Facebook Isn't Your Space Anymore: Discovery of Social Networking Websites*

I. INTRODUCTION

In his attorney's words, "Jerry" learned about the dangers of Facebook "the hard way."[1] After he sustained neck and back injuries in a car accident, Jerry retained Seattle personal-injury attorney Christopher Davis to represent him in a suit against another driver.[2] The defendant's insurer hired a lawyer, and each side commenced discovery.[3] Medical experts were hired, documents were exchanged, and depositions were taken.[4] Jerry testified in his deposition that the accident likely would require "periodic medical treatment off and on to treat his neck and back pain symptoms in the future."[5]

About a month before trial, the insurer's attorney sent Davis a CD loaded with photos and a video of Jerry snowboarding that the insurer intended to admit into evidence.[6] The video, produced years after the accident, showed Jerry "going off jumps on his snowboard at a high rate of speed."[7] The insurer's attorney downloaded the photos and video from the plaintiff's Facebook and MySpace pages.[8]

Davis, aware of "the perception that these materials were likely to create for the jury," contacted the insurer to settle the claim and avoid a trial.[9] The claims adjuster revised her previous assessment of Jerry's

---

* *Evan E. North*. J.D. candidate 2011, University of Kansas School of Law; M.A. 2006, Pace University; B.S. 2004, Northwestern University. The author would like to thank Kelly Bieri for bringing this issue to his attention and Professor Laura Hines for her helpful feedback.

1. Christopher Davis, *Insurance Company Discovers Client's FaceBook Page—Reduces Offer by $20,000*, SUBMIT YOUR ARTICLE, Sept. 13, 2009, http://www.submityourarticle.com/articles/Christopher-Davis-2363/settlement-devalued-64817.php. The name "Jerry" is a pseudonym for one of the author's clients. *Id.*
2. *Id.*
3. *Id.*
4. *Id.*
5. *Id.*
6. *Id.*
7. *Id.*
8. *Id.*
9. *Id.*

injuries based on the evidence that Jerry was in fact able to engage in aggressive sports activity, and she reduced the settlement offer by $20,000.[10]

At least one trial judge has ruled private social-networking information to be discoverable when a defendant has reason to believe there is relevant information on the profile.[11] The convergence of privacy issues and discovery is not new—personal diaries have long been held to be discoverable[12]—but application in the context of social-networking sites remains relatively untested in this country. Social-networking sites provide an online nexus for a myriad of social and professional relationships; many users understandably develop a sense of familiarity and privacy when using the sites to interact with friends on a daily basis.[13] But this sense of virtual comfort may come with an unreasonable expectation of privacy regarding the personal information included in a social-networking profile,[14] even when privacy restrictions are in place.[15] The explosive growth of Facebook and MySpace—and the attendant pervasiveness of the sites' use around the world—demands a workable framework within the complex arena of electronic discovery, or "e-discovery." This Comment argues that information shared with even a small group of users on a social-networking site should be discoverable when relevant to a cause of action. The inherent purpose of these sites undercuts any subjective expectation of privacy.

This Comment discusses the discoverability of social-networking information by private litigants in civil cases. It begins in Part II by discussing common e-discovery issues, as previously applied to corporate documents and e-mail communications. It then describes the backdrop of rapid growth of the use of social-networking sites. Next, it will consider the privacy issues surrounding discovery of access-limited social-networking profile information.

Through the development of analogies to cases addressing the expectation of privacy in Internet posts and private e-mail

10. *Id.*

11. Order Regarding Plaintiffs' Motion for Protective Order Pursuant to Fed. R. Civ. P. 26(c) Regarding Subpoenas Issued to Facebook, MySpace, Inc., and Meetup.com, Ledbetter v. Wal-Mart Stores, Inc., No. 06-cv-01958-WYD-MJW, 2009 WL 1067018, at *2 (D. Colo. Apr. 21, 2009).

12. *See* Ramsay v. Bailey, 531 F.2d 706, 707 (5th Cir. 1976).

13. Samantha L. Millier, Note, *The Facebook Frontier: Responding to the Changing Face of Privacy on the Internet*, 97 KY. L.J. 541, 542 (2009).

14. *See* Seth P. Berman et al., *Web 2.0: What's Evidence Between "Friends"?*, 53 BOSTON BAR J. 5, 6 (2009) ("Web 2.0 applications may record people's thought processes and impressions in unguarded moments, exactly the sort of evidence that can be invaluable during litigation.").

15. *See generally* Facebook, Privacy Policy, http://www.facebook.com/policy.php (last visited May 27, 2010).

communications, Part III will propose a test that weighs the user's subjective and objective expectation of privacy against the relevance of the material to the litigation. This section will survey disparate judicial treatments of the issue in the United States, which will demonstrate the need for a uniform approach. This approach will borrow from the opinions of several Canadian courts which, largely unnoticed in the United States, have developed sophisticated thinking on this issue. This section outlines some of the challenges currently facing courts that have led to different rulings and concludes that a uniform approach would promote predictability in litigation.

II. BACKGROUND

A. Overview of General E-Discovery Issues

In 1970, the Advisory Committee for the Federal Rules of Civil Procedure noted that revisions to the rules would be needed to keep pace with technological development.[16] In response to these concerns, the 1970 amendments included "data compilations" as a subset of discoverable documents.[17] It was not until 2006 that electronically stored information, or ESI, became a distinct category of discoverable information under Rule 34.[18] The unprecedented rise of technology during that thirty-six-year period likely influenced the Advisory Committee to note in 2006 that the amended rule "covers—either as documents or as electronically stored information—information 'stored in any medium' to encompass future developments in computer technology."[19]

This changing landscape of technology has presented a host of difficult questions for courts. In civil litigation, e-discovery has made the pretrial stage of many lawsuits more costly and perplexing for corporations.[20] In lawsuits between individuals and corporations, there has always been an inherent danger of litigation gamesmanship. Before e-discovery, companies could respond to an individual's discovery requests by "hiding the ball"—the pertinent information being sought—

16. Daniel B. Garrie & Yoav M. Griver, *Mobile Messaging and Electronic Discovery*, 8 LOY. L. & TECH. ANN. 95, 103 (2009) (citing *Proposed Amendments to the Federal Rules of Civil Procedure Relating to Discovery*, 48 F.R.D. 487, 527 (1970)).

17. *See* FED. R. CIV. P. 34 (1970) (modified 2006).

18. FED. R. CIV. P. 34.

19. *Id.* at note subdiv. (a).

20. *See* Thomas C. Tew, *Electronic Discovery Misconduct in Litigation: Letting the Punishment Fit the Crime*, 61 U. MIAMI L. REV. 289, 293–94 (2007).

in a mountain of paper documents. The dawn of e-discovery acted as an equalizer of sorts; even a modest small business can cheaply store the equivalent of 2000 four-drawer file cabinets in electronic form.[21] This made it easier for one party to serve a sweeping Rule 34 document request that might cost the requesting party "one-half hour at the word processor" while the responding party is hit with "a copying bill with more zeros than hit Pearl Harbor."[22]

Even before the start of litigation, there is a duty to preserve documents that a party knows or should know may be relevant to future litigation.[23] This duty extends to preservation of relevant documents that are "reasonably likely to be requested during discovery and/or is the subject of a pending discovery request."[24] The court may impose sanctions on a party that engages in spoliation of relevant documents.[25] "Spoliation is 'the destruction or significant alteration of evidence, or the failure to preserve property for another's use as evidence in pending or reasonably foreseeable litigation.'"[26] In the seminal e-discovery cases of *Zubulake v. UBS Warburg LLC*, best known for the judge's "cost-shifting" analysis factors, the court held that the duty to preserve evidence attaches, at the latest, on the date an action is filed.[27] In *Zubulake IV*, Judge Scheindlin wrote that this duty may attach "at the time that litigation [is] reasonably anticipated" if a party has reason to suspect a pending suit.[28] Circumstantial evidence such as deposition testimony or exchanges of communication about the relevant events may give rise to a reasonable expectation of pending litigation.[29]

---

21. John S. Wilson, Comment, *MySpace, Your Space, or Our Space? New Frontiers in Electronic Evidence*, 86 OR. L. REV. 1201, 1206 (2007) (citation omitted).

