Washington Journal of Law, Technology & Arts

Volume 8 | Issue 2 Article 5

10-1-2012

Get Outta My Face[book]: The Discoverability of Social Networking Data and the Passwords Needed to Access Them

Mallory Allen

Aaron Orheim

WASHINGTON JOURNAL OF LAW, TECHNOLOGY & ARTS
VOLUME 8, ISSUE 2 FALL 2012

GET OUTTA MY FACE[BOOK]: THE DISCOVERABILITY OF SOCIAL NETWORKING DATA AND THE PASSWORDS NEEDED TO ACCESS THEM

Mallory Allen & Aaron Orheim[*]

Cite as: 8 WASH J.L. TECH. & ARTS 137 (2012)
http://digital.law.washington.edu/dspace-law/handle/1773.1/1172

ABSTRACT

Under what circumstances can a social network user be compelled to turn over his or her user identification and password in civil litigation? In three recent cases, courts attempted to answer this question with varied results. The New York Supreme Court Appellate Division refused to allow discovery of private Facebook information in McCann v. Harleysville Insurance Co. *because the discovery request was not sufficiently tailored to reach discoverable information. Soon thereafter, the same court allowed discovery of similar material in* Romano v. Steelcase, Inc. *based on the level of publicity of the social networking account. In* McMillen v. Hummingbird Speedway, Inc., *the Pennsylvania Court of Common Pleas allowed discovery of private Facebook information based upon similar considerations as the* Romano *court. The* McMillen *court questioned whether the plaintiff should be allowed to block discovery by asserting an evidentiary privilege and determined that no reasonable expectation of confidentiality exists on social networking sites. The court determined that as long as a person's social network sites*

* Mallory Allen, University of Washington School of Law, Class of 2012. Aaron Orheim, University of Washington School of Law, Class of 2013. Mallory and Aaron would like to thank Professor Robert W. Gomulkiewicz and Craig Ball for their helpful advice on this article.

contain information relevant to the lawsuit, courts should allow litigants to utilize "all rational means for ascertaining the truth." This Article first summarizes the potential bases to prohibit discovery of social networking information and communication. It then examines the recent case law and identifies the level of protection courts are willing to afford social networking communication and the login information needed to access them in civil discovery.

TABLE OF CONTENTS

INTRODUCTION

As the popularity of social networking sites continues to surge, civil litigants increasingly demand disclosure of online communications. Opponents of broad social networking discovery have asserted several arguments as to why social media information should be protected from discovery. First, such requests are not relevant under Federal Rules of Civil Procedure ("FRCP") 34 and 45 and therefore not discoverable. Second, social networking information should be protected by an evidentiary privilege—akin to attorney-client privilege or marital privileges—

and inaccessible by opposing counsel. Finally, litigants sometimes argue that the Fourth Amendment affords some protection from unreasonable intrusions into their privacy.

In analyzing whether to order disclosure of online communications, courts have not only considered the above arguments, but have also looked at the social networking sites' terms of service and privacy policies. Those policies are relevant in determining whether users have a reasonable expectation of privacy in their online communications. Ultimately, few courts find a reasonable expectation of privacy because many sites warn that most information is not private.

This Article first summarizes the varying bodies of law that courts have employed in determining when social networking information is discoverable. Next, this Article looks at three recent decisions that apply one or more of the above rationales and shed light on the discoverability of social networking data and the credentials—i.e., the usernames and passwords—needed to access that data: *McMillen v. Hummingbird Speedway, Inc.*, *Romano v. Steelcase, Inc.*, and *McCann v. Harleysville Insurance Co.*, all decided in 2010.

I. THE FEDERAL RULES OF EVIDENCE AND SOCIAL NETWORKING DISCOVERY

A. Discoverability and Relevancy

Civil litigants attempt to protect social media communications from discovery in many ways, including arguments that the information is not relevant. However, under both FRCP 34—discovery directed at parties to the litigation—and FRCP 45(A)(1)(c)—discovery directed at non-parties—the bar for relevancy in the context of discovery is extremely low.[1] Although courts frame the judicial tests used to interpret these rules in different ways, all of these tests have a presumption in *favor* of discoverability.[2]

---

[1] Fed. R. Civ. P. 34; Fed. R. Civ. P. 45(a)(1)(C).

[2] *See* Fed. R. Civ. P. 34 and *infra* note 3.

