INTELLECTUAL PROPERTY
Course Handbook Series
Number G-1043

Information Technology Law Institute 2011:

Navigating the New Risks in Mobile Technology, Social Media, Electronic Records and Privacy

Co-Chairs
Peter Brown
Leonard T. Nuara

To order this book, call (800) 260-4PLI or fax us at (800) 321-0093. Ask our Customer Service Department for PLI order number 29060, Dept. BAV5.

Practising Law Institute
810 Seventh Avenue
New York, New York 10019

12

USING SOCIAL MEDIA IN LITIGATION

Kurt A. Kappes
Greenberg Traurig, LLP

Kishan Barot
University of California, Davis School of Law

Table of Contents

I. UPDATING CORPORATE DOCUMENT RETENTION POLICIES TO ACCOUNT FOR ELECTRONIC SOCIAL MEDIA

A. Duty to Preserve Social Media Evidence

i. The duty to preserve evidence turns on whether that evidence is in the party's possession, custody, or control under Fed. R. Civ. P. 34.

   a. Not surprisingly, determining possession, custody, or control is a straightforward determination with tangible items.

   b. Importantly, electronically stored information (ESI) is no less subject to preservation and disclosure than paper documents. *Zubulake v. UBS Warburg LLC*, 217 F.R.D. 309, 317 (S.D.N.Y. 2003).

ii. How is possession, custody, or control determined with social media?

   a. The direct users and owners of social networking sites have a duty to preserve social media: a user has control over their profile and the operators possess the data on their servers.

   b. Must employers preserve the social media usage of their employees?

      1. In these scenarios, the relevant factor to consider is whether the evidence was *entirely* beyond the control of the employer. *Adkins v. Wolever*, 554 F.3d 650, 653 (6th Cir. 2009).

         a) Thus, an employee's use of social media for business purposes certainly heightens the employer's duty to preserve that evidence. Lisa Thomas, *Social Networking in the Workplace: Are Private Employers Prepared to Comply with Discovery Requests for Posts and Tweets?*, 63 SMU L. REV. 1373, 1401 (2010).

         b) Similarly, an employer monitoring social media usage will likely heighten the duty to preserve that evidence. Steven C. Bennett, *Civil Discovery of Social Networking Information*, 39 SW. L. REV. 413, 429 (2010).

2. An important lesson from *Adkins* is that employers must be mindful of their computer usage policies. Strong business reasons exist to control computer usage or even issue such a policy.

    a) Simply put, computer usage policies and document retention policies should be developed in conjunction with each other.

B. Updating Document Retention Policies

i. Given that a company may be expected to preserve social media evidence, it makes sense that document retention policies should reflect that.

ii. Practice points in creating a document retention policy

a. Firstly, create policies based on your company's specific social media needs and your employees' actual social media usage. Bennett, *supra*, at 429.

1. There is no one-size-fits-all document retention policy.

b. Secondly, audit and enforce your policy.

1. Enforcement is the only way to give your policy any credibility in court. *ESI Trends, Technology & Document Retention Obligations*, THE LEGAL TALK NETWORK (Dec. 21, 2010), http://legaltalknetwork.com/podcasts/esi-report/2010/12/esi-trends-technology-document-retention-obligations/.

2. Obtain signed periodic acknowledgments of policy from employees. Bennett, *supra*, at 430-31.

c. Lastly, update retention policy to reflect any relevant technological developments.

1. For example, Facebook's recent entry into the email market will likely complicate existing document retention policies.

    a) Facemail, as it is popularly dubbed, does not currently allow for the deletion of emails from Facebook's servers. That is, emails will forever remain on Facebook's servers despite being removed from a user's mailbox.

b) Facemail is thus "a problem in that it means these e-mails will be outside the boundaries of [a company's] retention policy. . . . So, if [a company] typically delete[s] e-mail every 90 days, 2 years, etc., they will be unable to enforce that on e-mails created in this system." Shannon Green, *Is Facemail Going to Drive General Counsel Insane?*, LAW.COM, Nov. 11, 2010, *available at* http://www.law.com/jsp/cc/PubArticleCC.jsp?id=1202475162535.

2. Other challenging developments include cloud computing and smartphones. Like Facemail, these technologies involve storing data on devices typically not under a company's direct control and thus pose the same retention concerns.

