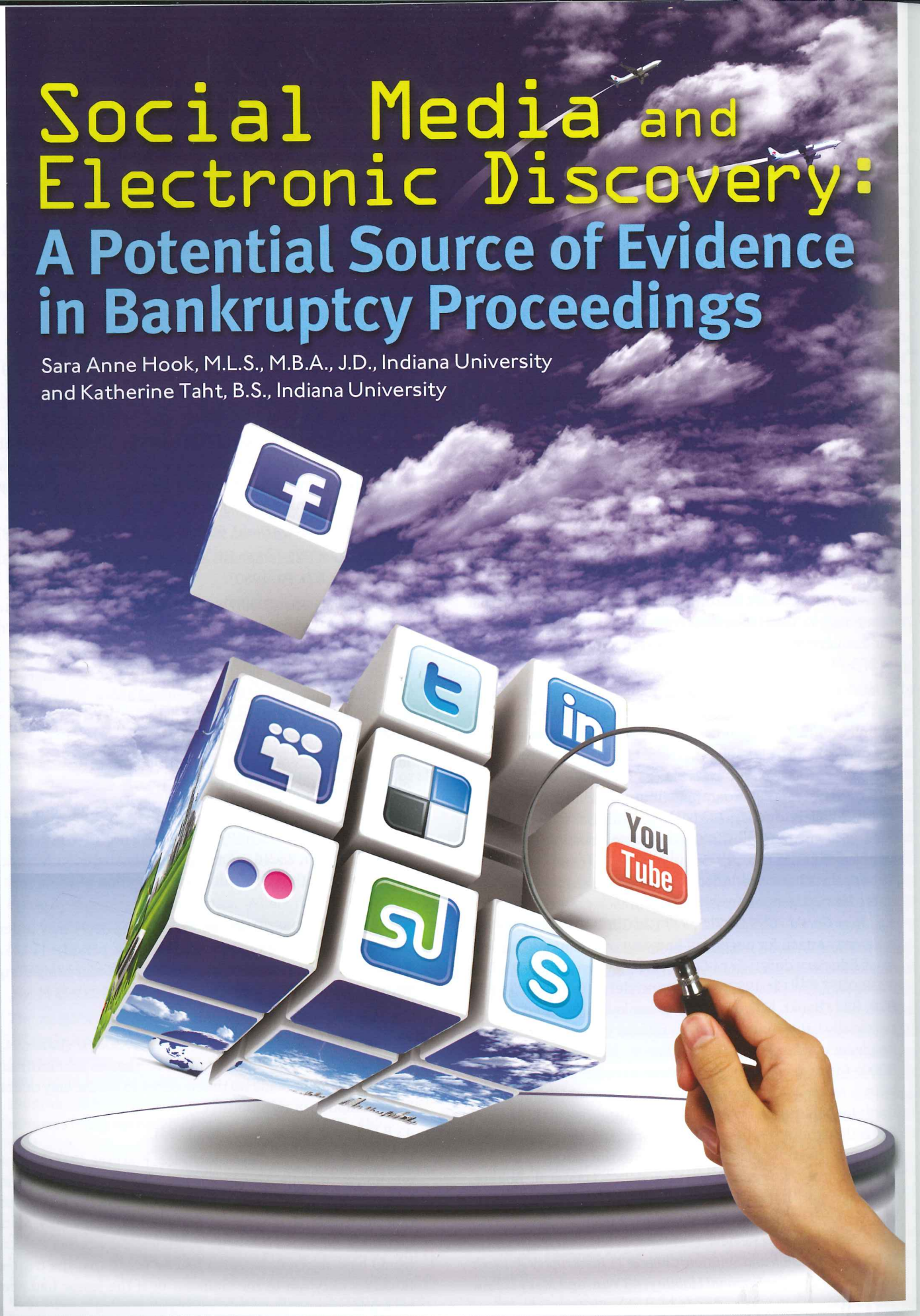
Social Media and Electronic Discovery: A Potential Source of Evidence in Bankruptcy Proceedings

Sara Anne Hook, M.L.S., M.B.A., J.D., Indiana University
and Katherine Taht, B.S., Indiana University



This article is the second in a series about electronic discovery in bankruptcy. The first article covered the basics of electronic discovery, including history, rules and resources. This article will discuss the discoverability of information found on social media sites such as Facebook, YouTube and LinkedIn, and how these sites can be rich sources of evidence for bankruptcy cases. Future articles will apply electronic discovery principles to bankruptcy law practice, review current technologies that can assist with electronic discovery before and during litigation and introduce examples where the failure to handle the electronic discovery process properly resulted in sanctions and the lessons that can be learned from these examples.