22. Tew, *supra* note 20, at 293–94 (quoting Jerold Solovy & Robert Byman, *There Ought to Be a Law*, NAT'L L.J., Jan. 27, 2003, at B6).

23. Silvestri v. Gen. Motors Corp., 271 F.3d 583, 591 (4th Cir. 2001) ("The duty to preserve material evidence arises not only during litigation but also extends to that period before the litigation when a party reasonably should know that the evidence may be relevant to anticipated litigation." (citing Kronisch v. United States, 150 F.3d 112, 126 (2d Cir. 1998))); Zubulake v. UBS Warburg LLC ("*Zubulake IV*"), 220 F.R.D. 212, 216 (S.D.N.Y. 2003) ("'The obligation to preserve evidence arises when the party has notice that the evidence is relevant to litigation or when a party should have known that the evidence may be relevant to future litigation.'" (quoting Fujitsu Ltd. v. Fed. Express Corp., 247 F.3d 423, 436 (2d Cir. 2001))).

24. Turner v. Hudson Transit Lines, Inc., 142 F.R.D. 68, 72 (S.D.N.Y. 1991).

25. *See id.* at 72 (imposing sanctions on company for destruction of maintenance records after a bus accident).

26. *Zubulake IV*, 220 F.R.D. at 216 (quoting West v. Goodyear Tire & Rubber Co., 167 F.3d 776, 779 (2d Cir. 1999)).

27. *Id.*

28. *Id.* at 216–17.

29. *See id.* (employees' exchange of e-mails about the need to fire the plaintiff made it reasonable for the company to expect litigation).

Before ESI was formally added to the Federal Rules, the prevailing view among judges was that the rules for discovery of physical documents could be applied to e-discovery.[30] The drafters of the 2006 amendments to the Federal Rules, clearly anticipating further technological innovation, disagreed. The Committee "recogniz[ed] that the traditional rules were incompatible with new technologies" when it set out to determine what changes would be necessary to address differences between conventional discovery and e-discovery.[31] When the rules were amended in 2006, the new language addressing e-discovery was broad: a party may request any relevant ESI within another party's "possession, custody, or control" that is "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."[32] The 2006 amendments are broad enough to permit judges to rule on discoverability of electronic information "stored in any medium," which clearly encompasses social-networking information.

More recently, a drafter of the Federal Rules of Civil Procedure predicted that e-discovery "may become more democratic" because corporations are no longer the sole provinces of vast data storage, and individual litigants risk the same problems with preservation and access to electronic information.[33] "One-way discovery," typified by the discovery requests served on the defendant in *Zubulake IV*,[34] may give way to "headaches for parties on both sides of the 'v.'" as individuals amass more potentially discoverable data on hard drives, e-mail servers, and social networks.[35] Just ten years ago, one trial court decried Internet data as "voodoo information."[36] Now it seems poised to take center stage in all manner of discovery disputes.

30. Wilson, *supra* note 21, at 1216.

31. *Id.* at 1217.

32. FED. R. CIV. P. 34(a)(1)(A).

33. Richard L. Marcus, *E-Discovery Beyond the Federal Rules*, 37 U. BALT. L. REV. 321, 344 (2008).

34. *Zubulake IV*, 220 F.R.D. at 215.

35. Marcus, *supra* note 33, at 344; *see also* Zubulake v. UBS Warburg LLC ("*Zubulake I*"), 217 F.R.D. 309, 321 (S.D.N.Y. 2003).

36. Carole Levitt & Mark Rosch, *Making Internet Searches Part of Due Diligence*, 29 L.A. LAW. 46, 46 (Feb. 2007) (quoting St. Clair v. Johnny's Oyster & Shrimp, 76 F. Supp. 2d 773, 775 (S.D. Tex. 1999)).

B. Explosion of Social-Networking Sites

Social-networking sites have been defined 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."[37] This 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.[38]

Tens of millions of Americans are members of social-networking websites. These sites facilitate online connections with current and former friends, classmates, and coworkers.[39] The most popular site, Facebook, claims to have four hundred million active users worldwide, half of whom visit the site on any given day.[40] The social-networking phenomenon got its start with younger generations. Just a year after it launched, Facebook claimed as members eighty-five percent of the enrolled students at 882 colleges nationwide.[41] But thirty-five and older is now the fastest-growing demographic.[42]

Today's most popular social-networking sites can be traced to forerunners from the late 1990s.[43] Sites such as LiveJournal and Friendster earned the earliest press coverage, but the two sites discussed in this Comment, Facebook and MySpace, quickly overtook the competition to become the behemoths of the industry they are today. These sites are hardly interchangeable: MySpace has always allowed anyone to join and create a profile, but Facebook originally was created for university students to connect with each other.[44] Many of the differences between the sites are aesthetic; Facebook remains slavishly

---

37. James Grimmelmann, *Saving Facebook*, 94 IOWA L. REV. 1137, 1142 (2009) (quoting Danah M. Boyd & Nicole B. Ellison, *Social Network Sites: Definition, History, and Scholarship*, J. COMPUTER-MEDIATED COMM. 13(1), art. 11 (2007), http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html).

38. *Id.* at 1143.

39. *See* Pamela D. Pengelley & Cozen O'Connor, *Fessing Up to Facebook: Recent Trends in the Use of Social Network Websites for Insurance Litigation*, Mar. 3, 2009, at 3, *available at* http://ssrn.com/abstract=1352670.

40. Facebook, Statistics, http://www.facebook.com/press/info.php?statistics (last visited Mar. 3, 2010).

41. Grimmelmann, *supra* note 37, at 1144.

42. John C. Abell, *Facebook* is *Your Father's (and Mother's) Social Network*, WIRED, Mar. 26, 2009, http://www.wired.com/epicenter/2009/03/facebook-isyour/.

43. Grimmelmann, *supra* note 37, at 1144.

44. *Id.* at 1144–45, 1148.

devoted to a clean interface, while MySpace has always allowed its users to radically depart from a traditional profile scheme.[45] Despite the differences, both sites enable users to craft an online identity, establish relationships with other users, and be a part of numerous communities.[46]

In the most basic sense, online social networking is a technological retooling of the social structures that community members have always used to communicate with each other.[47] These sites allow users to connect with existing personal friends, reconnect with old ones, or expand their networks by joining groups based around common interests.[48] New users can join the site in a matter of minutes by setting up a personal profile. User profiles may include biographical information, a relationship status, educational background, hobbies, and interests.[49] Most users also choose to upload photos of themselves and others and make these photos viewable by the "friends" they elect to add to their networks,[50] although some users will allow anyone with a member profile to access all of their content.[51]

On Facebook or MySpace, when a user wants to connect directly with another individual user, the user may request to be added to the other user's group of "friends." Most communication on these sites occurs between users who are connected in this way, although users can send private messages to other users with whom they do not share a formal connection. The average Facebook user has 130 friends on the site,[52] but many users have friends numbering in the thousands. Importantly, the default privacy settings on both sites limit the profile content accessible to users who have not made this deliberate connection.

Facebook, unlike MySpace, is structured around networks of users. Network associations make it easier for a new user to find others who attend the same school or work for the same company. While the network structure originally facilitated interaction among college students, Facebook soon added networks for high schools, employers, and geographic regions. Networks were designed to form groups of people who shared something in common, but many geographic regional

45. *Id.* at 1148–49.

46. *See id.* at 1148.

47. Wilson, *supra* note 21, at 1220.

48. *Id.*

49. Millier, *supra* note 13, at 544.

50. The term "friend" in the social-networking context means a person with whom an individual has acknowledged a connection.

