THE FEDERAL COURTS LAW REVIEW

Volume 5, Issue 2 2011

Discovery of Social Media

Kristen L. Mix*

TABLE OF CONTENTS

I. INTRODUCTION

This article explores the intersection of social media and litigation. As recent events in Egypt and elsewhere have demonstrated, "[s]ocial media is not a fad or frivolity, but a paradigm shift sweeping both the legal

* Kristen L. Mix graduated from Middlebury College, *cum laude*, with a degree in English and obtained her J.D. from the University of Colorado School of Law. She practiced with an expertise in labor and employment law in Denver until 2007, when she was appointed to the bench. Magistrate Judge Mix was recognized as a top employment lawyer both locally and nationally, having been honored in 2006 and 2007 by *Chambers U.S.A.* and named one of the top twenty-five women lawyers in Colorado by *5280 Magazine*. Judge Mix is on the faculty of the National Institute of Trial Advocacy and is a frequent speaker on the law.

profession and society at large."[1] Increasingly, courts are being asked to decide whether litigants are entitled to discover information contained in social media, how they may do so, and how such information may be used in litigation. A key issue is whether information contained in social media should be treated differently from other discoverable information, whether stored electronically or not.

Social media are "interactive web sites that connect users based on common interests and that allow subscribers to personalize individual web sites."[2] Examples include Facebook, MySpace, Xanga, LinkedIn, Plaxo[3] and YouTube.[4] Such internet based web-sites have been described as "'web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system.'"[5] As pointed out by one commentator, "[t]his definition emphasizes three primary activities on such sites: users create a unique online identity, establish relationships with other users, and join various communities of users who share connections."[6]

Facebook is currently the most popular social-networking web site.[7] In general, Facebook allows users to create online profiles that display information about themselves, and share that information with others.[8]

> Facebook members can share text with multiple people through a 'status update' or through information placed on the user's profile . . . . Users can also share text with another user individually through a direct message to the user or a wall post to the user's profile, or users can have a direct conversation with another user through Facebook's chat feature.[9]

---

1. Nicole Black & Carolyn Elefant, *Social Media for Solos and Small Firms*: *What It Is and Why It Matters*, N.Y.S. BAR ASS'N JOURNAL, Feb. 2011, at 18, 18.

2. John S. Wilson, *Myspace, Your Space, or Our Space? New Frontiers in Electronic Evidence*, 86 OR. L. REV. 1201, 1204 (2007).

3. *Id.*; *see also* Sharon Nelson et al., *The Legal Implications of Social Networking*, 22 REGENT U. L. REV. 1, 18 (2009-2010).

4. United States v. Am. Soc'y of Composers, Authors & Publishers, 616 F. Supp. 2d 447, 449 (S.D.N.Y. 2009).

5. Andrew C. Payne, *Twitigation: Old Rules in a New World*, 49 WASHBURN L.J. 841, 845-46 (Spring 2010) (quoting Danah M. Boyd & Nicole B. Ellison, *Social Network Sites: Definition, History, and Scholarship*, 13 J. COMPUTER-MEDIATED COMM. 1 (2007), *available at* http://jcmc.indiana.edulvoll3/issuel/boyd.ellison.html.

6. Evan E. North, Comment, *Facebook Isn't Your Space Anymore: Discovery of Social Networking Websites*, 58 U. KAN. L. REV. 1279, 1284 (2010).

7. Payne, *supra* note 5, at 846.

8. *Id.*

9. *Id.*

Facebook users may also share pictures and videos,[10] and may specifically identify who can view their information.[11] When posting photographs to Facebook, users may identify themselves or other site members by name, a process known as "tagging."[12] "A photo tag creates a link to that user's profile and identifies the person and her specific location in the photo. Anyone with access to a given user's photos can view photos in which that user is tagged, including group photos of that user and others identified by name."[13]

Twitter "allows users to share messages composed of 140 characters or less."[14] Messages may be shared with specified people or the public at large.[15] Users can either send a short message, or "tweet," or view others' messages through the Internet or a mobile phone.[16] Twitter users may also share pictures with other users.[17] Tweets are stored in a variety of ways, depending on the method of transmission, including on Twitter servers, mobile phone providers' servers or other application providers' servers.[18] Users who choose to have private Twitter accounts only display their tweets to specifically authorized persons.[19] Users who have public accounts display their tweets to the public.[20]

In general, there are three sources of information contained on social media. Such information may be obtained from the user, someone who has access to the user's page, or the website owner (e.g., Facebook, MySpace, etc.). "To gain full access to a person's [Facebook] page you have two options – join their network or become their friend."[21] Obtaining discovery through each of the sources may be problematic. Hence the solution forged by one United States Magistrate Judge, who offered to facilitate discovery of non-parties' Facebook pages by opening a Facebook account, friending the non-parties for the sole purpose of reviewing photographs and related

