

# PANNING FOR GOLD: Social Networking's Impact on E-Discovery

by Hon. Richard J. Sankovitz, Jay E. Grenig & William C. Gleisner III

What's new is old again. Not long ago, social networking – on platforms such as Facebook, MySpace, Twitter, YouTube, and the like – seemed exotic and avant-garde. But no longer. In 2011, social networking is commonplace.

In fact, social networking has so permeated the culture that competent lawyers cannot afford to ignore its customs and the trove of discoverable information to be found where it takes place. Just as lawyers last century needed to master the intricacies of email, so too this century with social networking. As one commentator puts it: "It should now be a matter of professional competence for attorneys to take the time to investigate social networking sites. You must pan for gold where the vein lies – and today, the mother lode is often online."<sup>1</sup>

This article summarizes practical recommendations and recent legal developments concerning:

- Helping clients understand how bad social networking habits can undermine their cases;
- Using commonly available resources to mine social networking sites (SNS) for discoverable information;
- Whether users of SNS have any right to shield what they post from discovery; and



Sankovitz



Grenig



Gleisner

Richard J. Sankovitz, Harvard 1983, is a Milwaukee County circuit court judge and teaches in the field of electronic discovery, presenting a program entitled "Electronic Discovery: New Wine in Old Bottles." He

seeks to reassure judges and lawyers that they need not be specialists or technicians to master these new tools.

Jay E. Grenig, California-Hastings 1971, is a professor of law at Marquette University Law School. He is a member of the Wisconsin Judicial Council and reporter for the Local Rules Committee of the U.S. District Court for the Eastern District of Wisconsin. He is coauthor of *eDiscovery & Digital Evidence*, *Electronic Discovery and Records Management Guide* and *Wisconsin Practice Series: Civil Discovery* and former managing editor of *Electronic Discovery and Records Management Quarterly*.

William C. Gleisner III, Marquette 1974, has an extensive background in state and federal litigation and focuses on the technical and legal aspects of obtaining, organizing, and managing electronic evidence. He provides computerized litigation support and "of counsel" assistance to law firms nationwide, helping them to plan, formulate, and execute e-discovery strategy. With Prof. Grenig, he is coauthor of *eDiscovery & Digital Evidence* and was a Summation-certified trainer for nearly 10 years. He thanks his associate, Matthew W. Surridge, for his research and drafting assistance.

- Whether users of SNS may be held liable for the defamatory content of their posts.

### The Ubiquity of Social Networking

It is commonplace for people to publish information about themselves, their activities, their histories, and their opinions on a variety of SNS platforms, including Facebook, MySpace, Twitter, and YouTube, not to mention on blogs, chatrooms, and so on. Seventy-five percent of people ages 18 to 24 have a profile on online social networks. One-third of adults ages 35 to 44 are active on online social networks, and nearly 20 percent of people ages 45 to 54 have profiles on a social network.<sup>2</sup>

### Cautions for Clients and Prospective Jurors

**The problem.** People who use social networks might not consider that the information they post about themselves can be used against them or the organizations for which they work. In today's wired world, litigants – adverse parties

and clients alike – may be in the habit of regularly posting experiences and opinions on SNS. They create videos and post them to YouTube, or they comment on videos created by others. They publish blogs and comment on blogs published by others. They chat in chatrooms. They create their own Web pages.<sup>3</sup> And other people may be posting unflattering or revealing information in cyberspace about the litigant without his or her knowledge. "In 2008, two weeks after being charged with drunk driving in an accident that seriously injured a woman, Joshua Lipton made the foolish decision to show up at a Halloween party in a prisoner costume with the label 'Jail Bird' on his orange jumpsuit. Someone posted the photo on Facebook and the prosecutor made effective use of the photo of this young man partying while his victim was recovering in a hospital. The judge called the photos 'depraved' and sentenced him to two years in prison."<sup>4</sup>

The problem is aggravated by clients and others who might not appreciate or candidly acknowledge

the degree to which their online disclosures may affect their cases, or how they might be sprung on them in a deposition or at trial.