51. Millier, *supra* note 13, at 544.

52. Facebook, Statistics, *supra* note 40.

networks grew to have millions of members.[53] The site removed regional networks in late 2009, noting that their tremendous size made it "no longer the best way for [users] to control [their] privacy."[54]

C. Potential Legal Issues Involving Social-Networking Sites

While online social networking is nothing new, its legal ramifications are just beginning to come into focus. Facebook is only five years old, and the site's popularity outside of universities is even younger. More established sites like MySpace and Friendster have not been around much longer.[55] But as these sites become more entrenched in the lives of Americans of all ages, they are beginning to assume a central role in the daily interactions of their users. It is likely that the average civil litigant not only uses social-networking sites, but also does so on a daily basis.[56] At the same time, the common stereotype of lawyers as technophobes is beginning to give way as older generations of attorneys join their younger counterparts online.[57] As attorneys join social networks themselves, there is a growing awareness of the potential pitfalls—and gold mines—to be found on these sites.[58] In civil lawsuits for damages, especially in the personal injury and insurance litigation context, potentially relevant and discoverable information is often abundant on these sites.

Over the past decade, the Internet user experience has transformed from simple information gathering to interactive content creation.[59] A new generation of users is more engaged with the Internet than ever before; they collaborate with like-minded strangers on Wikipedia entries,[60] publish their every thought and action on Twitter,[61] and connect

53. An Open Letter from Facebook Founder Mark Zuckerberg (Dec. 1, 2009), http://blog.facebook.com/blog.php?post=190423927130 (last visited Feb. 27, 2010).

54. *Id.*

55. MySpace was launched in 2004. MySpace, http://www.myspace.com/pressroom?url=/fact+sheet/ (last visited Feb. 27, 2010). Friendster was founded in 2002. Wikipedia, http://en.wikipedia.org/wiki/Friendster (last visited Feb. 27, 2010).

56. Facebook, Statistics, *supra* note 40 (stating that fifty percent of active users use the site on any given day).

57. Christopher Danzig, *Law 2.0: New Web Tools Help In-House Counsel Collaborate, But They Aren't Perfect*, INSIDE COUNSEL, Aug. 2009, 44, 44 (citing a 2009 survey by LexisNexis finding seventy-one percent of corporate counsel were part of social networks such as Facebook or LinkedIn).

58. Silvia Hsieh, *Divorce Attorneys Are Missing Evidence on Social Media Sites*, MINN. LAW., July 6, 2009, at 5 (describing the use of social-networking information in divorce cases).

59. Berman et al., *supra* note 14, at 5.

60. Wikipedia, http://www.wikipedia.org.

61. Twitter, http://www.twitter.com.

with old classmates and near-strangers on Facebook. All of this adds up to a deluge of personal information that is publicly disclosed. According to Facebook, its users collectively update their "status" messages—brief text messages used to quickly share new information with friends—at least sixty million times every day.[62] Recognizing the potential for far-reaching impact of such constant publicity, President Obama offered "practical political advice" to a group of high school students "'to be careful about what you post on Facebook, because in the YouTube age whatever you do, it will be pulled up again later somewhere in your life.'"[63]

One article refers to social networks as "a virtual information bonanza about a litigant's private life and state of mind."[64] In family law cases, for example, web-savvy attorneys may search a parent's Facebook profile for status updates or photos of a trip with a child to Disney World while the parent was restrained from taking the child out of the state.[65] In personal injury cases, like Jerry's, defense attorneys and insurance claims adjusters search Facebook, Twitter, and other interactive "Web 2.0" sites as a part of routine due diligence.[66] In the employment law arena, where human resources officers have for years made a practice of investigating potential new hires on the Internet, there have been several recent cases of "Facebook firings," such as a group of airline employees who made "references to jet engines and hygiene on aircraft" in a Facebook discussion.[67] Even the field of legal ethics and professional responsibility is atwitter, in the conventional sense, with questions about online attorney misconduct—from "friending" adverse parties in litigation,[68] to posting indiscreet opinions about judges to blogs.[69]

---

62. Facebook, Statistics, *supra* note 40.

63. Julianna Goldman & Kate Andersen Brower, *Obama's Advice to Aspiring Politicians: Be Careful on Facebook*, BLOOMBERG, Sept. 8, 2009, http://www.bloomberg.com/apps/news?pid=newsarchive&sid=aL6GJ25zYajY.

64. Ronald J. Levine & Susan L. Swatski-Lebson, *Whose Space? Discovery of Social Networking Web Sites*, PROD. LIAB. L. & STRATEGY (L.J. Newsl., New York, N.Y.), Nov. 2008, at 7, 11.

65. Hsieh, *supra* note 58, at 5.

66. Pengelley, *supra* note 39, at 3–4, 7–8; *see also supra* Part I.

67. Simon Thiel, *Virgin Atlantic Fires 13 Cabin Crew Following Facebook Comments*, BLOOMBERG, Nov. 1, 2008, http://www.bloomberg.com/apps/news?pid=newsarchive&sid=aObNS7eFKlUY.

68. Pengelley, *supra* note 39, at 8; *see also* PHILA. BAR ASS'N ETHICS OP. 2009-02, *available at* http://www.philadelphiabar.org/WebObjects/PBAReadOnly.woa/Contents/WebServerResources/CMSResources/Opinion_2009-2.pdf (March 2009) (discussing ethical propriety of an attorney using third parties to gain access to an adverse party's limited-access profile information).

69. John Schwartz, *A Legal Battle: Online Attitude vs. Rules of the Bar*, N.Y. TIMES, Sept. 12, 2009, at A1.

D. Privacy Controls and the User's Expectation of Privacy: Just Me and My 200 Million Friends

The types of information found on social-networking sites can be divided into three categories based on the level of public disclosure. First, public social-networking information may include any text or media that is available to the general public. Second, semi-private information includes content that is restricted to either a self-selected group of "friends" or a wider, unmanageable group of "friends of friends." Third, private information includes instant messages and user-to-user messages (essentially e-mails). It is generally up to the user to define the size and character of the group with access to a given set of data, such as a photo album, political and religious views, or contact information. Some of this data, such as a user's hometown or favorite quotes, can be more strictly controlled because it is solely associated with one user's profile. Other information, such as a group photo containing tags to several users, is associated with multiple profiles and can be more problematic.

Social-networking sites, by their very nature, involve the sharing of personal information.[70] Facebook's privacy policy makes clear that any information entered on the website could become public.[71] It states:

> We designed our privacy settings to enable you to control how you share your information on Facebook. . . . Here are some things to remember:
>
> . . . .
>
> - Certain categories of information such as your name, profile photo, list of friends and pages you are a fan of, gender, geographic region, and networks you belong to are considered publicly available, and therefore do not have privacy settings. You can limit the ability of others to find this information on third party search engines through your search privacy settings.[72]

The policy explains that such personal information may become public only in limited circumstances when the site decides sharing the information is legally required, permitted by the user, or "reasonably

---

70. Benita P. Collier, *Privacy on the Internet: What is Reasonable in a Wired World?*, 53 PRAC. LAW. 17, 22 (2007).

71. Facebook, Privacy Policy, *supra* note 15.

72. *Id.*

necessary to offer [the] service[]."[73] 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.[74]

Facebook's "Subpoena/Search Warrant Guidelines" describes the procedure for "law enforcement or legal counsel" requesting information about users from Facebook.[75] The company may provide a "Neoprint," which it describes as "an expanded view of a given user profile," in response to a subpoena.[76] 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."[77] These subpoena guidelines and the privacy policy are unclear as to how Facebook determines the level of data disclosure.

Social networking sites may not be so quick to grant access to the "information bonanza" under their control. Mark Howitson, Deputy General Counsel at Facebook, reportedly said that Facebook receives almost daily requests for user information from law enforcement and legal counsel.[78] According to one report of the conference, Howitson said Facebook "'[doesn't] want to have to deal with these requests,'" and "will only provide basic subscriber information unless that user gives his or her consent."[79] Citing privacy grounds, Facebook recently fought off a subpoena from an employer requesting information about a former employee with pending disability claims.[80] The company appears eager for a federal court to determine what information it can be compelled to disclose in response to subpoenas.[81]

Despite its customizable privacy settings, Facebook photos are organized and cataloged in a way that may allow unknown third parties

---

73. *Id.*

74. *Id.*

75. Posting of Preston Gralla to COMPUTER WORLD Blog, *Leaked intelligence documents: Here's what Facebook and Comcast will tell the police about you*, http://blogs.computerworld.com/15667/leaked_intelligence_documents_heres_what_facebook_and_comcast_will_tell_the_police_about_you (Mar. 1, 201, 10:53).