---

10. *Id*. at 846-47
11. *Id*. at 847.
12. North, *supra* note 6, at 1290.
13. *Id*.
14. Payne, *supra* note 5, at 847.
15. *Id*.
16. *Id*.
17. *Id*.
18. Laura Lewis Owens, *In the United States District Court for the District of Nirvana: Peter Powell vs. Doohicky, Inc. Brief of Doohickey, Inc. in Response to Plaintiff's Motion to Compel*, *in* ELECTRONIC DISCOVERY GUIDANCE 2009: WHAT CORPORATE AND OUTSIDE COUNSEL NEED TO KNOW 211, 219 (2009).
19. Payne, *supra* note 5, at 847.
20. *Id*.
21. Christopher R. Drake, *Digging Up Dirt on Facebook: Social Networking Site Becomes Valuable Tool in Litigation*, CONN. L. TRIB., Feb. 1, 2010, at 1, 2.

comments from their pages *in camera*, disseminating relevant information from the non-parties' Facebook pages to the parties, then closing his account.[22]

On Facebook:

> [A] user can limit not only who can see his or her information—ranging from only the user to everyone—but also limit the type of information visible to other specific users. [Thus], a stranger can obtain some social-networking information very easily, while other information may be more difficult or even impossible to obtain.[23]

Equally important, Facebook has a detailed subpoena policy:

> The company may provide a "Neoprint," which it describes as "an expanded view of a given user profile," in response to a subpoena. This can include the user's physical address, e-mail address, phone number, and IP address. Facebook may also provide a "Photoprint," which is "a compilation of all photos uploaded by the user that have not been deleted, along with all photos uploaded by any user which have the requested user tagged in them."[24]

Facebook's policy does not divulge how the company determines the level of data disclosure.[25] As one commentator has noted, because of the broad prohibitions of the Stored Communications Act, "[i]t appears unlikely that MySpace and Facebook would divulge private content subject to a civil subpoena without the user's consent."[26]

Twitter also has a privacy policy which specifically indicates that although Twitter stores information, "it will not release information unless required by a subpoena, court order, or legal process document."[27] Although Twitter often stores information on its servers for a short period of time, "a date preservation request can extend the period for which data is stored."[28]

Recently, the Canadian appellate courts have given in-depth review to discovery of social networking information, and have provided a road map for Canadian trial judges to use in resolving discovery disputes. Most

---

22. Barnes v. CUS Nashville, LLC, No. 3:09-cv-00764, 2010 WL 2265668, at *1 (M.D. Tenn. June 3, 2010).

23. Payne, *supra* note 5, at 864-65.

24. North, *supra* note 6, at 1289 (quoting Preston Gralla, *Leaked intelligence documents: Here's what Facebook and Comcast will tell the police about you*, COMPUTER WORLD BLOG (Mar. 1, 2011), http://blogs.computerworld.com/15667/leakedintelligencedocumentshereswhatfacebookandcomcast will tell the police-about you).

25. *Id*.

26. *Id*. at 1306.

27. Payne, *supra* note 5, at 848.

28. *Id*.

significantly, the Canadian approach discards the idea that social networking site content should be treated differently based upon the user's privacy settings. As one court concluded: "A party who maintains a private, or limited access, Facebook profile stands in no different position than one who sets up a publicly-available profile. Both are obliged to identify and produce any postings that relate to any matter in issue in the action."[29] This reasoning was based on the court's view that the potential for withholding relevant information in a case is great because Facebook's privacy controls are so easily manipulable:

> [T]o permit a party claiming very substantial damages for loss of enjoyment of life to hide behind self-set privacy controls on a website, the primary purpose of which is to enable people to share information about how they lead their social lives, risks depriving the opposite party of access to material that may be relevant to ensuring a fair trial.[30]

In a very practical and down-to-earth fashion, one Canadian judge noted that "[t]he plaintiff could not have a serious expectation of privacy given that 366 people have been granted access to [his] private site [on Facebook]."[31] Said another: "Facebook is not used as a means by which account holders carry on monologues with themselves . . . ."[32]

Other Canadian courts have interpreted these cases to require plaintiffs to preserve relevant photographs and other information on social-networking sites and to list this information in the equivalent of mandatory disclosures pursuant to Fed. R. Civ. Pro. 26(a)(1).[33] One federal judge in the United States has cited these cases with approval in the context of granting a request for discovery from sexual harassment plaintiffs' MySpace and Facebook pages relating to their "emotion[s], feeling[s] or mental state[s]."[34]

Have the Canadian courts taken the right approach? This article explores that question by addressing three litigation issues relating to information contained in social media: (1) Can you get it? (2) Can you use it? and (3) Is the Constitution involved? Finally, the author suggests tips for the practitioner.

---

29. *Leduc v. Roman*, [2009] O.J. No. 681, para. 32 (Can. Ont. S.C.J.) (QL).
30. *Id.* at para. 35.
31. *Murphy v. Perger*, [2007] O.J. No. 5511, para. 20 (Can. Ont. S.C.J.) (QL).
32. *Leduc v. Roman*, [2009] O.J. No. 681, para. 31 (Can. Ont. S.C.J.) (QL).
33. *Wice v. Dominion of Can. Gen. Ins. Co.*, [2009] O.J. No. 2946, para. 20 (Can. Ont. S.C.J.) (QL).
34. Equal Emp't Opportunity Comm'n. v. Simply Storage Mgmt., LLC, 270 F.R.D. 430, 431 (S.D. Ind. 2010).