II. PURSUING SOCIAL MEDIA COMMUNICATIONS IN PARTY AND THIRD-PARTY DISCOVERY

A. Obtaining Social Media Evidence through Independent Research

i. Start your search as soon as litigation is likely.

ii. Where to find the evidence?

a. Social Media Sites

1. Obviously, to find social media evidence, the best place to search is social media sites themselves.

2. It is important to note that most social media sites like Facebook and Twitter offer limited search functionality.

3. In many cases, however, social media sites can be somewhat troublesome to use or may not possess older content.

b. Google

1. Using an advanced Google search, you can search the contents of a website even if the website itself lacks a search feature. Google is sometimes unable to search social media sites due to their design.

2. Google also offers specialized search services for blogs and social media status updates: Google Blog Search

(http://blogsearch.google.com/) and Google Realtime (http://www.google.com/realtime).

c. Historical Databases

1. Numerous services, such as the Wayback Machine (http://web.archive.org/), archive historical copies of websites. While these are great resources to obtain deleted or offline content, they have a few limitations.

a) For one, these services often archive at unpredictable intervals, which means that not all versions of a website will be preserved.

b) Additionally, most services respect a website's decision to not be archived through its *robots.txt* settings.

1. Importantly, however, a party can be ordered by court to remain archivable to prevent spoliation of evidence. *Netbula, LLC v. Chordiant Software, Inc.*, No. C08-00019 JW (HRL), 2009 WL 3352588 (N.D. Cal. Oct. 15, 2009).

2. Another useful service is Topsy (http://www.topsy.com/), which archives public Twitter profiles.

a) One of the most notable features of this service is that a user's postings will remain on Topsy even if they privatized or deleted their account so long as they do not make a removal request.

d. A note on "deleted" content

1. Sometimes, even content that a user deleted from their profile may nonetheless remain on the host's servers.

2. One informal study found that, while Twitter and Flickr deleted images immediately upon request, Facebook and MySpace simply removed the images from the profiles without ever deleting the images from the servers themselves. Thus, direct URLS to these images can remain active for months after deletion. Jacqui Cheng, *Are 'deleted' photos really gone from Facebook? Not Always*, THE WEB, Jul. 3, 2009, http://arstechnica.com.

3. Be warned, however, that there is no single method to obtain these URLs. The process will require some creativity and web-savviness.

iii. How should social media evidence be captured and stored?

a. Traditionally, Internet evidence was preserved through "printing" the web page to a PDF file. Since websites are rarely designed to be printed, this option often results in formatting issues.

b. Recently, however, products have emerged from companies like Iterasi and Smarsh to preserve social media sites with better integrity and searchability.

1. Most importantly, however, these services are usually automated, thereby eliminating the risk of missing social media updates that are only temporarily online.

2. These services range significantly in price, quality, and purpose. *See generally* Tanzina Vega, *Tools to Help Companies Manage Their Social Media*, N.Y. TIMES, Nov 14, 2010, http://www.nytimes.com/2010/11/15/business/media/15social.html.

3. The Legal Talk Network has a useful discussion comparing these technologies: *Inside Social Media Archiving*, THE LEGAL TALK NETWORK (Oct. 25, 2010), http://legaltalknetwork.com/podcasts/digital-detectives/2010/10/inside-social-media-archiving/.

c. Whichever method you choose, you need to make sure it poses no authenticity issues. In general, this involves time-stamping the documents, recording the URLs, and keeping track of how you obtained the evidence.

B. Obtaining Social Media Evidence through Formal Discovery

i. The Discovery Process & Social Media Considerations

a. As any other form of electronically-stored information, social media is discoverable under Rule 34.

b. The following are some benchmarks during a case where you might want to consider discovering social media:

Method	Rule	Practice Points
Initial Disclosures	26(a)(1)	• Investigate the social media presence of the disclosed parties.
Discovery Conference	26(f)	• Discuss the issue of social media.
Interrogatories	33	• Ask for social media services used by the parties. • Determine relevant usernames or aliases. • Confirm ownership of accounts.
Requests for Admission	36	• Obtain admissions regarding specific postings (e.g. that the party did in fact make certain postings).
Requests for Production	34	• Ensure that all requests are narrowly tailored on breadth and relevancy grounds to avoid objections.
Depositions	30-32	• Explore details of the communications.
Stipulations	29	• At the very least, obtain stipulations regarding the more tedious aspects of the social media (e.g., identity and ownership of the accounts).

ii. Discovery of Corporate Social Media

a. As explained above, corporate social media is just as discoverable as any other corporate document.

    1. Thus, social media policies are important in determining a corporation's preservation duties.

iii. Discovery of Personal Social Media

a. It is no surprise that social media can be very personal and even embarrassing. Savvy users may even adjust their privacy settings to protect against the disclosure of such information. At what point, then, will discovery be limited to prevent the production of such evidence?