76. *Id.*

77. *Id.*

78. Amy Miller, *Facebook GC Tells Lawyers He's Looking for a Fight*, CORPORATE COUNSEL, Feb. 2, 2010, *available at* http://www.law.com/jsp/article.jsp?id=1202441887703&rss=newswire.

79. *Id.*

80. *Id.*; Declan McCullagh, *Facebook fights Virginia's demand for user data*, CNET NEWS, Sept. 14, 2009, http://news.cnet.com/8301-13578_3-10352587-38.html.

81. *See* Miller, *supra* note 78.

to view photos of a person who has restricted privacy settings.[82] For example, photo tagging is a popular feature that allows users to identify themselves or other members of the site by name in photos. A photo tag creates a link to that user's profile and identifies the person and her specific location in the photo.[83] 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.[84]

III. ANALYSIS

The convergence of social-networking sites and litigation presents a host of complex questions implicating user privacy. This Comment addresses three issues in particular. First, how can a court determine whether there is relevant information contained within a party's private social-networking profiles beyond relying on the requesting party's good-faith assertions? Second, a user who implements Facebook's privacy settings may have a higher expectation of privacy than a user who grants unfettered access to hundreds or even thousands of "friends," and users may expect more privacy with regard to some types of information. How can these expectations be measured for objectivity or reasonableness? Third, the complex interconnectedness of social-networking sites presents difficult questions surrounding the expectation of privacy in relevant content posted by third parties. When a user is tagged in a third party's photo and that photo is relevant, is the photo discoverable? While American courts have only scratched the surface of these issues, Canadian appellate courts have fashioned a workable approach that merits consideration. The varying judicial approaches to this type of discovery will be scrutinized in the context of these three primary issues.

A. Managing Discovery Requests for Private Social-Networking Information

When a profile is set to private, the requesting party can only guess as to the likely contents of the profile—usually based upon limited biographical information and a single, thumbnail-sized photo that most users post to enable non-friends to identify the account holder. A

82. *See* Millier, *supra* note 13, at 544 (describing the organizational system used for cataloging Facebook photos).

83. *Id.*

84. *Id.*

discovery request based solely on the existence of a Facebook or MySpace profile, without more, risks rejection as a "fishing expedition."

The most complete discussion by an American court on this problem appears in *Mackelprang v. Fidelity National Title Agency of Nevada, Inc.*[85] In *Mackelprang*, the court denied the defendant's motion to compel the plaintiff in a sexual harassment lawsuit to consent to the release of her private MySpace messages.[86] The defendant employer initially issued a subpoena to MySpace to learn the profile information and identity behind two accounts that it suspected belonged to the former employee.[87] The employer alleged that the former employee set up dual identities on MySpace, with one account listing her as single with no interest in children and the other listing her as married with six children.[88] The employer believed the plaintiff used the first account to send e-mails of a sexual nature to colleagues she accused of sexual harassment.[89] MySpace produced some "public" information associated with the account, but it declined to provide any private messages absent a search warrant or a letter of consent from the account holder.[90] The company complied with the defendant's subpoena *duces tecum* by providing a spreadsheet that confirmed the plaintiff as the user for two accounts on the site.[91] In other cases, MySpace has declined to provide substantive user content in response to subpoenas.[92] In its motion to compel the plaintiff to consent to a release of her MySpace communications, the defendant argued that the private messages could contain evidence that the plaintiff exchanged consensual, sexually charged e-mails with members of the site.[93] The court agreed with the plaintiff that the request amounted to a "fishing expedition" that "would allow Defendants to cast too wide a net for any information that might be

85. No. 2:06-cv-00788-JCM-GWF, 2007 WL 119149 (D. Nev. Jan. 9, 2007).

86. *Id.* at **2, 9.

87. *Id.* at *2.

88. *Id.*

89. *Id.* at *3.

90. *Id.* at *2.

91. Mackelprang v. Fidelity Nat'l Title Agency of Nev., Inc., No. CV-S-00788-JCM-GWF, 2006 U.S. Dist. Ct. Motions LEXIS 29842, at *3 (D. Nev. filed Nov. 27, 2006).

92. *See* Jessica C. Collier, *The Necessity, Reliability, and Admissibility of Informal Internet Research*, STRICTLY SPEAKING: DRI NEWSLETTER, Summer 2009, http://www.dri.org/ContentDirectory/Public/Newsletters/0200/2009%20Product%20Liability%20Committee%20Strictly%20Speaking%20Summer.pdf (discussing how courts have treated various social-networking discovery issues).

93. *Mackelprang*, 2007 WL 119149, at *3.

relevant and discoverable" and could result in discovery of irrelevant private communications.[94]

But the court invited a more narrowly tailored request, noting that the "proper method" would be to serve the plaintiff with "limited requests for production of *relevant* email communications[,]" including MySpace "private messages that contain information regarding her sexual harassment allegations in this lawsuit or which discuss her alleged emotional distress and the cause(s) thereof."[95] The court invited the defendant to provide "some basis, beyond mere speculation, to support a reasonable belief that Plaintiff engaged in sexually [sic] email communications on her Myspace.com accounts with former co-employees" to warrant reconsideration of the motion.[96] The court denied the defendant's motion without prejudice, leaving the door open for more targeted discovery.[97]

Two recent trial orders involving suits against schools demonstrate the wide usage of Facebook among young people and the potential for relevance to litigation. The procedure followed in *Bass v. Miss Porter's School*[98] illustrates a "best practice" for handling Facebook discovery requests. In *Bass*, the defendant school requested production of any text messages or Facebook content related to the teasing and taunting of the plaintiff, a student at the school, or any content related to communications involving the student's allegations.[99] The student, who had since lost access to her Facebook account, served a subpoena on Facebook to obtain content from her former profile to comply with the school's request.[100] When Facebook agreed to provide "reasonably available data" spanning the pertinent time period, the judge ordered the student to provide any *responsive* documents to the school and the entire set of documents "to the Court for *in camera* review . . . distinguishing the subset of documents provided to Defendants."[101] The student provided approximately one hundred pages of content in response to the school's request, and she provided "more than 750 pages of wall postings, messages, and pictures" to the court, which represented Facebook's complete production in response to the subpoena.[102] The

94. *Id.* at **2, 7.
95. *Id.* at *8.
96. *Id.* at *6 n.1.
97. *Id.* at *9.
98. No. 3:08cv1807 (JBA), 2009 U.S. Dist. LEXIS 99916 (D. Conn. Oct. 27, 2009).
99. *Id.* at *1.
100. *Id.* at *2.
101. *Id.* at **2–3.
102. *Id.* at *3.

court determined that there was "no meaningful distinction" between the documents the student provided to the school and those provided for *in camera* review.[103] The court ordered that the entire set of documents be made available to the school because relevance was "more in the eye of the beholder than subject to strict legal demarcations," and the student could not unilaterally determine which documents might be "'reasonably calculated to lead to the discovery of admissible evidence.'"[104]

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.[105] The school attempted discovery of the plaintiff's private Facebook and MySpace pages to show evidence of her mental state before and after the incident.[106] The student moved for a protective order for her private profile information, citing privacy rights and undue burden.[107] The trial judge granted the protective order "barring the defendants from seeking or obtaining any discovery or information" from the plaintiff's online profiles.[108] The court left the door open for later discovery if the school could make a particularized showing of relevance.[109]

The *Bass* court's creative solution to the defendant's discovery request indicates both fidelity to the liberal discovery regime under the Federal Rules and an open-mindedness about the potential relevance of social-networking information. By way of contrast under similar facts, the state trial court in *T.V.* required an up-front showing of relevance by the requesting party. The *Bass* approach of serving a subpoena on the social-networking site and requiring *in camera* review of all supplied documents removes the possibility that a responding party will selectively remove damaging photos or status updates from the discoverable documents. This approach also permits a responding party to file protective orders for certain documents after they are provided by the social-networking site but before they are given to the requesting party. It is sufficiently flexible to ensure that all relevant social-networking content is discovered while creating a safety valve to prevent especially private or prejudicial information from being discovered.

---

103. *Id.*

104. *Id.* at *4.