Introduction

The ways that people communicate have undergone a revolution in the last twenty years with the introduction of a variety of new information technologies. From email messages and websites in the mid-1990s, the first decade of the 21st century can be defined by the rise of social media and mobile devices. Information that might have been shared with only a few people through paper documents in the 20th century is now offered to millions, often without restrictions, through blogs, YouTube videos or profiles on LinkedIn, MySpace or Facebook. This ready access to information technology has provided a world that operates in a continuous 24-hour blur of instantaneous communication. The prevalence of social media is astonishing.[1] It is interesting to compare statistics from 2009 and 2010 to see how social media is being used by small business as an effective communication and marketing tool.[2] Many of these technologies also encourage communication that is more informal and spontaneous than when it sent via paper, resulting in people sharing their information in a way that may have unintended and unforeseen consequences. Moreover, this information, although deleted, may never be truly gone. In fact, social media technologies have proven to be rich sources of information in litigation, with most courts holding that the opposing party's need for access to the information outweighs any privacy concerns. Since most of the information on social media sites is fully discoverable as part of an electronic discovery process, attorneys, judges and trustees should be aware of the various kinds of social media that debtors and other parties might be using and how this information could be helpful in a bankruptcy proceeding. This includes, but is not limited to, revealing hidden assets or additional sources of income that were not declared as part of a bankruptcy filing.

What is Social Media?

The term *social media* refers to the "use of web-based and mobile technologies to turn communication into an interactive dialogue."[3] As defined in Wikipedia, "[s]ocial media can take on many different forms, including Internet forums, weblogs, social blogs, microblogging, wikis, podcasts, photographs or pictures, video, rating and social bookmarking."[4] Kaplan and Haenlein define social media as "a group of Internet-based applications that build on the ideological and technological foundations of Web 2.0, and that allow the creation and exchange of user-generated content."[5] According to Kaplan and Haenlein, there are six different types of social media: collaborative projects (e.g. Wikipedia), blogs and microblogs (e.g. Twitter), content communities (e.g. YouTube), social networking sites (e.g. Facebook), virtual game worlds (e.g. World of Warcraft), and virtual social worlds (e.g. Second Life).[6] One of the challenges of social media is determining the ownership of content, since content is generated through social media interactions by users through the site, but is hosted by a company. Some critics contend that the companies are making huge amount of money by using content that does not belong to them.[7] Of even more concern are the security and privacy of user-generated content and personal data that could be disclosed by these companies as well as provided to third-parties for a variety of purposes, not all of them admirable or welcomed by social media participants. Even several years ago, before social media was embraced by millions of users, scholars began to question the extent to which participation in social media would put a person's privacy at risk.[8]

This article will confine itself to two categories of social media, as defined by Kaplan and Haenlein: content communities (e.g. YouTube) and social networking sites (e.g. Facebook, LinkedIn, MySpace). The first author has been involved in the virtual social world of Second Life as Chessie Carlberg, but uses a younger, thinner and more fashion-forward female avatar than she appears in real life. However, she could have just as easily chosen to pose as a male avatar or non-human creature. Since participation in virtual worlds involves the freedom to select a persona that is quite different from reality, it may present less of a direct risk to privacy and security and be less useful as a source of information in bankruptcy proceedings than other categories of social media. However, the remaining categories of social media may also be worth exploring, especially if Twitter and other blog tools are mined for relevant information.

Privacy and Security of Social Media: Expectations versus Reality

In terms of using social networks, blogs, podcasts and other

About the Authors

Sara Anne Hook is Professor of Informatics, Indiana University School of Informatics, IUPUI, where she has developed a suite of online courses in the emerging field of legal informatics. She is also Adjunct Professor of Law in the Indiana University School of Law - Indianapolis, where she has taught courses in intellectual property law and professional responsibility, and Adjunct Professor of American Studies in the School of Liberal Arts. Previously, she was Associate Dean of the Faculties for IUPUI and Head Librarian at the Indiana University School of Dentistry. Professor Hook's research interests include intellectual property law, the emerging field of legal informatics, electronic discovery, legal technology, legal research techniques and issues related to privacy and security. She is a member of the American Intellectual Property Law Association (AIPLA), the Indiana State Bar Association, the International Legal Technology Association (ILTA) and the American Association for State and Local History (AASLH).