    1. The short answer is that discovery probably will not be limited as long as it seeks relevant information.

b. Keeping with the tenor of Rule 26, courts have consistently held that discoverability turns on relevancy, not privacy.

    1. Rule 26(b)(1) permits broad discovery by design:

        a) Discovery is permitted into "any matter, not privileged, that is relevant to the claim or defense of any party, including the existence, description, nature, custody, condition, and location of any books, documents, or other tangible things and the identity and location of persons having knowledge of any discoverable matter."

    2. One of the most discussed cases on this matter, *E.E.O.C. v. Simply Storage Mgmt., LLC* found that social media content is "not shielded from discovery simply because it is 'locked' or 'private,'" but instead "must be produced when it is relevant to a claim or defense in the case." *E.E.O.C. v. Simply Storage Mgmt., LLC*, 270 F.R.D. 430, 434 (S.D. Ind. 2010).

c. While no blanket privacy exception exists, there are a few privacy-related hurdles in discovering social media evidence:

    1. Firstly, discovery requests for social media evidence may be so broad that the production of private and irrelevant data is likely. Bennett, *supra*, at 420.

    2. Secondly, protective orders may be issued upon a showing of good cause to protect parties from "annoyance, embarrassment, oppression, or undue burden or expense" under Rule 26(c)(1).

    3. Thirdly, the Stored Communications Act (SCA) prohibits internet service providers from disclosing private

communications without a court order or the user's consent.

a) Some providers take their obligations under the SCA very seriously and will hesitate to produce even pursuant to a subpoena. Eric B. Meyer, *How Facebook Can Make or Break Your Case*, LAW.COM, Jul. 27, 2010, *available at* http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202463917586.

b) Importantly, however, the SCA is concerned only with the disclosure of *private* communications.

1. Clarifying this distinction, a California district court recently found that wall posts were public in nature, unlike direct messages, which were similar to private emails. *Crispin v. Christian Audigier, Inc.*, 717 F. Supp. 2d 965 (C.D. Cal. 2010).

d. A note on whether social media communications are even considered "private"

1. Courts are generally dismissive of the claim that social media communications are private.

2. For one, social networking sites exist to facilitate communication with large groups of people and even the general public.

a) "By providing personal information for others to see on a social networking site, a user is not seeking to preserve this information as private, but rather is making a conscious choice to publicize it." Ronald J. Levine & Susan L. Swatski-Lebson, *Social Networking and Litigation*, 25 E-COM. L. AND STRATEGY 1 (2009). *Accord Guest v. Leis*, 255 F.3d 325 (6th Cir. 2001) (holding that posts on public Internet forums lack a reasonable expectation of privacy); *Moreno v. Hanford Sentinel, Inc.*, 172 Cal. App. 4th 1125, 1130 (Cal. Ct. App. 2009) (discussing the affirmative and public nature of posting information on MySpace.com).

b) Even when a user limits access to their profile through privacy settings, a reasonable expectation of privacy may not exist because that content could be

disseminated by other users without the poster's consent. Kristin L. Mix, *Discovery of Social Media* (Sep. 23, 2010), http://facultyfederaladvocates.org/downloads/1009_mix_socialmedia.pdf. *Accord Guest v. Leis*, *supra*, at 333; *Romano v. Steelcase Inc.*, 907 N.Y.S.2d 650, 657 (N.Y. Sup. Ct. 2010).

3. Secondly, most social networking sites require users to accept terms of use that usually further diminish any reasonable expectation of privacy. *See McMillen v. Hummingbird Speedway, Inc.*, 2010 Pa. Dist. & Cnty. Dec. LEXIS 270, at *7-8 (Pa. County Ct. 2010) (discussing how Facebook's and MySpace's terms of use explicitly warn users that their information can be shared or monitored).

    a) For example, Facebook's privacy policy contains the following clause on the "[r]isks inherent in sharing information":

        1. "We cannot guarantee that only authorized persons will view your information. We cannot ensure that information you share on Facebook will not become publicly available." Facebook, *Privacy Policy*, http://www.facebook.com/policy.php (last visited Jan. 16, 2011).

4. Lastly, in the case of workplaces, courts have consistently held that an office computer policy can diminish any reasonable expectation of privacy an employee may have. *See Biby v. Bd. of Regents*, 419 F.3d 845, 850-51 (8th Cir. 2005); *United States v. Angevine*, 281 F.3d 1130,1133-35 (10th Cir. 2002); *Muick v. Glenayre Electronics*, 280 F.3d 741, 743 (7th Cir. 2002); *Wasson v. Sonoma County Jr. Coll. Dist.*, 4 F. Supp. 2d 893, 905-06 (N.D. Cal. 1997).

    a) On the other hand, courts have also held that employees do have a reasonable expectation of privacy in the absence of such a policy or regular computer monitoring. *See Leventhal v. Knapek*, 266 F.3d 64, 74 (2d Cir. 2001).

iv. Subpoenas on Third-Party Service Providers

a. For various reasons, it may become necessary to subpoena third-party service providers instead of the users themselves.

b. For instance, a party may want to sue an anonymous person who posted defamatory material on the Internet, but may be unable to ascertain that person's identity.