105. T.V. v. Union Twp. Bd. of Educ., No. UNN-L-4479-04 (N.J. Super. Ct. June 8, 2007) (unpublished disposition).

106. *See Discovery of Assault Victim's MySpace, Facebook Postings Denied*, 3-12 MEALEY'S PRIVACY REP. 6 (2007) [hereinafter *Discovery Denied*].

107. *See id.*

108. *T.V.*, No. UNN-L-4479-04.

109. *See Discovery Denied*, *supra* note 106.

While these and other American courts have wrestled with the issue of social-networking discovery, no published opinion to date has suggested a workable approach to social-networking discovery requests. In contrast, several Canadian appellate cases have given in-depth treatment to the discovery of social-networking information in civil cases and have provided a roadmap for trial judges to use. One of the most thorough discussions appears in *Leduc v. Roman*, a recent Canadian personal injury case.[110] In *Leduc*, the plaintiff claimed damages for physical and mental injuries sustained after a traffic accident with the defendant.[111] The defendant moved for production of the entire contents of the plaintiff's private Facebook profile on the basis of a single, publicly accessible profile photo and identifying information on the plaintiff's public Facebook page.[112] After a lower court denied the request, the appellate court reversed in part, reasoning that the private profile "likely contain[ed] some content relevant to the issue of how Mr. Leduc has been able to lead his life since the accident."[113]

The court referenced recent cases holding that a Facebook profile may contain documents relevant to the issues:

> Photographs of parties posted to their Facebook profiles have been admitted as evidence relevant to demonstrating a party's ability to engage in sports and other recreational activities where the plaintiff has put his enjoyment of life or ability to work in issue . . . . In one case the discovery of photographs of a party posted on a MySpace webpage formed the basis for a request to produce additional photographs not posted on the site . . . .[114]

The *Leduc* court also considered the socialization purpose of Facebook, noting that "Facebook is not used as a means by which account holders carry on monologues with themselves . . . [and] Facebook profiles are not designed to function as diaries."[115] The court aptly described the goal of social-networking sites to "enable users to construct personal networks or communities of 'friends' with whom they can share information about themselves, and on which 'friends' can post information about the user."[116] The court explained that Facebook

110. Leduc v. Roman, No. 06-CV-3054666PD3, [2009] O.J. No. 681, at *6 (O.S.C.J. Feb. 20, 2009).

111. *Id.*

112. *Id.* at *7.

113. *Id.* at *22.

114. *Id.* at *16 (internal citations omitted).

115. *Id.* at *21.

116. *Id.*

profiles are "'data and information in electronic form' producible as 'documents' under the *Rules of Civil Procedure*,"[117] and as such, should be disclosed when "relevant to the allegations in the pleadings."[118] Perhaps most importantly, *Leduc* dismissed the idea that public and semi-private profile contents should be treated differently: "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 an action."[119]

Leduc correctly recognized that social-networking information provides a wealth of relevant information about a plaintiff's condition before and after an accident in the personal injury litigation context. But despite the court's characterization of the social purpose of Facebook, it had to tackle the issue of the plaintiff's expectation of privacy in some of the information. The *Leduc* court dismissed these concerns rather summarily,[120] but other courts have struggled with the expectations of privacy in various forms of social-networking content.

B. Accounting for Differing Expectations of Privacy

Many users of social-networking sites have hundreds or even thousands of friends who can view their full profiles. Tom Anderson, a co-founder of MySpace, has more than 200 million "friends."[121] Ashton Kutcher, an actor, claims nearly four million "followers" on Twitter.[122] These celebrity users likely represent the most extreme levels of online social interaction, but users with far fewer "friends" or "followers" still share information broadly—and often with little regard for privacy. The type of information shared, the number of people with access, and any efforts to protect the information from wider disclosure may affect the reasonableness of a user's expectation of privacy in shared information.

A person who writes about her personal life or political convictions on a publicly available site, such as a blog or forum page, should understand that anyone with an Internet connection could access the

117. *Id.* at *19.

118. *Id.* at **19–20 (quoting CAN. R. CIV. P. 30.03(4)).

119. *Id.* at **21–22.

120. *See id.* at *24 ("To 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.").

121. Wilson, *supra* note 21, at 1220 n.90.

122. Ashton Kutcher's Twitter Page, http://twitter.com/APlusK (last visited Oct. 29, 2009).

content. In the traditional realm of privacy and tort law, personal information that is shared with others cannot be the subject of a privacy claim.[123] Cases involving public dissemination on the Internet apply the same rule.[124] For this reason, there is little doubt that a person cannot have an objectively reasonable expectation of privacy regarding information that is publicly available on the Internet.[125] This is true even when the person only expects a limited number of people to view the information.[126] Social-networking profiles that can be accessed by any registered site users—which, on Facebook, would be over 400 million people—are probably as discoverable as any other relevant Internet documents.[127] But a key difference between social-networking sites and other Internet resources, such as blogs or personal websites, is the user's ability to restrict access to certain profile information. This Comment addresses the more complicated question of whether limited-access social-networking information may be subject to civil discovery.

By limiting access to selected content, Facebook users may subjectively expect this content not to be shared beyond their group of friends. The sophisticated technical controls on Facebook likely encourage this privacy expectation. But this expectation is objectively unreasonable because other users can disseminate the content without obtaining consent from the user who posted it. This is analogous to the expectation of privacy in e-mail messages or mailed letters, which some courts have held terminates upon delivery of the correspondence.[128] Once content is shared with another user on Facebook, it can no longer be considered private. Under common law tort doctrine, some courts will not recognize a claim of invasion of privacy when the information at issue was known to the public or even "a small number of people who have a 'special relationship'" with the person.[129] In the social-networking context, this would seem to foreclose the possibility of

123. Collier, *supra* note 70, at 18 (citing Shulman v. Group W Prods., Inc., 955 P.2d 469 (Cal. 1998)).

124. Guest v. Leis, 255 F.3d 325, 333 (6th Cir. 2001) (no reasonable expectation of privacy in posts on password-protected bulletin board).

125. *See* Moreno v. Hanford Sentinel, Inc., 172 Cal. App. 4th 1125, 1130 (Cal. Ct. App. 2009) ("By posting the article on myspace.com, [the plaintiff] opened the article to the public at large. Her potential audience was vast.").

126. *Id.*

127. *See* Levine & Swatski-Lebson, *supra* note 64, at 8 (arguing that anyone who provides personal information on a social networking site "is not seeking to preserve this information as private, but rather is making a conscious choice to publicize it").

128. *See, e.g.*, *Guest*, 255 F.3d at 333.

129. *See, e.g.*, Cordts v. Chicago Tribune Co., 860 N.E.2d 444, 450–51 (Ill. App. Ct. 2006).

recognizing a right of privacy in content shared over the Internet with a group of online "friends."

Users of social-networking sites may have a subjective expectation of privacy in the information they associate with their online profiles. For purposes of discovery, courts normally focus on the objective expectation of privacy—whether a reasonable person would expect the information to remain private.[130] Courts have addressed the reasonableness of the expectation of privacy in online information in the context of online bulletin board posts, chat room conversations, and blog entries.[131] In *Guest v. Leis*, the Sixth Circuit held that a person who posts a message to an online bulletin board system—a predecessor to today's online forums that restrict access to registered users—has no reasonable expectation of privacy in the contents of the message.[132] Even though access to the bulletin board site was limited, the poster intended the information be published online for others to see.[133]

Any subjective expectation of privacy on Facebook or similar sites may be unreasonable because of the sites' inherent interconnectivity.[134] One commentator, James Grimmelmann, calls Facebook's privacy problems "Exhibit A for the surprising ineffectiveness of technical controls" because users choose socializing over maximizing privacy, thus negating the usefulness of the controls.[135] Grimmelmann argues that technical controls on socializing sites present "a deep, probably irreconcilable tension between the desire for reliable control over one's information and the desire for unplanned social interaction."[136] This tension is most often resolved in favor of socialization; one study found that nearly half of social-networking site users do not change the network's default privacy settings.[137] When users disclose personal information to even a small number of close friends on these sites, the information may be disseminated to an unlimited group of people if just one "friend" chooses to share it with a wider group.[138] Indeed, Facebook's privacy policy states that users should "understand that information might be re-shared or copied by other users."[139]

130. *Guest*, 255 F.3d at 333.
131. *See generally* Collier, *supra* note 70, at 17.
132. *Guest*, 255 F.3d at 333.
133. *Id.*
134. Collier, *supra* note 70, at 22.
135. Grimmelmann, *supra* note 37, at 1140.
136. *Id.* at 1185.
137. *Id.* (citation omitted).
138. *Id.* at 1186–87.
139. Facebook, Privacy Policy, *supra* note 15.