II. CAN YOU GET INFORMATION CONTAINED IN SOCIAL MEDIA?

A. Access to and Storage of Information

A social media user's privacy settings dictate a person's access to information contained on MySpace, Facebook and LinkedIn. A person must be a "friend" of a Facebook user to get access to his or her page.[35] However, a user's private comments on Facebook can be cut and pasted elsewhere, and thus may become generally accessible on the Internet.[36] Blog posts are generally readily accessible by any Internet user.[37] Tweets on public accounts can be accessed by any third party online.[38]

Storage of social media information is complicated. Tweets are stored on Twitter's servers unless deleted by the sender, but may also be stored on mobile phone providers' servers or other application providers' servers. Facebook information is not stored on the user's server, but instead is stored on Facebook's servers.[39]

B. Legal Issues

In general, case law and comments to date have identified the following legal issues related to discovery of social media: (1) application of the Federal Rules regarding electronically stored information (ESI); (2) scope of a party's "possession, custody or control" or ability to access information or both; (3) duty to preserve or spoliation; (4) privacy; (5) relevance; and (6) applicability of the Stored Communications Act and the Electronic Communications Privacy Act. Each of these issues is addressed separately below.

1. Application of the Federal Rules Regarding ESI

Some commentators have asserted that "courts have not yet concluded that [instant messages] and [T]witter communications are electronically stored information subject to discovery,"[40] because of the temporary nature of their storage. Others contend that:

> Because of the dynamic distinctions between ESI and social-networking information, courts should bypass the old ESI rules . . . . The

35. Payne, *supra* note 5, at 847.
36. Nelson, *supra* note 3, at 2.
37. North, *supra* note 6, at 1295-96.
38. Payne, *supra* note 5, at 847.
39. *Id*. at 863-64.
40. Owens, *supra* note 18, at 216.

> accessibility of social-networking information represents a large departure from traditional ESI because social-networking users cannot control the storage or retrieval of their information. Under the ESI amendments' two-tiered approach, a party must produce reasonably accessible information or produce inaccessible information upon a showing of good cause by the requesting party. The limits placed on the production of ESI under Rule 26(b)(2)(C) . . . leave out any consideration of a party's ability to control costs."[41]

2. Scope of a Party's Possession, Custody or Control and/or Access

One commentator argues that any relevant content that a user could access on Facebook should be discoverable, regardless of who uploaded it onto the site.[42] He points out:

> In other e-discovery and traditional discovery cases, courts have held that documents are within a party's control if the party has a legal right to obtain the documents. In the context of access-limited social-networking content, users have the ability—and arguably the legal right—to obtain third-party information posted to friends' profiles. The "legal right to obtain" interpretation of the possession, custody, or control standard likely encompasses all manner of third-party social-networking content, including relevant photos, wall posts, and status messages.[43]

Netbula, LLC v. Chordiant Software, Inc.[44] is a case about website pages which illustrates the point. Defendant moved to compel production of plaintiff's archived web pages.[45] The old versions of those pages had been automatically archived by a web-based data storage service called Internet Archive, which is also known as the "Wayback Machine."[46] Internet Archive is a "digital library" that provides access to archived websites.[47] Plaintiff argued that copies of its old web pages were beyond its control and thus could not be provided in response to a Rule 34 document request.[48] The court disagreed, reasoning that the plaintiff had "the legal right to obtain the documents on demand" and only needed to disable a single file on its website to allow the defendant to access the web pages on file at Internet Archive.[49] The court was unpersuaded by the argument that

---

41. Payne, *supra* note 5, at 865.
42. *See* North, *supra* note 6, at 1303.
43. *Id.*
44. No. C08-00019 JW (HRL), 2009 WL 335288 (N.D. Cal. Oct. 15, 2009).
45. *Id.* at *1.
46. *Id.*
47. *Id.*
48. *Id.*
49. *Id.* at *1-2.

defendant could subpoena Internet Archive directly, because that would involve "considerable burden, expense and disruption to its operations . . . whereas plaintiffs could permit access to the information in minutes and with minimal burden and expense."[50]

In *Arteria Property Pty Ltd. v. Universal Funding V.T.O., Inc.*[51], the court addressed plaintiff's motion for spoliation sanctions due to defendant's failure to produce a copy of its website as it existed when the parties' dispute first arose.[52] Defendant argued, among other things, that the website was not within its control as of the relevant date.[53] The court stated:

> This Court sees no reason to treat websites differently than other electronic files. Where, as here, Defendants had control over the content *posted* on its website, then it follows *a fortiori* that it had the power to delete such content. Although Defendants do not so posit, it may be argued that the website was maintained by a third party, perhaps a web design company who posted content on behalf of Defendants. But this is irrelevant, just as it'd be irrelevant if the website was maintained on a third party server rather than Defendant's own server (as is likely the case here). Despite the inevitable presence of an intermediary when posting content on the Web, the Court finds that Defendants still had the *ultimate* authority, and thus control, to add, delete, or modify the website's content. There is no evidence to the contrary.[54]

It remains to be seen whether the *Arteria* court's logic will be followed in the context of resolving disputes about social-networking site information.