   1. In these situations, it has become common practice to sue a John Doe, subpoena the service provider for the poster's identity, and then amend the Complaint to reflect to the true identity of poster.

   2. Importantly, the request will not be barred under the SCA if it is simply seeking the poster's identity and not any *private* messages. *See* Erica Johnstone, *Unmasking Anonymous Posters*, CAL. LAW., Dec. 2010, *available at* http://www.callawyer.com/story.cfm?eid=912908.

      a) Generally, courts have "consistently held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Smith v. Maryland*, 442 U.S. 735, 743–44 (1979). As such, several circuits have held that no reasonable expectation of privacy exists in Internet subscriber information (e.g., addressees of messages). *Rehberg v. Paulk*, 611 F.3d 828, 843 (11th Cir. 2010).

   3. In considering a motion to quash a subpoena, however, several jurisdictions require the requesting party to at least attempt to contact the poster and establish a prima facie case against them. *See* Philip Gordon, *Employers' Efforts to Combat Cybersmear Hit the First Amendment Shield*, LITTLER WORKPLACE PRIVACY COUNS. (Feb. 19, 2008), http://privacyblog.littler.com/.

   4. It is also important to note that these "John Doe lawsuits" have come under increased criticism ever since the Record Industry Association of America relied on them to sue scores of defendants alleged to have distributed copyrighted music unlawfully. ELECTRONIC FRONTIER FOUNDATION, RIAA V. THE PEOPLE: FIVE YEARS LATER, Sept. 2010, *available at* http://www.eff.org/wp/riaa-v-people-years-later (last visited Jan. 16, 2011).

5. Lastly, it is important to note that the process used to tie a posting on the Internet to an actual person can be problematic. For example, a posting made at a café through a shared IP address may mask the poster's identity.

c. Again, under the SCA, hosts typically produce private communications only if presented with the account holder's consent. Joel Patrick Schroeder & Leita Walker, *Social Media in Civil Litigation*, LAW360, Oct. 12, 2010, *available at* http://www.law360.com/web/articles/200684. Thus, third-party subpoenas to service providers are rarely proper. *O'Grady v. Superior Court*, 139 Cal. App. 4th 1423, 1445 (Cal. Ct. App. 2006).

d. Also consider subpoenaing the poster's friends, whose wall the poster may have written on. Meyer, *supra*.

C. Admitting the Evidence

i. A discussion concerning the admissibility of electronically stored information should consider *Lorraine v. Markel Am. Ins. Co.*, 241 F.R.D. 534 (D. Md. 2007).

a. *Lorraine* provides "an excellent guide to an important aspect of the care that may be or become necessary when parties attempt to offer electronic information into evidence." Patrick J. Hatfield et al., *From E-Discovery to EAdmissibility?:* Lorraine v. Markel *and What May Follow*, Jun. 1, 2007, http://www.lordbissell.com/Newsstand/2007-06_EDiscovery_Neiditz_Hatfield_Safer.pdf.

b. Judge Grimm, who presided over *Lorraine*, later co-authored an authoritative article that built upon the opinion: Hon. Paul W. Grimm et. al., *Back to the Future:* Lorraine v. Markel American Insurance Co. *and New Findings on the Admissibility of Electronically Stored Information*, 42 AKRON L. REV. 357 (2009).

c. To be clear, *Lorraine* covers all forms of electronically stored information, not just social media.

ii. What is *Lorraine v. Markel* about?

a. To paint in broad strokes, *Lorraine* is an attempt to remind practitioners that the admissibility rules apply just as strongly to electronic evidence as other forms of evidence.

b. To discuss the admissibility of social media evidence, this Presentation will borrow heavily from *Lorraine*.

iii. Authenticity is arguably the most challenging hurdle in admitting social media evidence.

a. Under Rule 901(a), the authenticity requirement is "satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims."

b. Courts may be distrustful of Internet evidence.