Deleterious online habits also afflict potential jurors. It has become almost commonplace for jury trials to be derailed by jurors who go online to post their opinions or information about their deliberations or to research extraneous information about the case before them. "A misbehaving juror in Arkansas posted eight tweets during a trial which resulted in a \$12.6 million dollar verdict [against defendant Stoam]. During the trial, the juror's tweets included one that said, 'oh and nobody buy Stoam. It's ... bad mojo and they'll probably cease to exist, now that their wallet is 12m lighter.'"<sup>5</sup>

**Some solutions.** Lawyers advising any kind of client involved in civil or criminal litigation – plaintiffs, defendants, individuals, corporate agents – should put Internet usage at or near the top of the list of things to discuss with the client at the outset of the litigation. Clients must be advised not only of the potential for damaging their own cases (and the need for candor in discussing what damage already may have been done) but also of the opportunity to discover useful information about adverse parties.

An attorney might even consider including a disclaimer or additional provision in retainer agreements, such as the following:

- 1) The client (and, if a corporate client, all of its officers and employees) promises not to post any information on the Internet about the subject *matter of the representation without first consulting with counsel.*
- 2) The client (including corporate employees) must be completely candid concerning all past Internet postings.
- 3) If the client is not candid about the client's Internet postings, counsel cannot be responsible for the consequences and reserves the right to withdraw.
- 4) Counsel cannot predict what will be found on the Internet regard-

ing a client and so reserves the right to withdraw as counsel after conducting counsel's own search of the Web for information concerning the client.

### **Discovery of Information Published on an SNS**

The two most common legal issues that arise when a party attempts to discover another's SNS posts are 1) whether the person who posted the information has any right to shield posts from discovery; and 2) whether the operator of the SNS has any duty to respond to discovery requests.

**Courts generally do not consider SNS posts privileged.** In *Ledbetter v. Walmart Stores Inc.*,<sup>6</sup> Walmart sent subpoenas to Facebook, MySpace, and Meetup.com seeking information about the plaintiffs, who had filed an action seeking damages for physical and mental injuries and loss of consortium. The court denied the plaintiffs' motion for a protective order based on the physician-patient and spousal privileges, finding the plaintiffs had waived the privileges by filing the lawsuit. The court found the information was relevant and reasonably calculated to lead to the discovery of admissible evidence.

In *EEOC v. Simply Storage Management*,<sup>7</sup> a case involving multiple claims of sexual harassment, requests were made directly to the plaintiffs about postings they had made to Facebook and MySpace. The EEOC objected to the production of all SNS content (and to deposition inquiries on the same subjects) on the grounds that the requests were overbroad and unduly burdensome (because they improperly infringed on the claimants' privacy) and would harass and embarrass the claimants.<sup>8</sup>

The defendants claimed the nature of the injuries the claimants had alleged "implicates all their social communications (i.e., all their Facebook and MySpace content)."<sup>9</sup> The court first observed that the discovery of SNS "requires the application of basic dis-

## **Search Engines for Locating Posts on Social Networking Sites**

Hundreds of search engines are available on the Web, and more are coming online all the time. The following are some helpful resources for locating evidence on social networking sites.