The most widely used test only requires that courts consider "whether or not evidence *might* be admissible, or reasonably calculated to lead to *any* evidence that might be found material, or relevant in determination of issues involved in proceeding."[3] The information sought need not be proven relevant, but only needs to "appear relevant."[4] Once this low threshold is met, the party resisting discovery has the burden to establish the lack of relevance. The resisting party must show that the information sought is of "such marginal relevance that the potential harm occasioned by discovery would outweigh the *ordinary presumption in favor of broad disclosure*."[5]

B. Discoverability and Evidentiary Privileges

While most courts will find that online social communications are relevant, those communications may still be excluded from discovery if they are protected by an evidentiary privilege.

Evidentiary privileges, such as the attorney-client privilege or marital privilege, are a creation of the common law and are not explicitly provided for in the Federal Rules of Evidence.[6] Under the Federal Rules of Evidence, common law privileges are to be strictly construed.[7] Courts may recognize a new category of privileges, but to do so the claimant of the privilege bears the

---

[3] Hess v. Pittsburgh Steel Foundry & Mach. Co., 49 F.R.D. 271, 272 (1970) (emphasis added); *see also* National Utility Service, Inc. v. Northwestern Steel & Wire Co., 426 F.2d 222, 225 (1970) (discovery "motion may be verified in *any reasonable manner* demonstrating that the material sought is relevant to the issues and that there is *some good reason* for enlisting the power of the court in uncovering the information.") (emphasis added) (citing Schlagenhauf v. Holder, 379 U.S. 104, 118–19 (1964)); U.S. v. 50.34 Acres of Land, More or Less, in Village of East Hills, Nassau County, N.Y., 13 F.R.D. 19, 21 (1952) (documents are discoverable "where they *might* give clues as to the existence or location of relevant facts, or where they *might* be useful for purposes of impeachment or corroboration.") (emphasis added).

[4] E.E.O.C. v. Thorman & Wright Corp., 243 F.R.D. 426, 429 (2007).

[5] *Id*. (emphasis added). A "potential harm" may well be the loss of privacy experienced by the litigant forced to turn over private information.

[6] Fed. R. Evid. 501, Advisory Committee Notes.

[7] Univ. of Pa. v. E.E.O.C., 493 U.S. 182, 189 (1990).

burden of proof and must meet a four-step test.[8] To establish a "social media communication privilege" litigants would be required to meet the following test:

> First, the claimant must establish that he or she divulged the communication with confidence that they would not be disclosed;
>
> Second, the claimant must show that the element of confidentiality is essential to fully and satisfactorily maintain the relationship between the parties;
>
> Third, the claimant must establish that there is community agreement that the relationship must be sedulously fostered; and
>
> Fourth, the claimant must show that the injury potentially sustained to the relationship because of the disclosure outweighs the benefit of correctly disposing of the litigation.[9]

If the claimant fails to establish the existence of any one of these four factors, the court will not recognize a privilege of confidentiality and, unless another exception applies, will require disclosure of the information sought by the opposing party.

In the case of a new "social media communication privilege," the litigant seeking the communication's exclusion would have to show that the conversations were presumed confidential, a difficult task when the entire premise of social media is to share information with a large number of people.

Even if the party resisting discovery can establish a presumption of privacy, that party would further have to show the importance of the relationship between the communicating parties and that social media relationships are deserving of protection. Courts would likely not find that social media communication should be "sedulously fostered" to the same degree as

---

[8] *See* McMillen v. Hummingbird Speedway, Inc. 2010 WL 4403285 (Pa. Com. Pl. Sept. 9, 2010) (citing Matter of Adoption of Embick, 506 A.2d 455, 461 (Pa. Super. 1986); *see also* 8 J. WIGMORE, EVIDENCE §2285 (McNaughton's rev. ed. 1961).

[9] 8 J. WIGMORE, EVIDENCE §2285 (McNaughton's rev. ed. 1961).

communications within marriage or communications with one's attorney. Moreover, the medium of exchange is unlike private one-on-one consultation between spouses or attorneys and their clients. The privilege was not established to protect public communications. And disclosure of confidential information—even on blogs or in online chats—results in a waiver of the privilege itself.[10]

In sum, litigants often cannot hide behind the low relevancy bar to discoverability and courts will rarely, if ever, create a new evidentiary privilege. Most civil litigants will face an uphill battle if they try to exclude social networking information under the FRCP or the Federal Rules of Evidence. As such, some litigants seeking to block such discovery have turned to the right to privacy contained in the Fourth Amendment.[11]