1. This distrust may be greater with social media, which are prone to fake accounts and sloppy security.

2. A particularly impassioned example of this distrust is reflected in *St. Clair v. Johnny's Oyster & Shrimp, Inc.*, 76 F. Supp. 2d 773 (S.D. Tex. 1999).

a) In this case, the plaintiffs sought to prove ownership of a boat through the U.S. Coast Guard's online vessel database.

b) Referring to such evidence as "voodoo information," the court opined:

1. "While some look to the Internet as an innovative vehicle for communication, the Court continues to warily and wearily view it largely as one large catalyst for rumor, innuendo, and misinformation. So as to not mince words, the Court reiterates that this so-called Web provides no way of verifying the authenticity of the alleged contentions that Plaintiff wishes to rely upon in his Response to Defendant's Motion. There is no way Plaintiff can overcome the presumption that the information he discovered on the Internet is inherently untrustworthy. Anyone can put anything on the Internet. No web-site is monitored for accuracy and nothing contained therein is under oath or even subject to

independent verification absent underlying documentation. Moreover, the Court holds no illusions that hackers can adulterate the content on any web-site from any location at any time. For these reasons, any evidence procured off the Internet is adequate for almost nothing, even under the most liberal interpretation of the hearsay exception rules found in Fed.R.Civ.P. 807." *Id. at* 774-75.

c) Written in 1999, the court's opinion perhaps reflects an early view of the Internet. Still, it raises the same authenticity concerns regarding accuracy and security that are present today with social media. Indeed, several opinions have continued to uphold *St. Clair* for this purpose. *See Monotype Imaging, Inc. v. Bitstream, Inc.*, 376 F. Supp. 2d 877, 893 (N.D. Ill. 2005); *Curran v. Amazon.com, Inc.*, No. 2:07-0354, 2008 WL 472433 (S.D.W. Va. Feb. 19, 2008); *Novak v. Tucows, Inc.*, No. 06CV1909, 2007 WL 922306 (E.D.N.Y. Mar. 26, 2007) aff'd, 330 F. App'x. 204 (2d Cir. 2009).

3. Thus, the question remains: how do we authenticate electronic evidence?

c. To address this concern, the *Lorraine* article analogized the authentication of ESI to the illustrations under Rule 901(b) (Hon. Paul W. Grimm et. al., *supra*, at 367-68). The relevant portions of this chart are reproduced below:

1. E-mail Evidence:

a) Rule 901(b)(1), "Testimony of a Witness with Knowledge"

b) Rule 901(b)(3), "Comparison by Trier or Expert Witness"

c) Rule 901(b)(4), "Distinctive Characteristics and the Like"

2. Internet Websites

a) Rule 901(b)(1), "Testimony of a Witness with Knowledge"

b) Rule 901(b)(3), "Comparison by Trier or Expert Witness"

c) Rule 901(b)(4), "Distinctive Characteristics and the Like"

d) Rule 901(b)(7), "Public Records or Reports"

e) Rule 901(b)(9), "Process or System"

3. Chat Room and Test Messages

a) Rule 901(b)(1), "Testimony of a Witness with Knowledge"

b) Rule 901(b)(4), "Distinctive Characteristics and the Like"

4. Digital Photographs

a) Rule 901(b)(9), "Process or System"

d. Importantly, authenticity can also be established by circumstantial evidence. *United States v. Clark*, 649 F.2d 534 (7th Cir. 1981).

1. Thus, marshaling identifying details from the evidence is key.

a) For instance, a Maryland court cited similar authority and found a printout of a MySpace profile to be sufficiently authenticated because it included a photograph, date of birth, and references to the account holder's children (*Griffin v. State*, 995 A.2d 791, 799 (MD App. 2010)).

e. For social media evidence, self-authentication is not likely.

1. Social media content usually comes with a degree of casualness that precludes the Rule 902 exceptions (e.g. certified documents, documents under seal, official publications, etc.)

iv. Best Evidence

a. Luckily, social media rarely poses a best evidence issue.

1. Original copies of evidence are required under Rule 1002.

2. However, under Rule 1001(3), if "data are stored in a computer or a similar device, any printout or other output

readable by sight, shown to reflect the data accurately, is an 'original.'"

b. Importantly, however, Rule 1002 is inapplicable unless party is seeking to prove the contents of the evidence.

v. Hearsay

a. In considering electronic evidence, *Lorraine* reminds practitioners to follow a standard hearsay analysis:

1. Is the evidence actually a "statement" at all?
2. Is the evidence made by a "declarant"?
3. Is the evidence offered for the truth of the matter asserted?
4. Is the evidence excluded from the definition of hearsay?
5. Is the evidence covered by the exceptions to hearsay?

b. Social media evidence may be able to take advantage of the hearsay exemptions or exceptions in multiple scenarios:

1. Present sense impressions can include a live chat where one side is typing up the contents of a verbal conversation.
2. Since social media is a cathartic release for some, admissions by party-opponents would undoubtedly be a common exception with social media hearsay.
3. In some cases, social media evidence may even be admissible as excited utterances.

a) With the popularization of smartphones, it has become commonplace for people to update their social media statuses with the minutiae of everyday life. In some cases, these may be excited utterances.

b) That the status update had to be typed out in a somewhat cool manner makes it less likely that the utterance was excited. Still, a colorable argument may be made in support of the exception in some situations.

vi. Unfair Prejudice under Rule 403

a. Often, social media evidence can be deeply personal and inflammatory, especially if it involves pictures or video.