- Top Ten Search Engines, [www.seoconsultants.com/search-engines](http://www.seoconsultants.com/search-engines)
- AltaVista, [www.altavista.com](http://www.altavista.com)
- Ask, [www.ask.com](http://www.ask.com)
- Bing, <http://www.bing.com>
- Cuil (billed as having the world's biggest index), [www.cuil.com](http://www.cuil.com)
- DuckDuckGo (eliminates clutter as it crawls), [www.duckduckgo.com](http://www.duckduckgo.com)
- Exalead (based in France, use to search European sources), [www.exalead.com/search](http://www.exalead.com/search)
- Factbites (answers in sentences using encyclopedias and other higher content sites), [www.factbites.com](http://www.factbites.com)
- Google, [www.google.com](http://www.google.com)
- Google for searching blogs, <http://blogsearch.google.com>
- Hakia (looks for meaning through semantic connections of words to concepts rather than relying on the standard keyword match), [www.hakia.com](http://www.hakia.com)
- Highbeam (searches approximately 80 million articles from archives of 6,500 newspapers, magazines, and more), [www.highbeam.com](http://www.highbeam.com)
- Kosmix (searches images, video, blogs, tweets), [www.kosmix.com](http://www.kosmix.com)
- Quintura (clusters results in a tag cloud that can be manipulated to alter the search), [www.quintura.com](http://www.quintura.com)
- Technorati (searches blogs), [www.technorati.com](http://www.technorati.com)
- SearchQuilt, [www.searchquilt.com](http://www.searchquilt.com)
- Yahoo, <http://search.yahoo.com>

### **Specialty search engines – for videos:**

- Bing, <http://www.bing.com/videos/browse>
- Google, <http://video.google.com>
- Yahoo Video, <http://video.search.yahoo.com>
- YouTube, [www.youtube.com](http://www.youtube.com)

### **Specialty search engines – for images:**

- Bing, <http://www.bing.com/images>
- Google, <http://images.google.com>
- Yahoo, <http://images.search.yahoo.com>

### **"Meta-search" engines (to search several engines at one time):**

- etools.ch (Swiss meta engine useful for searching European sites), <http://www.etools.ch>
- Fuzzfind (also searches social bookmarking sites), [www.fuzzfind.com](http://www.fuzzfind.com)
- iSeek, [www.iseek.com](http://www.iseek.com)
- MetaCrawler (simultaneously searches white pages, yellow pages, Ask, Bing, Google, Yahoo, and more), [www.metacrawler.com](http://www.metacrawler.com)
- Polymeta, [www.polymeta.com](http://www.polymeta.com)
- Yippy (searches images and Wikipedia), <http://search.yippy.com>
- Zuula, [www.zuula.com](http://www.zuula.com)

For more information about Web search tools, see Web Search Guide, [www.Web-searchguide.ca/index.html](http://www.Web-searchguide.ca/index.html); and Applied Discovery, [www.applieddiscovery.com](http://www.applieddiscovery.com).

## Social Networking, Jurors, and Jury Instructions

Jurors are online and networking, too, and the bad habits of some continue to make headlines, including:

- the juror in England who polled her Facebook friends to decide whether to vote guilty or not guilty;
- the juror in Arkansas who posted eight tweets during a trial, including one tweet denigrating the defendant, against which the jury had awarded a \$12.6 million verdict; and
- the juror in New York who, during deliberations, attempted to "friend" one of the witnesses.

### Wisconsin Jury Instructions

Wisconsin courts were among the first courts in the nation to address these concerns by alerting jurors about online pitfalls and explicitly instructing them to avoid the Internet during trial. In 2009, the Wisconsin Criminal Jury Instructions Committee modified its standard jury instruction on jury communications (Wis JI-Civ 50) to address specifically the potential for Internet abuse:

"... Do not consult dictionaries, computers, websites or other reference materials for additional information. Do not seek information regarding the public records of any party or witness in this case. Any information you obtain outside the courtroom could be misleading, inaccurate, or incomplete. Relying on this information is unfair because the parties would not have the opportunity to refute, explain, or correct it."

"Do not communicate with anyone about this trial or your experience as a juror while you are serving on this jury. Do not use a computer, cell phone or other electronic device with communication capabilities to share any information about this case. For example, do not communicate by blog, e-mail, text message, Twitter, Facebook, other social networking sites, or in any other way, on or off the computer."

### To Learn More ...

State Bar of Wisconsin Pinnacle™ will present the live webcast "**Amended Rules of Discovery**," on Thursday, March 31, 12 – 1:30 p.m. In July 2010, the Wisconsin Supreme Court adopted new discovery rules recognizing the influx of electronic discovery and regulating how e-discovery is practiced. The court further amended the rules in November to require a mandatory pre-discovery conference before engaging in e-discovery. The rules became effective Jan. 1, 2011.