Employers frequently argue that they lack control over their employees' personal email accounts and text messages, especially when there is no evidence that employees' personal ESI was created or preserved on a company network. Although employers may concede that their employees use personal email accounts for business purposes, they assert that any such statements are not official company statements and "not binding as to the company."[55] Employers usually point out that when employees' email accounts are not "hosted" by the employers, employees retain sole control to delete or preserve emails.[56] Similarly, employers often

---

50. *Id.* at *2.
51. No. 05-4896 (PSG), 2008 WL 4513696 (D.N.J. Oct. 1, 2008).
52. *Id.* at *5.
53. *Id.*
54. *Id.*
55. Owens, *supra* note 18, at 216.
56. *Id.* at 215.

assert that they lack reasonable access to instant messages, like Twitter, because they do not host the social networking site on which their employees' communications were made.[57]

3. Duty to Preserve/Spoliation

Courts have generally held that the duty to preserve electronic data arises when a party reasonably anticipates litigation.[58] When dealing specifically with information from social-networking sites, some commentators advocate distinctions between "sophisticated parties" and "unsophisticated parties."[59] In this construct, "[t]he duty to preserve social-networking information should apply only to parties who are experienced in litigation and in fact able to anticipate litigation. The court should analyze the experience and sophistication of the producing party before pronouncing a violation of the broad duty to preserve."[60] Although Twitter and Facebook fall under the rubric of "sophisticated parties" and should be subject to a duty to preserve information, they "require court orders for information to be preserved."[61] Currently no court appears to have adopted the particularized inquiry referenced above.

4. Privacy

Probably the most frequently litigated issue surrounding discovery of social-networking site information is the user's right to privacy. It is well known that "a Facebook profile can contain a virtual treasure trove of personal information, . . . [and] [a]s the list of features and applications available to those frequenting social networking sites has grown, so too has the depth of information about both who you are and who you know."[62] Moreover, it is equally well established that "courts have been unwilling to recognize a reasonable expectation of privacy for materials people willingly post on the Internet without taking any measures to restrict access to them, or otherwise protect them."[63]

Social networking sites, like Facebook, generally permit three levels of disclosure by the user: to everyone; to a self-selected group of friends or "friends of friends;" and to a specified user only. Facebook's privacy

57. *Id.* at 219-21.
58. *See, e.g.*, Zubulake v. UBS Warburg, LLC, 220 F.R.D. 212, 216 (S.D.N.Y. 2003).
59. Payne, *supra* note 5, at 866.
60. *Id.* at 867.
61. *Id.*
62. Nelson, *supra* note 3, at 21.
63. *Id.*

policy classifies certain categories of information as "public," but further explains that such information may become public only in limited circumstances; when the site decides that sharing the information is legally required, permitted by the user, or "reasonably necessary to offer [the] service."[64] The policy requires a "good faith belief that the response is required by law" before user information can be disclosed in response to a subpoena or court order.[65]

Some commentators have asserted that Facebook users who limit access to selected content may subjectively expect this content not to be shared beyond their group of friends: "But this expectation is objectively unreasonable because other users can disseminate the content without obtaining consent from the user who posted it."[66]

Courts have struggled with privacy issues in the context of disputes about discovery of social networking site information. In *Mackelprang v. Fidelity National Title Agency of Nevada, Inc.*,[67] the defendant moved to compel the plaintiff in a sexual harassment case to consent to release of her private MySpace messages. Defendant subpoenaed MySpace to learn the identity and profile information behind two accounts it believed belonged to Plaintiff.[68] Defendant alleged Plaintiff had established two profiles on MySpace: one listed her as single with no interest in children, and the other listed her as married with six children. Defendant believed that Plaintiff used the first account to send sexually explicit emails to colleagues she later accused of sexual harassment.[69]

MySpace refused to provide private messages without a search warrant or letter of consent from the account holder.[70] It complied with the subpoena by providing a spreadsheet which confirmed Plaintiff as the user on both accounts.[71] The court denied the motion to compel, on the grounds that the request amounted to a "fishing expedition"[72] that "would allow Defendants to cast too wide a net for any information that might be relevant and discoverable."[73] The Court, however, invited a more narrowly tailored request based on some basis, beyond mere speculation, to support a

---

64. *See generally* FACEBOOK PRIVACY POLICY, http://www.facebook.com/policy.php (last visited Mar. 27, 2011).
65. *Id*.
66. North, *supra* note 6, at 1296.
67. No. 2:06-cv-00788-JCM-GWF, 2007 WL 119149, at *2 (D. Nev. Jan. 9, 2007).
68. *Id*.
69. *Id*.
70. *Id*.
71. *Id*.
72. *Id*.
73. *Id*. at *7.

reasonable belief that Plaintiff engaged in sexually explicit email communications on her MySpace.com accounts with former co-employees.[74]