Katherine A. Taht is a graduate of Indiana University School of Informatics, 2011. She has received a Bachelor of Science in Media Arts Science, with an emphasis in animation and video production. As part of this degree, she took a course on electronic discovery. A previous student of fine art at Maine College of Art and San Antonio College, she has also completed a minor in art history at Herron School of Art and Design. Ms. Taht received a grant from the School of Informatics Undergraduate Research Opportunities Program in 2010 to support several research projects, with Professor Hook serving as her faculty mentor.

information from the Internet, there can be little to no expectation of privacy. A number of legal scholars have raised issues with the privacy of social media and the many ways that information gleaned from social media sites might be used in ways that participants had not anticipated, resulting in some unintended and perhaps unfavorable consequences.[9-16] Recent conferences and the professional literature have been filled with tales of attorneys canvassing all of these online repositories for information related to clients, opposing parties, other parties, opposing counsel, jury members, expert witnesses and lay witnesses, to name but a few. Most of this information has been freely and willingly provided by those who choose to participate in these kinds of information-sharing venues. Therefore, there are relatively few, if any, restrictions on finding and using this information in a legal case.

Some examples may be helpful. An employee blog could be used to share proprietary or trade secret information that should have been kept confidential. Parties in a divorce may find that they have provided less than flattering information about themselves through Facebook or YouTube. Young people eager to start their careers may find, to their dismay, that a potential employer was able to locate images of them partying, drinking and otherwise engaged in behavior that suggests someone who would be less than mature about the responsibilities of a new job or who would compromise their ethics and integrity when something more appealing or lucrative beckoned. Someone requesting reimbursement for a conference may find that he is denied support for his trip and that his professional credibility is damaged when photographs that he posted on Flickr indicate that he was at the beach on the same day he was supposedly giving his presentation at the conference. Brad Stephens, coach of the successful Butler University basketball program, noted that he now has to discuss social media with his players, something he did not have to do five years ago, and he cautions them to avoid the "stream of consciousness" sharing to these sites, which can result in damaged reputations and hurt feelings.[17] Heart-breaking situations are the result when a child commits suicide and his social media site reveals that he was bullied or when a roommate creates a video of a college student engaged in an intimate act and streams that content over the Internet. This may present the darker side of technology that was intended to bring people closer together and to make information more readily available.

Information from social media sites has even been allowed in criminal cases in several jurisdictions, although the admissibility of this information will still turn on meeting the other requirements for evidence, including authentication and relevancy. In the case of *Clark v. Indiana*, the trial court permitted the State to offer into evidence Clark's posting on the social networking site MySpace.[18] Clark was found guilty of murdering a two-year-old left in his care and he was sentenced to life in prison without parole. The Indiana Supreme Court held that the electronic evidence from MySpace was admissible and affirmed Clark's conviction and sentence. In an article entitled *The Pitfalls of an Internet Persona: Evidentiary and Privacy Concerns of Online Social Media*, Kate Mercer Lawson addresses this case in terms of the rules of evidence as they relate to electronically stored information, including relevance, hearsay, authentication and the "best evidence rule", as well as privacy considerations when dealing with online social media found in Constitutional and common law and in various federal regulations.[19]

Given the lack of privacy over what is shared through social media sites, blogs, podcasts and the web, and the fact that these technologies are such rich sources of information that may be damaging to a case or party, some attorneys are even insisting that, as a condition of representing a client, that client must agree to close and cease participation in his or her MySpace, Facebook, blog or other personal website. The intersection of employment law with the use of social networks by employees presents some special problems that were addressed in a presentation at the State Bar of Michigan Annual Meeting.[20] Moreover, the American Bar Association just issued a new ethics opinion related to an attorney's duty to protect the confidentiality of email communications with clients.[21] This opinion addresses some very common situations, including when a client uses a computer or other device or email provided by the employer to exchange information with the attorney, which creates the risk that a third-party may gain access to that information. A number of cases have held if a third party, such as an employer, does have access this information, this waives the attorney-client privilege, especially when the employer has made it clear through an Acceptable Use policy that it retains the right to monitor email and Internet use by its employees. Another common scenario is addressed in the formal opinion, where family members may be sharing email accounts or may otherwise allow access to each other's passwords.