The webinar will:

- provide a summary of the discovery rules;
- discuss the impact of the new rules on lawyers' discovery duties; and
- relate the current status of amendments before the Wisconsin Judicial Council's Evidence & Civil Procedure Committee.

Credits: 1.5 CLE credits. Tuition: \$95 members; \$115 nonmembers; \$0 Ultimate Pass holders. Register: (800) 728-7788; (608) 257-3838 Madison area.

### See also

- "What You Need to Know: New Electronic Discovery Rules," by Hon. Richard J. Sankovitz, Jay E. Grenig & William C. Gleisner III, July 2010 *Wisconsin Lawyer*

covery principles in a novel context."<sup>10</sup>

The defendants in *Simply Storage* cited one case in which a court required production of the plaintiff's entire SNS profile.<sup>11</sup> The court also discussed the case law it was able to find dealing with the issue of SNS requests directed to a party. According to the court, "[a] person's expectation and intent that her communications be maintained as private is not a legitimate basis for shielding those communications from discovery. ... *Murphy v. Perger*, 2007 WL 5354848 (S. Cal. 2007), ... held that a requesting party is not entitled to access all non-relevant material on a site, but that merely [blocking a] profile from public access does not prevent discovery either. ... As in other cases when privacy or confidentiality concerns have been raised, those interests can be addressed by an appropriate protective order, like the one already entered in this case."<sup>12</sup>

The court in *Simply Storage* determined that the appropriate scope of relevance of an SNS request to a plaintiff was "any profiles, postings or messages (including status updates, wall comments, causes joined, groups joined, activity streams, blog entries) ... that reveal, refer or relate to any emotion, feeling or mental state...."<sup>13</sup> Overall, the *Simply Storage* court was unsympathetic to the privacy concerns asserted by the plaintiffs. According to the court, "[t]he court agrees with the EEOC that broad discovery of the claimants' SNS could reveal private information that may embarrass them.... Further, the court finds that this concern is outweighed by the fact that the production here would be of information that the claimants have already shared with at least one other person through private messages or a larger number of people through postings."<sup>14</sup>

Another case in which postings to an SNS were deemed public, not private, was *Moreno v. Hanford Sentinel Inc.*<sup>15</sup> A student and her family sued a principal and a school district for invasion of privacy and intentional

infliction of emotional distress because of the re-publication of a journal entry from a social networking website. The student had published an ode on her MySpace page that contained derogatory remarks about her hometown. The ode was taken down after six days but the school principal was responsible for getting it published in the local newspaper, which led to death threats and other unfortunate acts. The *Moreno* court held that once the ode had been published on MySpace it was no longer private or entitled to an expectation of privacy. According to the court, “[t]he student’s] affirmative act made her article available to any person with a computer and thus opened it to the public eye. Under these circumstances, no reasonable person would have had an expectation of privacy regarding the published material.... [T]he fact that [the student] expected a limited audience does not change [this fact]. By posting the article on myspace.com, [the student] opened the article to the public at large.”<sup>16</sup>

However, not every court will permit the discovery of information stored on online social networks, at least if the user makes definitive efforts to protect the privacy of the information rather than broadcasting it generally. To the extent that a posting to an SNS resembles a private communication that is otherwise privileged, such a posting may be protected from discovery under the federal Stored Communications Act (SCA).<sup>17</sup>

In *Crispin v. Christian Audigier Inc.*,<sup>18</sup> several defendants sought to obtain access to the SNS postings of a plaintiff by serving subpoenas directly on the SNS operators. The plaintiff attempted to quash the subpoenas by asserting rights conferred on the SNS operators by the SCA.