Parties, then, should be mindful of an unfair prejudice objection.

III. REVIEWING THE ETHICAL CONSIDERATIONS SURROUNDING ATTORNEYS' SOCIAL MEDIA ACTIVITY

A. Maintaining Confidentiality

i. With every technological advance that facilitates communication comes increased pressures on attorneys to maintain the confidentiality of their clients.

ii. It is a reality that attorneys "love to discuss interesting cases they're working on, love to swap wars stories, and love to pad their professional credentials by revealing their prestigious clients and important matters" (JASON SCHULTZ ET AL., CAN LAWYERS TWEET ABOUT THEIR WORK? CONFIDENTIALITY & LEGAL PROFESSIONALISM IN THE AGE OF SOCIAL MEDIA,Oct. 23, 2009, *available at* http://www.law.berkeley.edu/files/Can-Lawyers-Tweet-about-Their-Work.pdf).

   a. While discussing confidential matters is risky enough in person, doing the same over social media is undoubtedly worse.

   b. For one, social media is particularly notorious for poor security – both on the user's end as well as the provider's.

   c. Secondly, there is no effective way to control the redistribution of this information over the Internet.

      1. If an opposing party accidentally receives confidential information, at least there are ethical rules designed to alleviate the damage.

iii. Over the past several years, confidentiality and privilege disclosures have increasingly appeared in the email signatures of attorneys. If social media usage among attorneys really is on the rise, perhaps it is time start including these disclosures in social media communications.

iv. Cloud computing brings similar confidentiality concerns.

   a. With cloud computing, users access software and data off an Internet server instead of their local machines. Google

Documents is one of the more popular examples of cloud computing.

b. In terms of confidentiality, cloud computing means storing data on third-party servers over the Internet, not on local disks. A breach in security could then result in the irreparable disclosure of confidential information.

c. Importantly, outsourcing is not new to the legal profession. It is, however, imperative that lawyers minimize risk by not comingling data and choosing a reputable provider. Kevin F. Brady, *Cloud Computing – Panacea or Ethical "Black Hole" for Lawyers*, THE BENCHER, Nov.-Dec. 2010, at 17, *available at* http://www.scribd.com/doc/40571128/The-Bencher-Nov-Dec-2010-Social-Media-and-the-Law.

B. Researching or Contacting the Opposing Party

i. Researching the opposing party through social media may also violate ethical rules against deceitful or dishonest conduct.

a. This is not to suggest that an attorney should not utilize social media. Indeed, in some cases, a colorful argument can be made that the duties of diligence and competent representation may require social media. Margaret Dibianca, *Complex Ethical Issues of Social Media*, THE BENCHER, Nov.-Dec. 2010, at 9, *available at* http://www.scribd.com/doc/40571128/The-Bencher-Nov-Dec-2010-Social-Media-and-the-Law.

ii. For example, can a lawyer instruct a third-party to befriend a witness without that witness knowing the relationship of the third-party to the lawyer?

a. No, the Philadelphia bar recently found that the omission of such a highly material fact is dishonest under Rule 8.4. Phila. Bar Ass'n Prof'l Guidance Comm., Op. 2009-02 (2009), *available at* http://www.philadelphiabar.org/WebObjects/PBAReadOnly.woa/Contents/WebServerResources/CMSResources/Opinion_2009-2.pdf.

iii. Still, there are many uncharted ethical issues presented by social media.

a. Following up on the Philadelphia Bar opinion, some commentators wondered about other potentially dishonest uses of social media.

1. For example, can an attorney change their location or regional network on Facebook to gain access to another party's profile? One informal study found no consensus among lawyers, students, and other legal professionals. Leora Maccabee, *When lawyers spy through Facebook: the ethics of 'regional network' changes*, THE LAWYERIST, Jul. 8, 2009, http://lawyerist.com.

iv. When researching opposing parties over social media, the best advice is to keep it safe: use a profile reflecting your true identity and avoid changing any settings before researching that party.