In addition to the danger of putting confidential client information at risk, a number of ethical principles should be considered when a lawyer participates in or communicates through social media. Among the potential ethical breaches are gaining access to the Facebook or MySpace pages of witnesses or opposing parties to find information for cross-examination, which could run afoul of the rules related to contact with persons other than clients, or "friending" between judges and lawyers or between a debtor and bankruptcy trustee.[22] Professionals in other fields are being cautioned about the use of social media, particularly when dealing with confidential information about clients, customers and patients, as well as the importance of being accurate and professional, separating personal and professional content and using appropriate privacy settings that reflect the nature of what is being shared.[23]

People who participate in social networking and other information-sharing venues need to note that this information is readily available through relatively simple searches. Any information that a person chooses to make available to the public could also be gathered into, indexed and then distributed through a third-party database service or through data mining technologies. An email address presents a simple example of the power of computer "robots" and complex data mining tools and algorithms to sift and aggregate information. Some people now list their email address as sahook[at]iupui[dot]edu to avoid technology that pulls email addresses into a database that has been designed to look for and retrieve strings of characters with the @ and the "." in standard email address format. Most of this information will not be protected through system security features. Even if a person has set his or her privacy settings to be higher than the default, the information may still be vulnerable due to the extent

that this information has been shared with others and has been stored and made available by them.

Privacy and security of information on social media has moved from being a subject of scholarship in the legal community to being a concern among the general public. Bowing to pressure from a number of constituencies and after a number of high-profile incidents, the CEO of Facebook promised new privacy controls that would be more robust and easier to use.[24] Still, there may be aspects of social media user agreements that may put a user's privacy at risk and may offer little protection against others who want to access the information for a variety of purposes, including investigation and litigation.[25] Many of the provisions authorizing this use are found under the fairly benign heading of "Some other things you need to know".[26] Additional information for users is found on the Facebook Security page.[27] Privacy and security are not so simple, as demonstrated by two doctoral students at Indiana University.[28] As reported in the article, the students discovered a security vulnerability on Facebook that allowed malicious websites to uncover a user's real name, access their private data and post bogus content on their behalf, which Facebook has indicated that it has corrected.[29] Another issue with social media sites is that even if a user deactivates or deletes an account, the system may still retain the information, either permanently in case a user wants to reactivate an account, or as back-up for as long as 90 days. Moreover, once a user's content is provided to other users, the user typically loses any control over what is done with that content in the future.

Perhaps the best lesson is that, absent any federal or state statutes to the contrary and without a sufficient argument against admissibility, any information located in social media sites, blogs, websites and other information-sharing technologies will be allowed as evidence in a case. Another important consideration is that even private information that might be considered to be de-identified might still be retrievable. Studies have shown that even with just a few bits of information, a researcher can identify either the specific person or narrow the subset of potential subjects to only a small group of possibilities. It is also important to note that even deleted information may not be gone, because computer forensics experts may be able to use even fragments of data to reconstruct the electronic "footprint" of what happened and who was involved.

How Does Social Media Fit into the Rules Regarding Electronic Discovery?

Even before the revisions to the Federal Rules of Civil Procedure, a number of cases had already extended discovery beyond paper and into the realm of digital technology. For example, Lange and Nimsger note a federal district court case in Utah that anticipated the value of computer data in discovery.[30] As technology progressed, various decisions clarified that discovery requests could include email messages, RAM, text messages, instant messages, chat rooms, message boards, social networking sites and sound recordings.[31] Moreover, the revised language of the Federal Rules of Civil Procedure uses the terminology Electronically Stored Information (ESI) to cast a wide net that will encompass both known and future communication technologies and also allows ESI to be inspected, tested and sampled. The text of Rule 34(a) states that:

A party may serve on any other party a request within the scope of Rule 26(b):

(1) to produce and permit the requesting party or its representative to inspect, copy, test, or sample the following items in the responding party's possession, custody, or control:

(A) any designated documents or *electronically stored information* — including writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations — *stored in any medium from which information can be obtained either directly or, if necessary, after translation by the responding party into a reasonably usable form*; or

(B) any designated tangible things; or

(2) to permit entry onto designated land or other property possessed or controlled by the responding party, so that the requesting party may *inspect*, measure, survey, photograph, *test*, or *sample* the property or any designated object or operation on it.[32]

Bahadur raised the issue of declining privacy in the transition to Web 2.0 and the impact of electronic discovery on the doctrines of attorney-client privilege, work-product protection and the attorney's duty of confidentiality.[33] More practical discussions on the discoverability of information from social media sites are offered by Goodfried and Dawson,[34] Cucco[35] and Pileggi.[36]

What Information Might Social Media Contain That Would Be Useful in a Bankruptcy Proceeding?

