by calling the witnesses.

*See also,* from the K&L Gates database:

- *Chewning v. Commonwealth of Virginia*, No. 2204-12-4, 2014 WL 931053 (Va. Ct. App. Mar. 11, 2014) (unpublished). Trial court did not err in admitting cell phone records or the content of text messages exchanged between Chewning and girlfriend (who pleaded guilty to murdering her mother) on the day of murder, as records were admissible as computer-generated records not requiring hearsay analysis, and, alternatively, as hearsay admissible under business records exception, text messages were admissible under exception for party and adoptive admissions, and authentication of records and texts was achieved through testimony of Verizon Wireless records custodian; further, court did not err in permitting prosecutor and detective to read aloud certain portions of texts during trial or in permitting the limited interpretation of abbreviations and misspellings provided by the readers.

**Motion in Limine**


A motion in limine is a motion used in a civil lawsuit to preclude evidentiary issues or conduct before it is seen or heard by a jury. The Latin term “in limine” means “at the threshold.” Motions in Limine are typically filed just before the commencement of trial. However, motions in limine can be filed after the trial begins. The primary advantage of the “in limine” motion is to avoid trying to undo harm done when jurors have been exposed to damaging evidence, even when later stricken by the court. Motions in limine play a critical role in pretrial and trial strategies. (*Id.*)
She then outlines the use of motions in limine as precluding the opposing party from introducing certain prejudicial evidence or instructing opposing counsel, and any person in opposing counsel’s control, to avoid any mention of certain evidence or testimony during trial or in argument in front of the jury (Id. at 2). She goes on to state that “[s]trategies for the presentation of motions in limine are as broad as the imagination of the trial team” and provides the more common types:

- Evidence that consumes unnecessary time or duplicative testimony or evidence;
- Evidence that creates a substantial danger of undue prejudice;
- Evidence that confuses the issues or is misleading when weighed against the probative value of the challenged evidence;
- Evidence that lacks foundation;
- Inadmissible business records or other writings relied upon by a witness;
- Evidence that raises authenticity issues;
- Scientific tests or studies not shown to be reliable;
- Witness’ non-felony criminal record;
- Evidence that would be barred by the discovery rules;
- Exclusion of experts not disclosed in response to a CCP 2034.210 demand;
- Exclusion of witnesses not listed in the witness list;
- Exclusion of expert opinions based on speculation (Id. at 2-3).

Stravitz also describes when a motion in limine can be especially useful when it involves social media that the client has already posted and that has not been requested by the opposing party (Eric Stravitz. Tackling Social Media in Litigation. Personal Injury Lawyer Blog, December 19, 2013, accessed 10/17/14). He states that “[i]f you determine that you must produce your client’s social media evidence (or are ordered to do so), a Motion in Limine would be your next line of defense for excluding arguably irrelevant material (under FRE 401 or 402) or unfairly prejudicial material (under FRE 403). Note that evidentiary impediments to the admissibility of such materials may also exist.” (Id. at 3) For a sample motion in limine that involves a high-profile case, see Defendant’s Motion in Limine Regarding the Use of Certain

**The author gratefully acknowledges the efforts of K&L Gates and Kroll Ontrack to provide databases of cases with case summaries. These databases are easy to search and their case summaries have been used extensively throughout these materials.}