The *Crispin* court ruled that the SCA protects electronic communications that are configured to be private.<sup>19</sup> Thus, some Internet communications are protected and some are not:

“With respect to Webmail and private messaging, the court is satisfied that those forms of communications media are inherently private such that stored messages are not readily accessible to the general public. ... With respect to the subpoenas seeking Facebook wall postings and MySpace comments, however, ... it appears... that a review of plaintiff’s privacy settings would definitively settle the question, [and so] the court does not reverse Judge McDermott’s order, but vacates it and remands so that Judge McDermott can direct the parties to develop a fuller evidentiary record regarding plaintiff’s privacy settings.”<sup>20</sup>

### SNS and Corporate Governance

Corporate record management administrators face unique and difficult challenges because of SNS. Some commentators have described social networking as an “e-discovery and

records management nightmare.”<sup>21</sup> According to these commentators:

“Is a tweet done on firm resources a ‘record’ for purposes of retention requirements and ESI preservation/production? ... Much of this remains unsettled ground. If you find that scary, you’re not alone. ... Twitter, blogs, and social networks have given almost everyone a Goliath-sized headache. Whether you are thinking in terms of your own law firm or your clients, you must now consider these new technologies.”<sup>22</sup>

One record management administrator has described tweets as “being no different from letters, e-mail, or text messages: they can be damaging and discoverable, which could be especially problematic for companies that are required to preserve electronic records, such as the securities industry and federal contractors.”<sup>23</sup>

Besides impeding record  
(continued on page 61)

## ONLAW Trial Technologies, LLC

Courtroom Technology • eDiscovery • Computer Forensics

- Computer Forensics
- Hard Drive Imaging and Forensic Analysis
- Data Acquisition and Preservation
- eDiscovery Consulting
- Meet and Confer Consulting
- Special Master/Referee
- Third Party Neutral

Expert Witness Services by:  
Bruce A. Olson, J.D., CCE  
ISFCE Certified Computer Examiner

[WWW.ONLAWTEC.COM](http://WWW.ONLAWTEC.COM)



920.750.8083

(from page 17)

management, social networking could complicate the business world in other ways. Employers already face a number of difficulties arising from employee misuse of work computers.<sup>24</sup> Access to SNS websites or blogs actually may give rise to employee privacy rights that one would not expect to exist during the use of company computers.<sup>25</sup>

Employees, however, need to realize that emails they send or postings they make to an SNS concerning an employer can come back to haunt them.<sup>26</sup> Problematic situations include those associated with trade-secret theft via email or social networking posts<sup>27</sup> and an employee making disparaging remarks about an employer on what the employee thought was a secure network.<sup>28</sup>

### Legal Implications for Badmouthing Others on an SNS

The spontaneity and immediacy of SNS postings tend to make them frank, sometimes too much so. Frank comments have the potential to do real damage to a client or a client's business.

But before considering legal action for defamation or business disparagement, lawyers need to reflect on the fact that there is a growing trend to treat blogs and social networks as news and thus protected, as are traditional news outlets, by the First Amendment and laws that shield press informants. In *O'Grady v. Superior Court*,<sup>29</sup> the court was confronted with a charge by Apple Computer that certain unknown persons had caused the publication of trade secrets. Apple issued subpoenas to the publishers of the websites on which the information was published. The *O'Grady* court concluded, "We decline the implicit invitation to embroil ourselves in questions of what constitutes 'legitimate journalism[.]' The shield law is intended to protect the gathering and dissemination of news, and that is what petitioners did

here. We can think of no workable test or principle that would distinguish 'legitimate' from 'illegitimate' news. Any attempt by courts to draw such a distinction would imperil a fundamental purpose of the First Amendment."<sup>30</sup>

### Searching for and Using SNS Data

**Searches.** What if a client long ago created a Web page that could prove embarrassing today? Even if the Web page was taken down years ago, a forensic investigator can use tools such as the "Wayback Machine"<sup>31</sup> to retrieve that Web page. According to the creator of the Wayback Machine, it can be used to "[b]rowse through over 150 billion Web pages archived from 1996 to a few months ago."<sup>32</sup> With the Wayback Machine, a forensic investigator can retrieve copies of a website even though it was taken down many years ago and the server where it had been located has ceased to operate.