Social media sites can be a rich repository for information about a party. For example, in a personal injury case, the defendants requested an *in camera* review of the plaintiff's Facebook and MySpace accounts.[37] The defendants were able to argue that the information on these social media sites might reveal the plaintiff's social life, physical capabilities and emotional state and would thus be relevant in determining the extent of his injuries and the impact on his current lifestyle. After a review of the information on Facebook, the court agreed that the photographs and postings were relevant to the case because these items showed that the plaintiff continued to ride motorcycles, went hunting and rode a mule. The court ordered production of the information, indicating confusion about why the court's intervention was needed when the parties had already determined that the information was relevant and that plaintiff should have reviewed his own Facebook account without asking for the court's assistance.

In the bankruptcy context, a party's Facebook or MySpace page may suggest a more lavish lifestyle than has been asserted in the filings. Photographs may reveal hidden assets, such as cars, boats or recreational vehicles, or expensive travel. While a party claims to be unemployed or underemployed, a LinkedIn site may disclose continued employment or ownership interest in a company, freelance income on the side or other sources of income that have not been reported. An inheritance might have been received. Videos posted on YouTube might show the debtor enjoying a vacation or engaging in costly leisure activities. Social media sites might also reveal transfers of money or property to relatives or charitable organizations. The debtor might also note how various creditors have been paid or even offer advice on how best to avoid paying certain creditors. The tidbits of useful information that might be collected from social media sites are limitless, given the propensity of people to share information that, in retrospect, was better kept private or secret,

especially to the extent that it reveals improper conduct or a less-than-honest motive.

Recent Case Rulings on Social Media in Electronic Discovery

Several recent electronic discovery cases may illuminate some of the issues related to requesting and producing information from social media sites. The underlying theme of these cases is that the user can have little to no expectation of privacy on these sites, even when information has been designed as "non-public" through the user's profile settings. Moreover, the client may also be under a duty to preserve the information on a social media site in its original state once there is a reasonable anticipation of litigation.

As part of a personal injury case, the defendants in *Romano v. Steelcase* requested access to the plaintiff's current and historical Facebook and MySpace accounts, including all deleted pages and any related information.[38] The public portions of the plaintiff's sites on Facebook and MySpace indicated that her injuries were not as severe as she claimed and were not hampering her from having an active lifestyle. The court agreed with the defendant that there was a reasonable likelihood of relevant and material information on the private portions of these sites and that to deny the defendant an opportunity to access these sites would go against the liberal discovery policies of the state of New York.[39] Moreover, for the court to refuse access to the defendant would have also condoned the plaintiff's attempt to hide relevant information behind her self-regulated privacy settings.[40] In addressing the plaintiff's privacy concerns, the court noted language in the policies and the warnings of MySpace and Facebook which indicted that users post content at their own risk.[41] As the court stated,

> [t]hus, when Plaintiff created her Facebook and MySpace accounts, she consented to the fact that her personal information would be shared with others, notwithstanding her privacy settings. Indeed, that is the very nature and purpose of these social networking sites else they would cease to exist. Since Plaintiff knew that her information may become publicly available, she cannot now claim that she had a reasonable expectation of privacy. [42]

The court ended its analysis with the comment that defendant's need for access to the information outweighed any privacy concerns that the plaintiff might have, especially when the attempts of the defendant to obtain the information by other means were thwarted by the plaintiff's attorney.[43]

Other courts have reached the similar conclusions. For example, in *McMillen v. Hummingbird Speedway*, the court refused to find a new "social network site privilege" in addition to the existing exceptions for privilege between attorney-client, clergy-penitent and physician-patient, noting that evidentiary privileges are to be narrowly construed and outlining four criteria that must be established before a new privilege should be recognized.[44] In addition, the court provided an analysis of the terms and privacy policies as well as the overall purpose of social media sites to dispel arguments about the plaintiff's expectations of privacy for the information he had posted, including language in the MySpace terms of use that reserved the right for it to monitor a user's conduct and content.[45] The court went on to note that "[m]illions of people join Facebook, MySpace, and other social network sites, and as various news accounts have attested, more than a few use those sites indiscreetly. . . . When they do and their indiscretions are pertinent to issues raised in a lawsuit in which they have been named, the search for truth should prevail to bring to light relevant information that may not otherwise have been known."[46] Likewise, the court in *Zimmerman v. Weis Markets*, citing both *Romano v. Steelcase* and *McMillen v. Hummingbird Speedway*, held that no privilege exists in Pennsylvania for information posted in the non-public sections of social media websites, that liberal discovery is generally allowable and the pursuit of truth as to alleged claims is a paramount ideal.[47] On the other hand, as part of dispute over the rights to license and use works of art on apparel, the court in *Crispin v. Christian Audigier* provided a robust analysis of various provisions of the Stored Communications Act (SCA) and its application to social media sites.[48] The court remanded the case for further investigation of the plaintiff's privacy settings and the extent of access allowed to his Facebook wall and MySpace comments.[49] However, citing *Konop*, the court also noted that because the SCA was written prior to the advent of the Internet and the World Wide Web, its existing statutory framework is not well-suited to address modern forms of communication like Facebook and MySpace.[50] This case provides an especially helpful discussion of the Stored Communications Act and how it has been applied to analyze cases dealing with a variety of information technologies.