IV. ADDRESSING THE SPECIAL ISSUES POSED BY SOCIAL MEDIA USAGE IN THE CONTEXT OF TRIAL

A. Utilizing Social Media for Jury Selection

i. Social media can be just as valuable in researching jurors as in researching the opposing party.

ii. Recently, a New Jersey appellate court upheld the use of laptops in the courtroom to research potential jurors during voir dire. Charles Toutant, *N.J. Court OKs Googling Jurors During Voir Dire*, LAW.COM, Sept. 10, 2010, *available at* http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202471933994.

iii. That said, be mindful of your ethical obligations. Improper communications with the jury is always a concern. Even "friending" a juror will likely be going too far.

B. Juries and Social Media

i. Examples of juror misconduct involving social media abound:

a. Jurors have improperly researched cases. *E.g.,* John Schwartz, *As Jurors Turn to Web, Mistrials Are Popping Up*, N.Y. TIMES, Mar. 14, 2010, http://www.nytimes.com/2009/03/18/us/18juries.html.

b. Jurors have improperly commented on cases. *See* Noeleen G. Walder, *Jurors' Online Activity Poses Challenges for Bench*,

LAW.COM, Mar. 5, 2010, *available at* http://www.law.com/jsp/article.jsp?id=1202445530564.

c. Jurors have "friended" other people in the courtroom. *E.g.,* Robert Little, Juror contact in '06 with Dixon, witness could cause mistrial, Balt. Sun, Dec. 5, 2009, http://www.baltimoresun.com/news/maryland/bal-md.juror05dec05,0,2389300.story.

ii. So how do you prevent this? Attorney Harry A. Valetk has a few suggestions:

> *Probe jurors during voir dire on Facebook and Twitter use. Establish frequency of use and a juror's ability to refrain from using social networking tools during trial.*
>
> *Monitor juror Facebook and Twitter activity during trial. Tools like Social Mention allow you to search blogs, microblogs, networks, videos and much more. This engine also allows you to create alerts for your search terms that you can have e-mailed to you daily.*
>
> *Ask the trial judge to remind jurors that they may come forward to report a fellow juror's misconduct. The judge should also remind jurors about the fines and other potential consequences for failing to follow the court's ban on communicating with others about the case.*
>
> *Warn jurors before and after every jury break about the court's ban on communicating with others about the case during trial, including the use of Facebook, Twitter and other web-based tools.*
>
> *Explain the logic behind the presumption of juror prejudice. Jurors today may be more receptive to complying with court-ordered bans on communicating with others during trial if they understand the logic behind the ban.*
>
> Harry A. Valetk, *Facebooking in Court: Coping with Socially Networked Jurors*, LAW.COM, Oct. 11, 2010, *available at* http://www.law.com/jsp/article.jsp?id=1202473157232.

C. Judges and Social Media

i. Social networking in itself is not a violation of judicial ethics.

a. Social networking is analyzed under the "same rules that govern a judge's ability to socialize and communicate in person, on paper and over the telephone." Cal. Judges Assoc. Comm. on Judicial Ethics, Op. 66 (2010), at 3, *available at* http://www.caljudges.org/files/pdf/Opinion%2066FinalShort.pdf.

1. These rules do not require judges to avoid all communications with the public. Indeed, the commentary

to Canon 4A expressly states that "a judge should not become isolated from the community in which the judge lives." *Id*.

ii. At what point, then, does social networking become unethical?

a. Canon 4A requires that a judge's extrajudicial activities be conducted so that they do not (1) cast reasonable doubt on the judge's capacity to act impartially, (2) demean the judicial office, or (3) interfere with the proper performance of judicial duties.

b. Social media thus provides another medium through which judges run the risk of clear ethical violations.

1. Judges should not use social networking to comment on pending cases.

2. Additionally, they should also avoid posting anything on their profiles that may give the suggestion of bias or prejudice.

3. Similarly, their profiles should not demean the judiciary.

a) "While it may be acceptable for a college student to post photographs of himself or herself engaged in a drunken revelry, it is not appropriate for a judge to do so." *Id*. at 5.

4. Lastly, endorsing or opposing political candidates is just as impermissible online as it is in person.

iii. Can judges include lawyers in their social networks?

a. Usually, judges are allowed to befriend attorneys, even ones that practice in their jurisdiction. *See* Andrew Sternlight, *Judges on Facebook*, EN BANC, Apr. 5, 2010, http://lacbablog.typepad.com.

1. Under Canon 4A, judges are allowed and even encouraged to join bar associations and other legal organizations to promote civility and professionalism.