Facebook's customizable privacy settings allow users to restrict access to any component of their profile, and users can do so selectively for certain groups or individuals. Users also are able to share individual photo albums with particular friends or networks of friends—or selectively restrict individuals from viewing some or all photos. This high degree of control over access to personal content probably goes overlooked by most courts and even most lawyers. The savviest of Facebook users can practically fashion two identities from one profile by carefully determining which users could see certain photo albums and profile information. When Facebook introduced more sophisticated privacy controls in December 2009, the site prompted users to update privacy settings.[140] The site's "transition tool" set new privacy defaults for each type of content and permitted users to retain old settings or use the new defaults.[141] The new recommended settings opened up more personal information to wider audiences.[142] For example, users who accepted the new default privacy settings opened up access to their status updates and relationship status to everyone.[143]

Facebook makes clear to users that any information shared on the site may be publicly disclosed. Its privacy policy reminds users that the company "cannot control the actions of other users with whom you share your information" and "cannot ensure that information you share on Facebook will not become publicly available."[144] This language may be sufficiently clear to negate the reasonableness of any expectation of privacy in text or media uploaded to the site by the user. At the very least, however, it should render general profile content—such as biographical information, relationship status, and other textual content—discoverable if relevant. The most public information, such as the thumbnail-sized active profile photo that any visitor to the site can view, is inherently the least private information a user can post. As Facebook's privacy policy reminds users, "name, profile photo, list of friends and pages you are a fan of, gender, geographic region, and networks you belong to are considered publicly available to everyone, including Facebook-enhanced applications, and therefore do not have privacy settings."[145] This data is as accessible as any ordinary Internet site and

140. Sarah Perez, *The 3 Facebook Settings Every User Should Check Now*, N.Y. TIMES, Jan. 20, 2010, http://www.nytimes.com/external/readwriteweb/2010/01/20/20readwriteweb-the-3-facebook-settings-every-user-should-c-29287.html?em.

141. *Id.*

142. *Id.*

143. *Id.*

144. Facebook, Privacy Policy, *supra* note 15.

145. *See supra* note 72 and accompanying text.

can be found through search engines unless the user chooses to restrict search privacy settings.[146] Users who restrict search settings can be "invisible" to users they are not friends with, and it would be effectively impossible to find evidence of their Facebook presence without establishing a connection on the site.

The wide array of content available on social-networking sites has likely been a factor in the varying judicial approaches to social-networking discovery. *Mackelprang* involved discovery of private MySpace messages, which are tantamount to e-mail and therefore arguably are entitled to a higher degree of privacy than other profile information that the user expects multiple "friends" to see.[147] In a different case, *Ledbetter v. Wal-Mart Stores, Inc.*, messages posted on an access-controlled social-networking site were at the heart of a discovery dispute. Wal-Mart served subpoenas on Facebook, MySpace, and Meetup.com to discover information about Ledbetter, who alleged a host of physical and psychological injuries as a result of being injured at Wal-Mart.[148] The plaintiffs claimed that, if discovered, their profile contents should be inspected *in camera* because they were protected by physician-patient and spousal privileges.[149] Both of these privileges were deemed waived; the physician-patient privilege was waived upon the filing of the suit for mental and physical injuries, and the marital privilege was waived because the wife filed a loss of consortium claim, thus putting the marital relationship at issue.[150] Ledbetter moved for a protective order to prevent Wal-Mart from discovering the access-limited content of his social-networking profiles.[151] The court denied Ledbetter's motion for a protective order and determined that the information Wal-Mart requested was reasonably calculated to lead to discovery of admissible evidence.[152]

As demonstrated by the doppelganger accounts in *Mackelprang*,[153] social-networking sites lack meaningful controls to prevent users from falsifying information to mislead other users. Facebook has tried to reduce the likelihood of misrepresentation by maintaining a database of

146. Facebook, Privacy Policy, *supra* note 15.

147. *See supra* notes 85–97 and accompanying text.

148. Order Regarding Plaintiffs' Motion for Protective Order Pursuant to Fed. R. Civ. P. 26(c) Regarding Subpoenas Issued to Facebook, My Space, Inc., and Meetup.com, Ledbetter v. Wal-Mart Stores, Inc., No. 06-cv-01958-WYD-MJW, 2009 WL 1067018, at *1 (D. Colo. April 21, 2009).

149. *Id.* at *1.

150. *Id.*

151. *Id.*

152. *Id.* at *2.

153. *See supra* notes 88–89 and accompanying text.

names it believes users could employ to establish false identities.[154] For example, it is not possible to register an account under the name Bill Self, the head coach of the University of Kansas men's basketball team.[155] But for all practical purposes, anyone could create multiple identities on Facebook or any other social networking site simply by registering with the same name twice and maintaining separate groups of friends on each account. Misrepresentation is possible if a user were to register using someone else's name and post incriminating information.[156]

The private messaging function on Facebook is sufficiently similar to e-mail communications to apply the same jurisprudence. As with e-mail, the site's user-to-user interface allows messages to be sent to a single recipient or several recipients. While a private message between individual users should be entitled to a higher degree of privacy than profile content shared with multiple users, this privacy interest should be balanced against the relevance to the action and the requesting party's demonstrated need for the information.[157]

Instead of adopting ad hoc reasoning and balancing, American courts should look to the Canadian approach, typified by *Leduc v. Roman*, for an effective framework. *Leduc* correctly reasoned that the potential for withholding relevant information in a case is great because Facebook's privacy controls are so easily manipulable:

> To 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.[158]

A flexible yet predictable approach to social-networking discovery issues would relieve some of the uncertainty surrounding this issue. Any expectation of privacy in social-networking content, whether for a public

---

154. Justine Parker, *What's in a Facebook Name?*, BBC NEWS, Oct. 30, 2007, http://news.bbc.co.uk/2/hi/7067150.stm.

155. An attempt to register an account under this name returned this error message: "Our automated system will not approve this name. If you believe this is an error, please contact us."

156. Ethan J. Wall, *Social Networking Sites Look Like Plunder to Attorneys*, LAW.COM, Feb. 20, 2009, http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202428417060.

157. *See* S. Cal. Hous. Rights Ctr. v. Los Feliz Towers Homeowners Ass'n, No. CV 04-2716-CBM, 2005 U.S. Dist. LEXIS 41106 (C.D. Cal. Apr. 25, 2005) (ordering discovery of private information when the importance of the information to the plaintiff's claims outweighed privacy interests).

158. Leduc v. Roman, No. 06-CV-3054666PD3, [2009] O.J. No. 681, at *24 (O.S.C.J. Feb. 20, 2009).

profile or an access-limited profile, is probably unreasonable. At the same time, there is a high likelihood that much of a person's social-networking content will be irrelevant. The procedure proposed by the Canadian court in *Leduc* sufficiently addresses these competing concerns. That court proposed a three-step process, whereby the party with relevant, potentially discoverable content must preserve online data by printing it out, provide an affidavit of the relevant content, and "permit the opposite party to cross-examine on the affidavit of documents in order to ascertain what content is posted on the site."[159] The court in *Bass v. Miss Porter's School* slightly modified this process; the responding party provided all of her Facebook content to the court for *in camera* review, and the court determined that all of the content was discoverable.[160]

Leduc cited another Canadian personal injury case, *Murphy v. Perger*, for the proposition that the potential invasion of privacy in allowing discovery of access-limited Facebook photos was minimal because "[t]he plaintiff could not have a serious expectation of privacy given that 366 people have been granted access to the private site."[161] In *Murphy*, the court quoted an earlier case in consideration of the plaintiff's concern about the release of potentially embarrassing photos that others tagged her in:

> In considering whether to make an order compelling disclosure of private documents . . . the Court ought to ask itself whether the particular invasion of privacy is necessary to the proper administration of justice and, if so, whether some terms are appropriate to limit that invasion. . . .
>
> On the one hand, a person who has been injured by the tort or [sic] breach of fiduciary duty of another ought not to be driven from the judgment seat by fear of unwarranted disclosure a sort of blackmail by legal process. If such a thing were to happen, the injured person would be twice a victim.
>
> But, on the other hand, a defendant ought not to be deprived of an assessment of the loss he actually caused, founded on all relevant evidence. It would be as much a miscarriage of justice for him to be ordered to pay a million dollars when, if all the relevant evidence were before the court, the award would be for one-tenth that sum, as it would

159. *Id.* at *23.