Another interesting question is the extent to which a user who changes the content of his page on a social media site rather than preserving it in its original format will be subject to sanctions for spoliation. In *Katiroll v. Kati Roll & Platters*, a trademark infringement case between two restaurants with similar food offerings, the court ordered the defendant to re-post a picture that had been removed from its Facebook page so that the plaintiff could print what it contended would show the infringement of its trade dress, after which the defendant would then replace it with the non-infringing image.[51] The court provided an analysis of when sanctions for spoliation could be imposed, noting that the best rule is to use the amount of prejudice to the opposing party to help determine the degree of fault required, and concluded that the spoliation was unintentional but somewhat prejudicial.[52] The court expressed dismay about the already considerable animosity between the parties and directed counsel to conduct themselves with the collegiality, professionalism and good faith befitting of attorneys in the jurisdiction.[53] It is important to remember that one of the underlying themes of the revisions to the Federal Rules of Civil Procedure is that counsel will collaborate throughout an electronic discovery process to reach agreements for what kinds of electronically stored information will be requested, how it will be produced and any agreements about the handling of privileged, confidential or inaccessible information rather than turning to the court to settle these disputes.

Conclusions

The information technology tools available in the 21st century have resulted in unprecedented access to and sharing of information. At the same time, these technologies have challenged well-established notions about privacy and the extent to which third parties can use this information, often without the consent

of those who are providing it. The revisions to the Federal Rules of Civil Procedure, various state court rules and recent decisions allow attorneys to cast a wide net to capture nearly any kind of electronically stored information, including information that might be found on social media sites such as YouTube, MySpace and Facebook, that is likely to be both relevant and admissible. These social media sites may provide information that would be helpful in a bankruptcy proceeding and should be considered as part of an overall discovery plan by counsel and trustees.

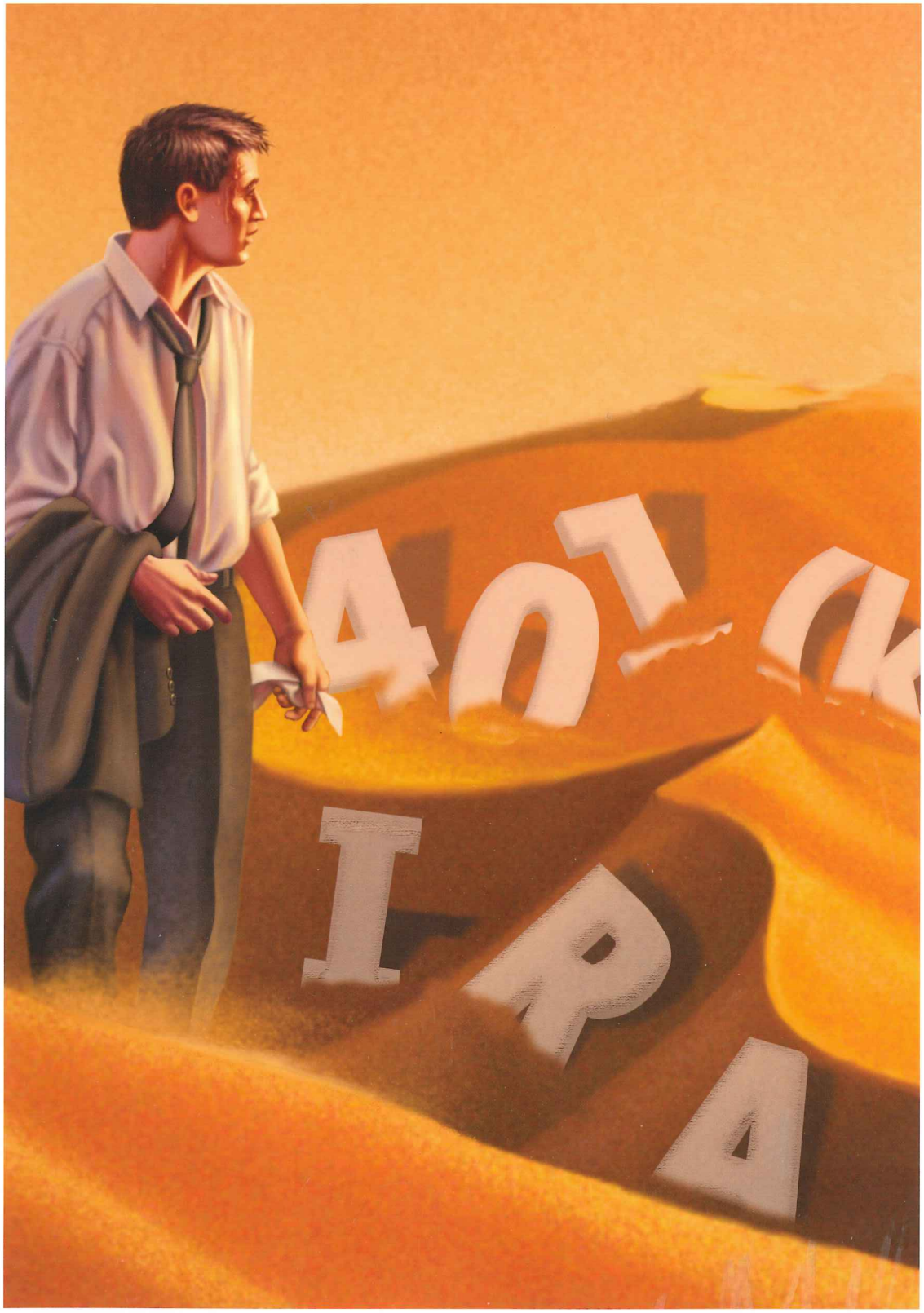
Footnotes:

1. *Social Media Statistics That Might Surprise You*, January 31, 2011, , accessed 9/29/2011.
2. *Social Media and Small Business Statistics 2010 – Usage, Achievements, Accomplishments*. October 19, 2010, , accessed 9/29/2011.
3. *Social Media*, Wikipedia, , accessed 8/30/11.
4. *Id.*
5. Kaplan, Andreas M. and Haelein, Michael H. Users of the world, unite! The challenges and opportunities of social media. *Business Horizons* 53 (1): 59–68, 2010.
6. *Id.*
7. DigitalAnalog. *How Much Is Your Content Worth?* , June 28, 2011, accessed 8/30/11.
8. *See* Jones, Harvey and Soltren, Jose H. *Facebook: Threats to Privacy*. Cambridge, MA: MIT, December 14, 2005.
9. Bonneau, Joseph, and Preibusch, Soren. *The Privacy Jungle: On the Market for Data Protection in Social Networks*. The Eighth Workshop on the Economics of Information Security, 2009.
10. Sprague, Robert. Emerging technology and employee privacy: Symposium: Rethinking information privacy in an age of online transparency. 25 *Hofstra Lab. & Emp. L.J.* 395, Spring 2008.
11. McGeveran, William. Disclosure, endorsement, and identity in social marketing. 2009 *U. Ill. L. Rev*. 1105, 2009.
12. Levin, Avner and Abril, Patricia Sanchez. Two notions of privacy online. 11 *Vand. J. Ent. & Tech. Law* 1001, Summer 2009.
13. Azriel, Joshua N. Social networking as a communications weapon to harm victims: Facebook, MySpace and Twitter demonstrate a need to amend Section 230 of the Communications Decency Act. 26 *J. Marshall J. Computer & Info. Law* 415, Spring 2009.
14. Thomas, Liisa and Newman, Robert. Social networking and blogging: The new legal frontier. 9 *J. Marshall Rev. Intell. Prop. L.* 500, 2009.
15. Grimmelmann, James. Saving Facebook. 94 Iowa L. Rev. 1137, May 2009.
16. Sabin, Jonathan. Every click you make: how the proposed disclosure of law students' online identities violates their First Amendment right to free association. 17 *J.L. & Pol'y* 699, 2009.
17. Stephens, Brad. Presentation to the Rotary Club of Indianapolis, August 30, 2011.
18. *Clark v. State*, 915 N.E. 2d 126 (Ind. 2009). *See also Commonwealth v. Williams*, 926 N.E.2d 1162 (Mass 2010); *Griffin v. State*, 419 Md. 343, 19 A.3d. 415 (Md. 2011); *People v. Clevenstein*, 891 N.Y.S.2d 511 (2009); and *State v. Eleck*, 2011 WL 3278663 (Conn. App. Aug. 9, 2011).
19. Lawson, Kate Mercer. The pitfalls of an Internet persona: Evidentiary and privacy concerns of online social media. *Michigan IT Lawyer* 28(2): 9-25, March 2011.
20. "On Beyond E-Mail" – The Emerging Labor and Employment Issues with Social Media, State Bar of Michigan Annual Meeting, September 30, 2010. *See also* Dryer, Randy L. Advising your clients (and you!) in the new world of social media: what every lawyer should know about Twitter, Facebook, YouTube & Wikis. 23 *Utah Bar J.* 16, May/June 2010.
21. ABA Formal Opinion 11-459. Duty to Protect the Confidentiality of E-mail Communication with One's Client, August 4, 2011. *See also City of Ontario v. Quon*, 130 S. Ct. 2619, (U.S. June 17, 2010).