In *T.V. v. Union Township Board of Education*, a middle school student sued her school for emotional distress resulting from a sexual assault allegedly perpetrated by another student on school grounds.[75] The school attempted to discover plaintiff's MySpace and Facebook pages to show evidence of her mental state before and after the incident.[76] When the plaintiff moved for a protective order on the grounds of her privacy rights, the court granted the motion, but "left the door open for later discovery if the school could make a particularized showing of relevance."[77]

One commentator has identified three reasons why courts have not acknowledged privacy rights in social-networking information:

> First, the courts are unwilling to give any privacy protection to information deliberately placed in the public sphere . . . . Second, courts balance relevant evidence against privacy in favor of production . . . . Third, one [California state] court has held that a person has no reasonable expectation of privacy for information posted on a social-networking site.[78]

This commentator suggests "[a] blanket judicial interpretation that users have no expectation of privacy in social-networking information threatens the social benefits of the websites."[79]

5. Relevance

Two principles emerge from the case law regarding the relevance of information contained on social networking sites. First, courts are reluctant to allow the user to unilaterally determine which information is relevant. Second, courts are reluctant to find social networking information to be privileged.

In *Bass v. Miss Porter's School*, defendant requested production of Facebook content relating to alleged teasing and taunting of plaintiff, a student at the school.[80] Plaintiff had lost access to her Facebook account,

---

74. *Id*. at *8.

75. North, *supra* note 6, at 1293 (citing T.V. v. Union Township Board of Education, No. UNN-L-4479-04 (N.J. Super. Ct. June 8, 2007)).

76. North, *supra* note 6, at 1293.

77. *Id*.

78. Payne, *supra* note 5, at 861.

79. *Id*. at 869.

80. Bass *ex rel*. Bass v. Miss Porter's Sch., No. 3:08cv1807 (JBA), 2009 WL 3724968, at *1 (D. Conn. Oct. 27, 2009).

and served a subpoena on Facebook to obtain the information that would comply with defendant's request.[81] The court initially ordered plaintiff to provide any responsive documents to defendant, and to provide the entire set of documents to the court for an *in camera* review.[82] After such review, the court held that there was "no meaningful distinction" between the documents plaintiff provided to defendant and those provided to the court for review:

> [R]elevance of the content of Plaintiff's Facebook usage as to both liability and damages in this case is more in the eye of the beholder than subject to strict legal demarcations, and production should not be limited to Plaintiff's own determination of what may be "reasonably calculated to lead to the discovery of admissible evidence."[83]

In *Ledbetter v. Wal-Mart Stores, Inc.*, plaintiffs asserted personal injuries as the result of an incident at Wal-Mart.[84] Defendant served subpoenas on Facebook, MySpace and Meetup.com to discover information about Ledbetter, the plaintiff.[85] Plaintiff asked for, and got, an *in camera* inspection of the produced documents on the grounds that they were protected by the physician-patient and spousal privileges.[86]

The Court deemed both privileges waived because of the filing of the lawsuit for mental and physical injuries, and because plaintiff's wife asserted a claim for loss of consortium. The Court further held that the information obtained from the social media was protected as confidential pursuant to the parties' Stipulated Protective Order, and that no further order was necessary to protect privacy interests.[87]

6. Applicability of Stored Communications Act and Electronic Communications Privacy Act

Congress passed the Stored Communications Act (SCA) in 1986 as part of the Electronic Communications Privacy Act (ECPA).[88] In general, the SCA prevents providers of communication services from divulging

---

81. *Id.*
82. *Id.*
83. *Id.*
84. Ledbetter v. Wal-Mart Stores, Inc., No. 06-cv-01958-WYD-MJW, 2009 WL 1067018, at *1 (D. Colo. Apr. 21, 2009).
85. *Id.*
86. *Id.*
87. *Id.* at *2.
88. Electronic Communications Privacy Act of 1986 (ECPA), Pub. L. No. 99-508, 100 Stat. 1848, 1860-68 (1986) (ECPA codified as amended in scattered sections of 18 U.S.C.) (Stored Communications Act (SCA) codified as amended in 18 U.S.C. §§ 2701-12 (2006)).

private communications to certain entities and individuals.[89] The statute distinguishes between a remote computing service (RCS) provider and an electronic communication service (ECS) provider. It defines an RCS as an entity that provides to the public "computer storage or processing services by means of an electronic communications system."[90] It defines an ECS as "any service which provides to users thereof the ability to send or receive wire or electronic communications."[91] Although the statute was specifically enacted to deal with the advent of the Internet and "a host of potential privacy breaches that the Fourth Amendment does not address,"[92] it was adopted long before any social networking websites had been developed.