II. THE FOURTH AMENDMENT'S "RIGHT TO PRIVACY" AND DISCOVERABILITY

The right to privacy under the Fourth Amendment was first proposed by Samuel Warren and Louis Brandeis in an 1890 Harvard Law Review article.[12] The right was characterized as essentially the "right to be left alone." It was not until the Supreme Court decided *Katz v. United States* in 1967 that the right to privacy under the Fourth Amendment gained traction.[13] In what would come to be the predominant constitutional test, Justice Harlan in his concurrence proposed a two-part analysis to determine whether an individual's Fourth Amendment right to privacy has been violated: first, whether the individual had an actual expectation of privacy; and second, whether the individual's expectation was "one that society is prepared to recognize as 'reasonable.'"[14] If either prong fails, the individual has no

[10] *See* Lenz v. Universal Music Corp., 2010 WL 4789099 at *1150 (N.D. Cal. Nov. 17, 2010).

[11] *See* Romano v. Steelcase, Inc., 30 Misc.3d 426 (N.Y. Sup. Ct. 2010).

[12] *See* Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

[13] 389 U.S. 347 (1967).

[14] *Id*. at 361 (Harlan, J., concurring).

reasonable expectation of privacy, and the government intrusion does not violate the Fourth Amendment.[15] The Fourth Amendment only protects against government intrusions that violate a *reasonable expectation of privacy*.

The *Katz* court further held that there is no reasonable expectation of privacy in information you have "knowingly exposed" to a third-party.[16] As such, Supreme Court cases following *Katz* have held that there is no reasonable expectation of privacy in phone records, bank records, or trash set out for collection.[17]

Does the Fourth Amendment's protection of privacy extend to civil discovery requests? Likely it does not. The Fourth Amendment only curtails government action and does not apply to private searches.[18] And one federal district court proclaimed in dicta that "[i]t strains common sense and constitutional analysis to conclude that the fourth amendment was meant to protect against unreasonable discovery demands made by a private litigant in the course of civil litigation."[19] But litigants should not ignore the *Katz*

---

[15] *Id*.

[16] *See id.* at 351 (majority opinion) ("what a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.") (citing Lewis v. United States, 385 U.S. 206, 210 (1966) and United States v. Lee, 274 U.S. 559, 563 (1927)).

[17] *See* California v. Greenwood, 486 U.S. 35, 40–41 (1988) ("respondents exposed their garbage to the public sufficiently to defeat their claim to Fourth Amendment protection," as they "deposited their garbage 'in an area particularly suited for public inspection and, in a manner of speaking, public consumption, for the express purpose of having strangers take it.'") (quoting United States v. Reicherter, 647 F.2d 397, 399 (3rd Cir. 1981); United States v. White, 401 U.S. 745, 752–53 (1971) (no reasonable expectation of privacy in recorded conversations by police informant when defendant volunteered information to this third-party); United States v. Miller, 425 U.S. 435, 443 (1976) ("the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.") (citing United States v. White, 401 U.S. at 1126; Hoffa v. United States, 385 U.S. 293, 302 (1966); and Lopez v. United States, 373 U.S. 427 (1963)).

[18] United States v. Jacobsen, 466 U.S. 109, 113 (1984).

[19] United States v. Int'l Bus. Machs. Corp., 83 F.R.D. 97, 102 (S.D.N.Y.1979).

test altogether in the civil context. Some courts still entertain Fourth Amendment challenges to discovery requests, and courts often look to the reasonableness of a party's expectation of privacy in social networking communication.[20]

III. SOCIAL NETWORKING SITES' TERMS OF SERVICE AND PRIVACY POLICIES

Several courts have looked to social networking sites' terms of service as a factor in determining the degree of privacy expected by the user. These terms of service and their relevant disclaimers illustrate the lack of privacy protections in place for social network users who wish to keep their data undiscoverable.

For example, Facebook's Data Use Policy reads in pertinent part:

> Your information is the information that's required when you sign up for the site, as well as the information you choose to share.
>
> Registration information: When you sign up for Facebook, you are required to provide your name, email address, birthday, and gender.
>
> Information you choose to share: Your information also includes the information you choose to share on Facebook, such as when you post a status update, upload a photo, or comment on a friend's story.
>
> It also includes the information you choose to share when you take an action, such as when you add a friend, like a Page or a website, add a place to your story, find friends using our contact importers, or indicate you are in a relationship.
>
> Your name, profile pictures, cover photos, gender, networks, username and User ID are treated just like information you choose to make public. . . .

[20] *See* Romano v. Steelcase, Inc., 30 Misc.3d 426 (N.Y. Sup. Ct. 2010).