160. Bass v. Miss Porter's Sch., No. 3:08cv1807 (JBA), 2009 U.S. Dist. LEXIS 99916, at **2–3 (D. Conn. Oct. 27, 2009).

161. *Leduc*, [2009] O.J. No. 681, at *18 (quoting Murphy v. Perger, No. 45623/04, [2007] O.J. No. 5511 (O.S.C.J. Oct. 3, 2007)).

> be for the injured person to feel compelled to retire from the field of battle because of a demand for documents containing intensely personal matters of little relevance.[162]

The *Murphy* court held that the plaintiff's private Facebook profile contents should be disclosed as documents related to matters in issue.[163]

Other Canadian courts have interpreted *Leduc* to require plaintiffs to preserve relevant photos and other information on social-networking sites and list this information as "relevant documents" in the affidavit of documents provided at the start of discovery.[164] In *Wice v. Dominion of Canada General Insurance Co.*, the defendant insurer sought a more comprehensive affidavit from the plaintiff to determine which Facebook information was relevant to the personal injury action.[165] In granting the motion for a revised affidavit, the court reasoned that the subject matter of the plaintiff's Facebook photos was likely relevant to his claims:

> The case at bar, while not a tort case, does raise the issue of Mr. Wice's ability to function—at least in certain defined circumstances. As I have already pointed out, his ability to function in a wide range of social situations may be circumstantial evidence from which a trier of fact could draw an inference about his ability to function in the defined circumstances in issue. The Defendant has produced evidence demonstrating that there are relevant photographs of the Plaintiff participating in social activities posted on his Facebook profile. The court may also infer from the nature of the Facebook service, that other relevant documents are likely included in the Plaintiff's profile.
>
> Accordingly, I order that the Plaintiff produce a further and better Affidavit of Documents within 30 days which is to include relevant documents contained in his Facebook account, or any other similar account.[166]

The court also ordered the plaintiff to "preserve any and all information and documentation in his Facebook account or other similar accounts for the duration of this litigation."[167]

---

162. *Murphy*, [2007] O.J. No. 5511, at **9–10 (quoting M.(A.) v. Ryan, [1994] 98 B.C.L.R.2d 1 (B.C.C.A.), *aff'd*, [1997] 1 S.C.R. 157 (Can.)).

163. *Id.* at *10.

164. *See* Wice v. Dominion of Can. Gen. Ins. Co., No. 06-0166, [2009] O.J. No. 2946, at **8–9 (O.S.C.J. July 6, 2009) (ordering the plaintiff to supplement his Affidavit of Documents with relevant documents from his social-networking accounts).

165. *Id.* at *7.

166. *Id.* at *9.

167. *Id.* at **9–10.

C. Discovery of Relevant Third-Party Content

Under the Federal Rules, a party may serve another party with a request for documents or ESI within the responding party's "possession, custody, or control."[168] 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.[169] 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. As such, any relevant content that a user could access on Facebook, regardless of the original uploading user, should be discoverable through a civil discovery request.

Third-party-generated content often may be relevant to an action. Take, for example, the common instance of a user who uploads photos from a house party to her access-limited Facebook profile. The user can tag someone who appears in a photo by indicating the portion of the photo where the person appears, and upon the tagged user's consent, a link will associate the user's name and profile with the photo. Depending on the user's privacy settings, the photo may be integrated seamlessly with the tagged user's profile as if the tagged user uploaded it personally. For purposes of discovery, it should not matter whether a party uploaded a photo directly or was tagged in a photo by a third party. In either case, the photo would be within the party's possession, custody, or control. The photo may remain under the control of the user who uploaded it—who alone has the ability to completely remove the photo from the site—but tagged users have the legal right to obtain access to the photo.

There are several safety valves associated with photo tagging. Once one user tags another in a photo, the tagged user has the option to remove her identity from the photo. When a user removes a tag, other users are prevented from tagging the same person again in that photo. The actual photo will remain on Facebook unless the uploading user removes it, but it will not appear in the formerly tagged user's list of photos. There is also a separate privacy setting for "Photos and Videos of Me" that allows

168. FED. R. CIV. P. 34(a)(1).

169. *See, e.g.*, Export-Import Bank of U.S. v. Asia Pulp & Paper Co., 233 F.R.D. 338, 341 (S.D.N.Y. 2005); *In re* Folding Carton Antitrust Litig., 76 F.R.D. 420, 423 (N.D. Ill. 1977).

a user to restrict access to tagged photos and videos to friends or friends of friends. This feature also permits users to exclude individual users from viewing this content.

Despite these disassociation measures, photos remain on the site unless the uploading user removes them. Even users with restrictive privacy settings who diligently remove tags will not be able to prevent other users' photos of them from being viewed by thousands of strangers.[170] One common problem occurs when one person in a group photo permits public, unrestricted access to her photos. Anyone on Facebook could view the group photo and the names of anyone tagged in the photo. Of course, it is possible for these tags to be incorrect. And, to be sure, users are notified when they are tagged in a photo so that they can remove the tag if they wish.

Facebook founder and CEO Mark Zuckerberg's public statements reveal the site's preference for openness. In December 2009, Zuckerberg said that social norms had evolved in the direction of sharing information "more openly and with more people."[171] He cited Facebook's recent decision to make key biographical information completely public by default as the company's recognition of this evolution.[172]

D. Discovery Mechanisms: Party Requests Versus Serving Social-Networking Sites with Subpoenas

The cases discussed in this Comment demonstrate that there are numerous approaches to discovering relevant social-networking content. In *Mackelprang* and *Ledbetter*, the defendants served subpoenas on the sites directly.[173] In *Bass*, the plaintiff served a subpoena on Facebook to respond to the defendant's discovery request.[174] In the Canadian cases, defendants requested that relevant social-networking content be included in an affidavit of documents.[175] The best approach for a litigant seeking discovery will depend on the information sought and the likelihood that a

170. Millier, *supra* note 13, at 542–43.

171. Posting of Ian Paul to Today@PCWorld, *Facebook CEO Challenges the Social Norm of Privacy*, http://www.pcworld.com/article/186584/facebook_ceo_challenges_the_social_norm_of_privacy.html (Jan. 11, 2010, 12:03).

172. *Id.*

173. *See* Mackelprang v. Fid. Nat'l Title Agency of Nev., Inc., No. 2:06-cv-00788-JCM-GWF, 2007 WL 119149, at *2 (D. Nev. Jan. 9, 2007); Ledbetter v. Wal-Mart Stores, Inc., No. 06-CV-01958-WYD-MJW, 2009 WL 1067018, at *1 (D. Colo. Apr. 21, 2009).

174. Bass v. Miss Porter's Sch., No. 3:08cv1807 (JBA), 2009 U.S. LEXIS 9916, at *2 (D. Conn. Oct. 27, 2009).

175. *See supra* notes 158–67 and accompanying text.

subpoena will result in production. A request for relevant documents from the user, coupled with a showing of relevance to the case, is most likely to succeed.