Recently, a federal court in the Central District of California quashed subpoenas to MySpace and Facebook on the grounds that some of the content on those sites is protected by the SCA, and because the user had selected certain privacy settings intended to limit access to his pages.[93] In *Crispin v. Christian Audigier Inc.*, the plaintiff artist alleged that defendants used his artwork in violation of their oral agreement, and filed suit for copyright infringement.[94] The Court held that private messaging and email services provided by social networking sites constitute ECS, and that such sites are both ECS and RCS providers as to wall postings and comments posted on an account holder's web page.[95] The court concluded that webmail and private messaging services provided on social networking websites are not subject to subpoena under the SCA, because such messages were not readily accessible to the general public and were, therefore, inherently private.[96]

The decision has been harshly criticized as applying "outmoded federal electronic privacy laws from the 1980s" to "new technologies."[97] One commentator points out that computer usage has changed dramatically since 1986, when subscribers used third-party network services for two main purposes: "sending communications, such as e-mail, and outsourcing resource-intensive computing tasks, such as storing large files or processing

---

89. *See* 18 U.S.C. §§ 2701-12.

90. 18 U.S.C. § 2711(2) (2006) (defining remote computing service).

91. 18 U.S.C. § 2510(15) (2006) (defining electronic communication service).

92. Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 971 (C.D. Cal. 2010) (citing Quon v. Arch Wireless Operating Co., Inc., 529 F.3d 892, 900 (9th Cir. 2008)).

93. *Id*. at 991.

94. *Id*. at 968.

95. *Id*. at 980, 990.

96. *Id*. at 991.

97. *See* Alan Klein et al., *Social Networking Sites: Subject to Discovery? Ruling Holds that Messages and Comments Visible to a Restricted Set of Users Are Protected*, NAT'L L. J., Aug. 23, 2010, at 15, 15.

data."[98] The author states that the definitions of the SCA and ECPA do not readily fit the capabilities of social-networking sites. Moreover, the author points out that the decision does not address "how restricted access to content must be in order for that content to be considered private, [and] the interaction between a provider's policies and an individual's privacy choices."[99] Of course, one could argue that these questions have been left undecided by the entirety of applicable jurisprudence.

A slightly older case relied on the ECPA to limit discovery of social networking site information. In September of 2009, Facebook fought a subpoena issued in a Virginia workers' compensation case which sought photographs posted by the claimant.[100] The employer hoped the photographs would demonstrate the claimant's alleged back injury was not as serious as claimed.[101] The Deputy Commissioner agreed that pursuant to the Electronic Communications Privacy Act,[102] the claimant's "privacy decision" must be respected and could be enforced by Facebook in order to protect its user's data.[103]

Another interesting case rejected a subpoena for "all emails sent or received by anyone" at the plaintiff's company on the grounds of overbreadth pursuant to Federal Rule of Civil Procedure 45.[104] A panel of the Ninth Circuit Court of Appeals reversed the trial court's dismissal of the plaintiff's SCA claim against its ISP provider who had responded to the subpoena.[105] Judge Alex Kozinski wrote that the Act "reflects Congress's judgment that users have a legitimate interest in the confidentiality of communications in electronic storage at a communications facility."[106] He concluded that because the overbroad subpoena "transparently and egregiously" violated the Federal Rules of Civil Procedure, the ISP's production of emails created a cognizable claim under the Act.[107]

C. Cost-Shifting Issues

In general, the federal courts have adopted three approaches to the cost-shifting analysis as it applies to electronic discovery. First, the

---

98. *Id.*
99. *Id.* at 19.
100. *See* Drake, *supra* note 21.
101. *Id.*
102. *See* 18 U.S.C. § 2702 (2006).
103. Payne, *supra* note 3, at 846-47.
104. Theofel v. Farey-Jones, 359 F.3d 1066, 1071 (9th Cir. 2004).
105. *Id.* at 1079.
106. *Id.* at 1072.
107. *Id.* at 1074, 1079.

"marginal utility" approach to balancing the costs of e-discovery has its roots in *McPeek v. Ashcroft*.[108] This approach reasons that the more likely it is that a resource, like a back-up tape, contains relevant information, the fairer it is to impose the costs of production on the producing party.[109]

The second approach was generated by *Rowe Entertainment, Inc. v. William Morris Agency, Inc.*[110] The court listed eight factors that had been used in other cases to determine when an undue burden or expense justified shifting the cost of discovery.[111]

Finally, the most recent—and best used—cost-shifting approach was developed in *Zubulake v. UBS Warburg, LLC*.[112] There the court eliminated or modified two prongs of the *Rowe* test and developed a new test devised of seven factors.[113] The court noted that the seven factors should not be weighed equally, and that the central question is whether the discovery request imposes an undue burden or expense on the responding party, or "put another way, 'how important is the sought-after evidence in comparison to the cost of production?'"[114]

Several courts have used the *Zubulake* cost-shifting approach with regard to electronic discovery.[115] One commentator has suggested a universal adoption of the *Zubulake* cost-shifting analysis to discovery disputes involving social media information because "under this framework, courts will be able to protect producing parties from undue and unpredictable production expenses that lay outside of the producing party's control and shift some of those costs to the requesting party."[116]

---

108. McPeek v. Ashcroft, 202 F.R.D. 31, 34 (D.D.C. 2001).
109. *Id.*
110. Rowe Entm't, Inc. v. William Morris Agency, 205 F.R.D. 421 (S.D.N.Y. 2002).
111. *Id.* at 429.
112. Zubulake v. UBS Warburg, LLC, 217 F.R.D. 309 (S.D.N.Y. 2003)
113. *Zubulake* introduced seven factors:

> (1) the extent to which the request is specifically tailored to discover relevant information; (2) the availability of such information from other sources; (3) the total cost of production, compared to the amount in controversy; (4) the total cost of production, compared to the resources available to each party; (5) the relative ability of each party to control costs and its incentive to do so; (6) the importance of the issues at stake in the litigation; and (7) the relative benefits to the parties of obtaining the information.