2. Associating with lawyers over social media is thus permissible to promote the same ends.

b. Florida is a notable exception to this trend.

1. While acknowledging that the term "friend" carries a different meaning with social media, the Florida Judicial

Ethics Advisory Committee found that social networking may violate the judiciary's obligation to avoid even the appearance of impropriety. Fla. Judicial Ethics Advisory Comm., Op. 2009-20 (2009), *available at* http://www.jud6.org/LegalCommunity/LegalPractice/opinions/jeacopinions/2009/2009-20.html.

2. Notably, however, this position received some criticism for not realizing that social networking is now a part of modern life.

   a) "Judges do not 'drop out of society when they become judges. . . . The people who were their friends before they went on the bench remained their friends, and many of them were lawyers.'" John Schwartz, *For Judges on Facebook, Friendship Has Limits*, N.Y. TIMES, Dec. 10, 2009, http://www.nytimes.com/2009/12/11/us/11judges.html.

   b) Some judges may also distinguish between Facebook friends and an intimate circle of close friends.

c. While judges generally can befriend other attorneys, at least one Judges Association found that they cannot remain friends with lawyers who have cases pending before them in order to avoid the appearance of impropriety.

   1. Specifically, the California Judges Association recommends de-friending that attorney. Cal. Judges Assoc. Comm. on Judicial Ethics, *supra*, at 10-11.

ADDITIONAL READING

Awsumb, Shannon, *Social Networking Sites: The Next E-Discovery Frontier*, 66-NOV BENCH & B. MINN. 22.

Ballon, Ian C., E-COMMERCE & INTERNET LAW: A LEGAL TREATISE WITH FORMS (2010).

Bennett, Steven C., *Ethics of Lawyer Social Networking*, 73 ALB. L. REV. 113 (2009).

Blank, Aaron, *On the Precipe of E-Discovery: Can Litigants Obtain Employee Social Networking Web Site Information Through Employers?*, 18 COMMLAW CONSPECTUS 487 (2010).

Booker, Matthew R., *Informal Discovery: Google, Facebook and Beyond* (May 20, 2010), http://www.heylroyster.com/_data/files/Seminar_2010/2010_CP_F_MRB.pdf.

BOW-TIE LAW BLOG, http://bowtielaw.wordpress.com/.

Compliance Building, *Social Media Policies Database*, http://www.compliancebuilding.com/about/publications/social-media-policies/ (last visited Jan. 19, 2011).

Crist, Maria Perez, *Preserving the Duty to Preserve: The Increasing Vulnerability of Electronic Information*, 58 S.C. L. REV. 7, 8 (2006).

Gilliland, Joshua C. & Thomas J. Kelley, *Modern Issues in E-Discovery*, 42 CREIGHTON L. REV. 505 (2009).

LaBreche, Beth, *Navigating Social Media's Wild West*, MINN. BUS., Dec. 1, 2010, *available at* http://www.minnesotabusiness.com/navigating-social-media%E2%80%99s-wild-west.

Lauby, Sharlyn, *10 Must-Haves for Your Social Media Policy*, MASHABLE, (Jun. 2, 2009) http://mashable.com/2009/06/02/social-media-policy-musts/.

Legal Talk Network, *ESI Report*, http://legaltalknetwork.com/podcasts/esi-report/.

Nelson, Sharon et al., *The Legal Implications of Social Networking*, 22 REGENT U. L. REV. 1 (2010).

O'Brien, Angela, *Are Attorneys and Judges One Tweet, Blog or Friend Request Away from Facing A Disciplinary Committee?*, 11 LOY. J. PUB. INT. L. 511 (2010).

Pepe, Louis R. & Jared Cohane, *Document Retention, Electronic Discovery, E-Discovery Cost Allocation and Spoliation of Evidence: The Four Horsemen of the Apocalypse in Litigation Today*, 80 CONN. B.J. 331 (2006).

Raysman, Richard & Peter Brown, *Discoverability and Ethics of Social Media Data*, LAW.COM, Dec. 15, 2010, *available at* http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202476191700.

Ross, Joshua-Michele, *A Corporate Guide For Social Media*, FORBES, Jun. 30, 2009, *available at* http://www.forbes.com/2009/06/30/social-media-guidelines-intelligent-technology-oreilly.html.

Williams, Meredith L., *eDiscovery & Social Media*, NAT'L L. REV., Nov. 23, 2010, *available at* http://www.natlawreview.com/article/ediscovery-social-media.

Wilson, John S., *Myspace, Your Space, or Our Space? New Frontiers in Electronic Evidence*, 86 OR. L. REV. 1201, 1202 (2007).

NOTES