In a recent legal malpractice case, a defendant firm claimed it had absolutely no knowledge of a particular specialty and nothing on its Web page or in ordinary searches of the Web indicated anything to the contrary. Representatives of the defendant firm swore under oath that the firm never had any expertise in that specialty. However, using the Wayback Machine, the plaintiff's attorney discovered a Web page published by the defendant firm six years earlier that was devoted entirely to that specialty, including statements about how much knowledge the defendant firm had concerning that specialty and maintaining an "ask the expert feature" about the specialty. This Web page revealed that many of the firm members who were now denying any knowledge of the specialty had claimed extensive knowledge six years earlier. In fact, using the Wayback Machine led to the discovery that the defendant firm had even published a client newsletter concerning the specialty.

All litigators should become familiar with the wide variety of search

## Disputes Happen ... It's How You *Resolve Them* That Matters



**Jim Cole**  
**Mediation & Arbitration Services**

Certified Mediator –  
The Franklin Pierce Law Center

Elected – Board of Directors  
State Bar ADR Section and  
Wisconsin Mediators Association

Member – American Arbitration Association  
Panel of Mediators & Arbitrators

Member – ADR Systems of  
America Panel of Neutrals

Member – Resolute Systems Panel of  
Mediators & Arbitrators

#### DESIGNATED:

The Best Lawyers in America  
Alternative Dispute Resolution (2005 – )

Chambers USA

Wisconsin Super Lawyers

Dane County's Top Alternative Dispute  
Resolution Attorneys (2004 – )

#### TESTIMONIAL:

"Jim brings to the table the insight from years of experience in litigation, great people skills, and a true sense of fairness. He treats parties with respect and finds creative ways to resolve complex disputes. I highly recommend Jim as a mediator."

~ Philip J. Bradbury, Melli, Walker,  
Pease & Ruhly, S.C. – Madison

**Cole** Dispute Resolution

33 E. Main St., Suite 900 | Madison, WI 53703  
Phone: (608) 283-2403  
Email: [jim@coleadr.com](mailto:jim@coleadr.com)

[www.coleadr.com](http://www.coleadr.com)

engines that are available for conducting Web searches. The accompanying sidebar includes several search engines and their Web addresses. While some of the listed websites charge an access fee, they can be used to supplement private investigators' findings and can help obtain far greater information about an individual or a business than one might find using Google, for example. Highbeam will provide access to newspaper and magazine archives, which often can point to interesting discovery leads. It is not easy to search for blogs or blog entries using basic search engines. Thus, for such a chore, one should consider using advanced search engines like Google's blogsearch or Kosmix. Sometimes it is useful to use a search methodology that is not based on keywords. For example, a person can use Hakia to search using

semantic connections. Case law or white papers dealing with e-discovery often will be important, and these may be found using the Lexis Applied Discovery site.

Litigators also should become familiar with Web crawlers.<sup>33</sup> A Web crawler is an Internet search device that continuously and automatically searches the Web for sites that address or mention topics the user specifies, for example, news items on a subject that interests the user. For example, Google "news alerts" help keep computer users apprised of news developments about particular issues. Litigators also might consider creating searchbots. "A Searchbot is your own personal search robot that continuously searches the Internet trying to find all the best Websites it can on your behalf. When you build a Searchbot you give it a personality and then

program its search circuits with all the things you want to find. You can search for Websites based on factual information like tags and locations.... You can even ask your Searchbot a question and it will talk to other Searchbots to find you an answer."<sup>34</sup>

**Admissibility of information obtained from an SNS.** There is a difference between asserting SNS posts are discoverable and defending their admissibility in court. Milwaukee County Family Court Judge Michael J. Dwyer has stated that SNS posts are often irrelevant to the legal crux of a case.<sup>35</sup> Judge Dwyer also has stated that an SNS post will be considered inadmissible hearsay if one cannot authenticate the source of the post. According to Judge Dwyer, "If a party denies making the post, it's not admissible."<sup>36</sup> Milwaukee divorce attorney Richard J. Podell has stated that SNS "posts he's provided in cases were allowed as a rebuttal where a spouse denies an extramarital affair."<sup>37</sup> Regardless of their admissibility at trial, the fact is that SNS posts clearly are discoverable, may lead to other discoverable evidence, and may well present serious challenges for counsel before and during trial, especially if used as impeachment.