Zubulake v. UBS Warburg, LLC, 216 F.R.D. 280, 284 (S.D.N.Y. 2003).
114. *Zubulake*, 217 F.R.D. at 322-23.
115. *See, e.g.*, Major Tours, Inc. v. Colorel, No. 05-3091, 2009 WL 3446761, at *5 (D.N.J. Oct. 20, 2009); Ex Parte Cooper Tire & Rubber Co., 987 So. 2d 1090, 1106 (Ala. 2007).
116. Payne, *supra* note 5, at 866.

III. CAN YOU USE INFORMATION OBTAINED FROM SOCIAL MEDIA?

One federal court has concluded that a proponent of electronically stored information must generally clear five evidentiary hurdles: relevance (Fed. R. Evid. 401), authenticity (Fed. R. Evid. 901(a)), prohibition on hearsay (Fed .R. Evid. 801, 803, 804, 807), requirement of an original writing (Fed. R. Evid. 1001-1008), and probative value outweighs the danger of unfair prejudice (Fed. R. Evid. 403).[117] Indeed, numerous commentators have described the dangers of attempting to introduce into evidence electronic information obtained by a lawyer (or at a lawyer's request) without formal discovery. Unless email is authenticated by a recipient or a sender, or by an I.T. or systems administrator, for example, it may not be admissible into evidence.[118] Moreover, email may not be a business record, and thus an exception to the hearsay rule, unless a business can establish that it maintains adequate and consistent practices regarding electronic mail.[119]

Commentators have also opined that "it seems unlikely that information gathered on social networking sites could be described as self-authenticating."[120] Courts have pointed out that "[p]rintouts from a website do not bear the indicia of reliability demanded for other self-authenticating documents under Fed. R. Evid. 902."[121] "Anyone may purchase an Internet address, and so, without proceeding to discovery or some other means of authentication, it is premature to assume that a webpage is owned by a company merely because its trade name appears in the uniform resource locator."[122] To properly authenticate web page content, "some statement or affidavit from someone with knowledge is required; for example, a webmaster or someone else with personal knowledge."[123]

Likewise, third-party information gatherers who copy information from social networking sites—including statements and photographs—will have to overcome the Federal Rules' prohibition on hearsay. Even the "catch-all" exception to the hearsay rule may be unavailing, as the

---

117. Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 538 (D. Md. 2007).

118. 4 IAN C. BALLON, E-COMMERCE & INTERNET LAW § 58.02[1] (2d ed. Supp. 2009-2010).

119. *Id.*

120. Wilson, *supra* note 2, at 1229; *see also* Dennis R. Kiker et al., *Trial Practice Management*, *in* EDISCOVERY FOR CORPORATE COUNSEL ch. 15, § 15:6 (Carole Basri & Mary Mack eds., 2010).

121. *In re* Homestore.com Sec. Litig., 347 F. Supp. 2d 769, 782 (C.D. Cal. 2004).

122. Victaulic Co. v. Tieman, 499 F.3d 227, 236 (3d Cir. 2007).

123. *In re Homestore.com*, 347 F. Supp. 2d at 782-783; *see also* Kiker et al., *supra* note 120.

requirement for "circumstantial guarantees of trustworthiness . . . seems lacking in evidence gathered on social networking sites."[124] However, at least one federal court has admitted copies of an archived web site of a skinhead organization that posted the name, address and picture of the victim, along with a call to attack him.[125] The pages were obtained from Internet Archive. The court held that the opponent offered no evidence that Internet Archive is unreliable or biased, and had not denied that the pages were accurate or challenged their veracity.[126] Instead, the pages were merely images and text showing what the web page once looked like, and were deemed to be an admission of a party opponent.[127]

Moreover, a federal judge held that photographs of a defendant from his MySpace page were relevant in his criminal trial asserting possession of firearms and drugs—without commenting as to the page's authenticity—despite the fact that the photographs were not produced by the defendant or MySpace, but instead were apparently obtained by the prosecutor.[128]

IV. CONSTITUTIONAL ISSUES

A. Fourth Amendment Right to Freedom From Unreasonable Searches

Commentators have raised the question of whether a person has a reasonable expectation of privacy under the Fourth Amendment in a personal web site that has been secured by some form of privacy protection, like limitations on access to certain users.[129] More specifically, questions about the right of law enforcement officers to use social-networking sites to gather evidence of crimes and, once such evidence is gathered, to use it in court remain unresolved.[130]

B. First Amendment Right to Freedom of Speech

Arguments surrounding the First Amendment play a significant role in litigation against anonymous bloggers. As stated by one court:

---

124. Wilson, *supra* note 2, at 1232 (internal quotations and citation omitted).

125. Telewizja Polska USA, Inc. v. Echostar Satellite Corp., No. 02 C 3293, 2004 WL 2367740, at *5-6 (N.D. Ill. Oct. 15, 2004).