Courts may weigh the relative burden of a party request compared to a non-party subpoena in the Internet discovery context. In *Netbula, LLC v. Chordiant Software, Inc.*, the court granted the defendant's motion to compel discovery of the plaintiff's archived Web pages.[176] The old versions of some of the plaintiff's Web pages had been automatically archived by a Web-based data storage service called Internet Archive, which is also known as the Wayback Machine.[177] Internet Archive is a "'digital library' that provides access to archived websites and other artifacts."[178] The plaintiff argued that the copies of its old Web pages saved by Internet Archive were beyond its control and thus could not be provided in response to a Rule 34 document request.[179] The court disagreed, reasoning that the plaintiff had "a 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.[180] The court dismissed the plaintiff's argument that the information should be obtained by serving a subpoena directly on Internet Archive, a non-party.[181] While Internet Archive could access the data itself, this route involved "considerable burden, expense and disruption to its operations . . . whereas plaintiffs could permit access to the information in minutes and with minimal burden and expense."[182] In granting the defendant's motion to compel discovery, the court added that the plaintiffs had failed to "convincingly demonstrate[] that the burden and expense of the discovery sought outweighs its likely benefit."[183]

The *Netbula* facts can easily be analogized to a discovery dispute involving access to limited-access social-networking content. It is easier for a party to provide limited-access social-networking content directly than it would be for the sites to respond to a Rule 45 subpoena. If access to the content has been cut off, another approach is for the responding

176. Order (1) Vacating Motion Hearing; and (2) Granting Defendant's Motion to Compel, Netbula, LLC v. Chordiant Software, Inc., No. C08-00019 JW (HRL), 2009 WL 3352588, at *2 (N.D. Cal. Oct. 15, 2009).

177. *Id.* at *1.

178. *Id.*

179. *Id.*

180. *Id.* at **1–2.

181. *Id.* at *2.

182. *Id.* (citations omitted).

183. *Id.*

party to subpoena the social-networking site for the contents and provide the documents to the court for *in camera* review, as illustrated in *Bass*. Once relevance is established, courts are likely to employ the approach from *Netbula* or *Bass* and compel production of the social-networking content.

When private litigants serve subpoenas on companies operating social-networking sites, the sites face a difficult predicament. Facebook and MySpace, like Internet service providers (ISP), store vast quantities of personal information on their servers. Just like an ISP faced with a subpoena to produce e-mails, social-networking sites must determine how much and what types of information to disclose to comply with a subpoena.

It appears unlikely that MySpace and Facebook would divulge private content subject to a civil subpoena without the user's consent. The Stored Communications Act, which Congress passed in 1986 alongside the Electronic Communications Privacy Act, prohibits ISPs from voluntarily divulging a customer's private communications without the customer's consent.[184] There is an exception for voluntary disclosure of customer "records" or subscription information to third parties,[185] but ISPs cannot be required to produce private communications in response to civil discovery subpoenas issued under Rule 45.[186] Courts have applied this statute to refuse enforcement of civil subpoenas served on ISPs for customer information or private communications.[187]

In some cases, an overly broad subpoena may violate Rule 45's requirement that the issuing party "take reasonable steps to avoid imposing undue burden or expense on a person subject to the subpoena."[188] In *Theofel v. Farey-Jones*, the defendant company served a "patently unlawful" subpoena on an ISP requesting "all copies of emails sent or received by anyone" at the plaintiff's company, without

184. *See* 18 U.S.C. § 2702(c) (2008).

185. *Id.*

186. *See In re* Subpoena Duces Tecum to AOL, LLC, 550 F. Supp. 2d 606, 609 (E.D. Va. 2008) ("[T]he plain language of the [ECPA] prohibits AOL from producing the [non-party witnesses'] e-mails, and the issuance of a civil discovery subpoena is not an exception to the provisions of the Privacy Act that would allow an [I]nternet service provider to disclose the communications at issue here.").

187. *See id.* at 610 ("[The ECPA] creates a zone of privacy to protect [I]nternet subscribers from having their personal information wrongfully used and publicly disclosed by 'unauthorized private parties . . . .'"); O'Grady v. Superior Court, 44 Cal. Rptr. 3d 72, 76–77 (Cal. Ct. App. 2006) (noting that enforcement of a civil subpoena issued to an ISP is inconsistent with the ECPA, which prevents disclosure of e-mails by ISPs).

188. FED. R. CIV. P. 45(c)(1).

limits on time or scope.[189] Judge Alex Kozinski, writing for a Ninth Circuit panel, reversed the trial court's dismissal of the Stored Communications Act claim.[190] 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."[191] Because the overly broad subpoena "'transparently and egregiously' violated the Federal Rules," the ISP's sample production of e-mails—many of which were irrelevant, privileged, or personal—created a cognizable claim against the requesting parties under the Act.[192]

There do not appear to be any cases applying the Stored Communications Act or Electronic Communications Privacy Act to social-networking sites, but these statutes conceivably could apply to these companies if they disclosed substantive content from user profiles in response to a civil subpoena.[193] MySpace likely accounted for this possibility in *Mackelprang* when it provided limited identifying information about an account holder while refusing to produce the account holder's substantive content in response to a party's subpoena for private messages.[194]

Discovery requests should be narrowly tailored to ensure only relevant content is divulged. Trial courts should balance the requesting party's need for the content and its relevance to the action against the likelihood of undue burden on the adverse party. As illustrated in *Netbula*, courts should favor motions to compel discovery over subpoenas for online information from third parties whenever possible. While social-networking sites appear willing to divulge user content when subjected to discovery subpoenas, this avenue places an undue burden upon a non-party to disclose information that is readily available to a party. When a party fails to disclose relevant social-networking content in response to a Rule 34 document request, the proper recourse is a motion to compel.

189. 359 F.3d 1066, 1071 (9th Cir. 2004).

190. *Id.* at 1079.

191. *Id.* at 1072.

192. *Id.* at 1074–75.

193. Collier, *supra* note 70.

194. *See* Mackelprang v. Fid. Nat'l Title Agency of Nev., Inc., No. 2:06-cv-00788-JCM-GWF, 2007 WL 119149, at *2 (D. Nev. Jan. 9, 2007).

E. Competent Discovery Now Requires More Informal Internet Research

As demonstrated in the Introduction, even a cursory Internet search can reveal information—damaging or helpful—that is relevant to a case. Unlike limited-access social-networking content, content on blogs, forums, and personal websites are usually publicly accessible. Attorneys should recognize the vast potential for discoverable information on the Internet and conduct due diligence searches, both as a prerequisite to establishing a client relationship and at regular intervals during litigation.

An attorney who unearths damaging information about a potential client would be wise to consider declining or limiting the scope of any representation, especially when it is likely that opposing counsel will learn of its existence. If research uncovers useful information about an adverse party, proof of such information may be leveraged in settlement discussions, even if a court refuses discovery or introduction into evidence. And regardless of which side the information may help, any relevant Internet information should be carefully preserved to avoid spoliation issues.

Responsible, thorough Internet research on a client should begin with a Google search that utilizes related terms and connectors, such as a hometown, school, employer, or spouse's name to narrow results. Similar searches should be performed for co-parties, likely witnesses, close relatives, and former employers. Attorneys should also search Facebook, MySpace, Friendster, Orkut, and Hi5—all examples of social-networking sites—bearing in mind that the popularity of these sites will likely return multiple results for more common names. Any content that may be relevant should be requested as relevant documents in discovery. Any request should be coupled with a demand that the information be preserved in its current state.

IV. CONCLUSION

Social-networking sites play a central role in the daily lives of many people of all ages. As the sites' prominent position in society expands by the day, it is becoming increasingly clear that the technology is not just a fad. The relevant cases demonstrate that courts are grappling with complex questions of privacy and relevance. Litigants and their attorneys should be aware of the need to preserve potentially discoverable online content and disclose its existence in discovery. They should also identify potential sources of helpful information about an

adverse party and request disclosure of any relevant social-networking content.

In ruling on motions to compel and protective orders, courts should consider the purpose and organization of social-networking sites. The technology itself exists to share information with others, usually a select group of people, and this reduces or eliminates the reasonableness of any expectation of privacy in the information shared. Even so, the extensive use of these sites by many users makes it highly likely that an overbroad discovery order could lead to disclosure of irrelevant or prejudicial content. Discovery orders should be narrowly tailored to ensure only relevant content is produced. Most importantly, trial courts should play an active role in the process by closely monitoring the content of responsive documents and utilizing *in camera* review to relieve the responding party of the responsibility to determine what content is responsive to the request.