There is a world of difference in using SNS posts in the context of a civil dispute versus in a criminal dispute, but one obvious concern is whether an attempt by law enforcement to obtain communications posted on an SNS infringes the user's rights under the Fourth Amendment. In *United States v. Warshak*,<sup>38</sup> the court ruled that a suspect may have an expectation of privacy in email communications that bars the production of the information without a warrant. The court explained,

"If we accept that an email is analogous to a letter or a phone call, it is manifest that agents of the government cannot compel a commercial ISP to turn over the contents of an email without triggering the Fourth Amendment.... [T]he ISP is the functional equivalent of a post office or a tele-

If eDiscovery was as easy as pressing a button, you wouldn't need our help.

Data Preservation  
Forensic Analysis  
eDiscovery  
Expert Testimony  
Pre Discovery Planning

\*Find

Digital Intelligence  
Mastering the science of digital forensics

tel: 262-782-3332 or 866-344-4683

phone company.... [I]f government agents compel an ISP to surrender the contents of a subscriber's emails, those agents have thereby conducted a Fourth Amendment search, which necessitates compliance with the warrant requirement absent some exception.<sup>39</sup>

## Conclusion

In the social networking era, attorneys face an entirely new challenge that directly affects client representation. It is essential that attorneys and judges keep up to date with these developments. The law is just beginning to evolve in response to SNS data and its use, but the average lawyer cannot afford to ignore the very real potential for legal good and harm that may result from social networking.

## Endnotes

<sup>1</sup>Sharon Nelson et al., *The Legal Implications of Social Networking*, 22 Regent U. L. Rev. 1, 14 (2010).

<sup>2</sup>Karen Barth Menzies & Wesley K. Polischuk, *Is Your Client an Online Social Butterfly?* Trial, Oct. 2010, at 23, 24.

<sup>3</sup>Online resources that can be used to create and host Web pages are emerging at a breathtaking pace. See [www.intuit.com/Website-building-software](http://www.intuit.com/Website-building-software) or <http://mediatemple.net>.

<sup>4</sup>Nelson, *supra* note 1, at 12.

<sup>5</sup>*Id.* at 4.

<sup>6</sup>2009 WL 1067018 (D. Colo. Apr. 21, 2009).

<sup>7</sup>EEOC v. Simply Storage Mgmt., 2010 U.S. Dist. Lexis 52766 (S.D. Ind. May 11, 2010).

<sup>8</sup>*Id.* at \*4.

<sup>9</sup>*Id.* at \*7.

<sup>10</sup>*Id.* at \*8.

<sup>11</sup>Bass v. Miss Porter's School, 2009 WL 3724968 (D. Conn. Oct. 27, 2009).

<sup>12</sup>*Id.* at 8-9.

<sup>13</sup>*Id.* at 14-15.

<sup>14</sup>*Id.* at 18.

<sup>15</sup>172 Cal. App. 4th 1125, 91 Cal. Rptr. 3d 858 (Cal. App. 2009).

<sup>16</sup>*Id.* at 1130. *See also Commonwealth v. Proetto*, 771 A.2d 823, 831-32 (Pa. Super Ct. 2001).

<sup>17</sup>18 U.S.C. §§ 2701-2712.

<sup>18</sup>717 F. Supp. 2d 965 (M.D. Cal. 2010).

<sup>19</sup>*Id.* at 989.

<sup>20</sup>*Id.* at 991.