126. *Id*. at *6.

127. *Id*. at *5; *see also* Beth C. Boggs & Misty L. Edwards, *Does What Happens on Facebook Stay on Facebook? Discovery, Admissibility, Ethics, and Social Media*, 98 ILL. B. J. 366 (July 2010); Kiker, et al., *supra* note 120, § 15.5.

128. United States v. Drummond, No. 1:09-cr-00159, 2010 WL 1329059, at *2 (M.D. Pa. Mar. 29, 2010).

129. Wilson, *supra* note 2, at 1203.

130. *Id*. at 1224-36.

> The protections of the First Amendment extend to the Internet. Courts have recognized the Internet as a valuable forum for robust exchange and debate. Through the use of chat rooms, any person with a phone line can become a town crier with a voice that resonates farther than it could from any soapbox. Courts also recognize that anonymity is a particularly important component of Internet speech. Internet anonymity facilitates the rich, diverse and far ranging exchange of ideas; the constitutional rights of Internet users, including the First Amendment right to speak anonymously, must be carefully safeguarded.[131]

However, as anticipated, all anonymous Internet speech is not free speech. Several courts have held that those who harm others or violate agreements through Internet speech are not protected by the First Amendment.[132] Courts have devised various tests for "balancing the conflicting rights of an anonymous online speaker and an allegedly injured party."[133] In a Title VII discrimination speech, one court applied a four-part test: whether (1) the subpoena was issued in good faith, (2) "the information sought relates to a core claim or defense, (3) the identifying information is directly and materially relevant to that claim or defense, and (4) information sufficient to establish or to disprove that claim or defense is unavailable from any other source."[134] In a public figure defamation case, the Delaware Supreme Court held that "before a defamation plaintiff can obtain the identity of an anonymous defendant . . . he must support his defamation claim with facts sufficient to defeat a summary judgment motion."[135] Recently, the Ninth Circuit held that the Delaware Supreme Court test is too harsh in cases involving commercial speech, which enjoys less First Amendment protection than political speech.[136]

V. PRACTICE TIPS

1. Seek discovery of social networking information from the opposing party before subpoenaing Facebook or other social networking websites.
2. Perform a public search for information usually available on a social networking website.

---

131. Best W. Int'l, Inc. v. Doe, No. CV-06-1537-PHX-DGC, 2006 WL 2091695, at *3 (D. Ariz. 2006) (internal quotation marks and citations omitted).

132. *See, e.g.*, Immunomedics, Inc. v. Doe, 775 A.2d 773, 777-78 (N.J. Super. A.D. 2001).

133. McVicker v. King, 266 F.R.D. 92, 94 (W.D. Pa. 2010).

134. *Id.* at 96-97.

135. Doe v. Cahill, 884 A.2d 451, 460 (Del. 2005).

136. *In re* Anonymous Online Speakers, 611 F.3d 653, 661 (9th Cir. 2010).

3. Be mindful of your ethical responsibilities. Hiring a private investigator to "friend" the opposing party may be "inherently deceitful and unethical, even if the investigator uses his own name."[137] Contacting the opponent yourself would likely be impermissible direct contact, and may also violate the rule providing that a lawyer may not "engage in conduct involving dishonesty, fraud, deceit, or misrepresentation."[138]
4. In complex cases, explore the possibility of "unbundling," or development of a litigation management team to handle electronic data.[139]
5. This is not your father's discovery. Successful discovery of social networking information may require significant efforts to educate the judiciary about the fallacy underlying electronic discovery (just because something is electronic, it can be searched and produced instantly) and the actual cost and burden of production.
6. Advise your clients to be prudent and avoid spoliation sanctions. "The courts have a right to expect that litigants and counsel will take the necessary steps to ensure that relevant records are preserved when litigation is reasonably anticipated, and that such records are collected, reviewed, and produced to the opposing party."[140]

---

137. *See, e.g.*, Robert S. Kelner & Gail S. Kelner, *Social Networks and Personal Injury Suits*, N.Y.L.J., (Sept. 24, 2009), www.law.com/jsp/nylj/PubArticleFriendlyNY.jsp?hubtype=&id=1202434026615.

138. Phil. Bar Ass'n Prof'l Guidance Comm. Op. 2009-02 (Mar. 2009), *available at* http://www.philadelphiabar.org/WebObjects/PBAReadOnly.woa/Contents/WebServerResources/CMSResources/Opinion_2009-2.pdf; *see* MODEL RULES OF PROF'L CONDUCT R. 8.4 (2009).

139. Howard B. Iwrey et al., *A Multidimensional Solution to the Problems of Runaway Discovery*, OF COUNSEL, June 2010 at 12, 12.

140. Pension Comm. of the Univ. of Montreal Pension Plan v. Bank of Am. Sec. LLC, 685 F. Supp. 2d 456, 461 (S.D.N.Y. 2010).