22. ISBA Legal Ethics Committee. Legal ethics involved in online social media and networking: an overview. *Res Gestae*, March 2011, pp. 29-33, at 30. *See also* ABA Model Rules of Professional Conduct, Rules 4.1, 4.2, 4.3 and 4.4, Legal Information Institute, , accessed 9/30/11). Interestingly, in the case of *Barnes v. CUS Nashville, LLC*, 2010 L 2265668 (M.D. Tenn. June 3, 2010), to resolve disputes and delays over discovery, the magistrate judge offered to created a Facebook account and "friend" the witnesses in order to conduct a review of photographs and related comments *in camera*, after which he would promptly close the account.
23. AMA adopts recommendations on physician' social media use. *iHealthBeat*, November 10, 2010, , accessed 9/29/11.
24. Patterson, Ben. Contrite Facebook CEO promises new privacy controls. *Today in Tech: The Gadget Hound*, May 24, 2010, , accessed 9/29/11.
25. Facebook Data Use Policy, , accessed 9/29/11.
26. Some other things you need to know, , accessed 9/29/11.
27. Facebook Security, , accessed 9/29/11.
28. Two IUB students uncover Facebook vulnerability. *Indiana Informatics*, p. 5, Summer 2011.
29. *Id.*
30. Lange, Michele .C.S. and Nimsger, Kristen M. *Electronic Evidence and Discovery: What Every Lawyer Should Know Now*, 2nd ed. Chicago, IL: American Bar Association, 2009, p. 62, citing *Bills v. Kennecott Corp.*, 108 F.R.D. 459 (C.D. Utah 1985). The authors note that this was just one year after the 3.5 inch floppy disk was introduced to the public.
31. *Id.* at 62-64.
32. Federal Rules of Civil Procedure, Legal Information Institute, , accessed 9/29/11.
33. Bahadur, Rory. Electronic discovery, informational privacy, Facebook and utopian civil justice. 79 *Miss. L.J.* 317, Winter 2009.
34. Goodfried, Michael and Dawson, Martha. Discovery of Social Networking Sites. *E-Discovery Connection*, vol. 5, issue 3, December 23, 2010.
35. Cucco, Joseph. Electronic discovery of social media networking sites. *Albany Government Law Review Fireplace*, June 20, 2011, , accessed 9/29/11.
36. Pileggi, Francis G.X. Electronic discovery and social networking sites. *The Bencher*, November /December 2010, , accessed 9/29/11.
37. *Offenback v. L.M. Bowman, Inc.*, 2011 WL 2491371 (M.D. Pa. June 22, 2011).
38. *Romano v. Steelcase, Inc.*, 907 N.Y.S.2d 650 (Sept. 21, 2010).
39. *Id.* at 655.
40. *Id.*
41. *Id.* at 656.
42. *Id.* at 657.
43. *Id.*
44. *McMillen v. Hummingbird Speedway, Inc.*, No. 113-2010 CD (C.P. Jefferson Sept. 9, 2010.
45. *Id.*
46. *Id.* at 6-7.
47. *Zimmerman v. Weis Markets, Inc.*, No. CV-09-1535 (C.P. Northumberland May 19, 2011).
48. Crispin v. Christian Audigier, Inc., 717 F.Supp.2d 965 (C.D. Cal. 2010).
49. *Id.* at 991.
50. *Id.* at 988, citing *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 874 (9th Cir. 2001).
51. *Katiroll Co., Inc. v. Kati Roll & Platters, Inc.*, 2011 WL 3583408 (D.N.J. Aug. 3, 2011).
52. *Id.* at 2.
53. *Id.* at 8.

JOURNAL OF THE NATIONAL ASSOCIATION OF BANKRUPTCY TRUSTEES

NABTALK®

IN THIS ISSUE:



WINTER 2011
VOLUME 27
ISSUE 4