<sup>21</sup>Nelson, *supra* note 1, at 15.

<sup>22</sup>*Id.* at 15-16.

<sup>23</sup>*Id.* at 16. For an excellent general discussion of the duty to preserve, see Maria Perez Crist. *Preserving the Duty to Preserve: The Increasing Vulnerability of Electronic Information*, 58

S.C. L. Rev. 7 (2006).

<sup>24</sup>Louis J. Papa & Stuart L. Bass, *How Employers Can Protect Themselves from Liability for Employees' Misuse of Computer, Internet and E-mail Systems in the Workplace*, 10 B.U. J. Sci. & Tech. L. 110 (2004).

<sup>25</sup>See *Stengart v. Loving Care Agency Inc.*, 973 A.2d 330 (N.J. App. 2009) (holding employee's emails exchanged with her attorney through her personal, password-protected, Web-based email account were protected by attorney-client privilege).

<sup>26</sup>See Joshua C. Gilliland & Thomas J. Kelley, *Modern Issues in e-Discovery*, 42 Creighton L. Rev. 505, 518-21 (2009).

<sup>27</sup>See, e.g., *Rinkus Consulting Group Inc. v. Cammarata*, 688 F. Supp. 2d 598 (S.D. Tex. 2010) ("Rinkus argues that the September 30, 2006 email Bell forwarded to himself is evidence of trade secret misappropriation. At a discovery hearing held on September 2, 2009, this court allowed Rinkus to subpoena Google, an email provider, to obtain emails Bell sent and received." *Id.* at 626).

<sup>28</sup>See *Konop v. Hawaiian Airlines*, 302 F.3d 868 (9th Cir. 2002). In *Konop*, a pilot sued the airline, his employer, alleging that the airline had viewed his secure website, on which he posted bulletins critical of the airline, its officers, and the incumbent union,

without authorization. Two other pilots who had permission to access the website allowed an airline officer to use their names to establish accounts and passwords and access the website. *Id.* at 872. Cf. *Intel Corp. v. Hamidi*, 30 Cal. 4th 1342 (Cal. Sup. Ct. 2003) (company sued former employee for trespass because he sought to send disparaging emails to current employees).

<sup>29</sup>139 Cal. App. 4th 1423, 44 Cal. App. 6 (Cal. App. 2006).

<sup>30</sup>*Id.* at 1457.

<sup>31</sup>Wayback Machine, [www.archive.org/web/web.php](http://www.archive.org/web/web.php). Other archive sites include the Biblioteca Alexandrina, [www.bibalex.org/Home/Default\\_EN.aspx](http://www.bibalex.org/Home/Default_EN.aspx); and the Library of Congress National Digital Library Program, <http://memory.loc.gov/ammem/dli2/html/lcdlp.html>. See [http://en.wikipedia.org/wiki/Internet\\_Archive](http://en.wikipedia.org/wiki/Internet_Archive).

<sup>32</sup>[www.archive.org/web/web.php](http://www.archive.org/web/web.php).

<sup>33</sup>[http://en.wikipedia.org/wiki/Web\\_crawler](http://en.wikipedia.org/wiki/Web_crawler).

<sup>34</sup>[www.searchbots.net/about](http://www.searchbots.net/about).

<sup>35</sup>Jack Zemlicka, *High-Tech Hearsay?* 24 Wis. L. J. 1 (Daily Reporter Pub'g Co. Ed., Dec. 20, 2010)

<sup>36</sup>*Id.* at 7.

<sup>37</sup>*Id.*

<sup>38</sup>2010 WL 5071766 (6th Cir. Dec. 14, 2010).

<sup>39</sup>*Id.* at \*12. 

## STATE BAR LAWYER ASSISTANCE PROGRAMS



# Because life is hard.

# WisLAP

Wisconsin Lawyers Assistance Program

Confidential help 24/7 – (800) 543-2625



STATE BAR OF WISCONSIN

Your Practice. Our Purpose.™

LAP10-WLRD 1/11