> We receive information about you from your friends and others, such as when they upload your contact information, post a photo of you, tag you in a photo or status update, or at a location, or add you to a group.
>
> When people use Facebook, they may store and share information about you and others that they have, such as when they upload and manage their invites and contacts. . . .
>
> [F]or information others share about you, they control how it is shared. . . .
>
> We store data for as long as it is necessary to provide products and services to you and others. . . . Typically, information associated with your account will be kept until your account is deleted. For certain categories of data, we may also tell you about specific data retention practices.[21]

Moreover, Facebook's Data Use Policy states that in order to respond to legal requests and prevent harm, Facebook's operators may disclose information pursuant to subpoenas, court orders, or other civil or criminal requests if they have a good faith belief that the law requires them to respond.[22]

MySpace has very similar policies that read in pertinent part:

> There may be instances when Myspace may access or disclose PII [Personal Identifiable Information], Profile Information or non-PII without providing you a choice in order to: (i) protect or defend the legal rights or property of Myspace, our Affiliated Companies or their employees, agents and contractors (including enforcement of our agreements); (ii) protect the safety and security of Users of the Myspace Services or members of the

[21] *Data Use* Policy, FACEBOOK, http://www.facebook.com/full_data_use_policy (last revised June 8, 2012).

[22] *Id*.

> public including acting in urgent circumstances; (iii) protect against fraud or for risk management purposes; or (iv) comply with the law or legal process.[23]

Litigants attempting to invoke their right to privacy based on a reasonable expectation that information stored on either Facebook or MySpace is private may face difficulty overcoming the fact that according to the plain language of most social networking sites' policies, little to no privacy is guaranteed.

IV. *MCMILLEN V. HUMMINGBIRD SPEEDWAY, INC.*

In *McMillen v. Hummingbird Speedway, Inc.*, a personal injury action, plaintiff McMillen filed suit in an attempt to recover damages for injuries he sustained when he was rear-ended after a stock car race.[24] McMillen alleged substantial injuries, including possible permanent impairment, loss of general health, and loss of enjoyment of life.[25]

The defendants sent a discovery request asking if McMillen was a member of Facebook or any other social networking sites, and if so, requested disclosure of his login information. McMillen responded that he was a Facebook member, but that his user name and password were confidential and privileged.[26]

After reviewing the public portion of McMillen's Facebook account and discovering comments about his fishing trip and attendance at another car race in Florida, the defendants filed a motion to compel discovery, based on the assertion that such information was relevant to the sufficiency of the plaintiff's damages claims.[27] Specifically, the defendants wanted to be able "to determine whether or not plaintiff has made any other

---

[23] *Privacy Policy*, MYSPACE, http://www.myspace.com/Help/Privacy (last updated October 1, 2012).

[24] 2010 WL 4403285 (Pa. Com. Pl. 2010).

[25] *Id*. at *1.

[26] *Id*.

[27] *Id*.

comments which impeach and contradict his disability and damages claims."[28]

The court granted the defendants' motion to compel based on two judicial considerations. First, it noted that courts "should allow litigants to utilize 'all rational means for ascertaining the truth'" where there exists some indication that social networking sites contain relevant information.[29] And second, it stated that courts generally disfavor granting evidentiary privileges.[30]

The court recognized that our system of discovery allows for broader pre-trial discovery of evidence than may ultimately be admissible in trial. Anything relevant to the matter will be discoverable at the outset of litigation, regardless of whether it will be excluded in trial for other reasons.[31] Also, the court noted that the law disfavors privileges because of the fundamental belief that broad discovery best serves justice.[32] Because privileges are a "derogation of the search for the truth," they should be strictly construed.[33] Based upon these two fundamental premises, the court determined that access to social networking sites should be freely granted.

While the court did not explicitly undertake a Fourth Amendment privacy analysis, the court further commented on the reasonable privacy expectations of a social networking site user and determined that it is unrealistic for a user to expect that social media communications will be kept confidential. In fact, such users are assured only a "modicum of privacy."[34] The privacy terms on the social networking sites in question should dispel any belief of confidentiality on behalf of the plaintiff.[35] The court commented that "the complete access afforded to the Facebook and MySpace operators alone defeats [Plaintiff's] proposition that

---

[28] *Id*. at *2.

[29] *Id*. at *7 (quoting Koken v. One Beacon Ins. Co., 911 A.2d 1021, 1027 (Pa. Commw. Ct. 2006)).

[30] *Id*.

[31] *Id*. at *2.

[32] *Id*.

[33] *Id*. (quoting Hutchison v. Luddy, 606 A.2d 905, 908–09 (Pa. Super. 1992)).

[34] *Id*. at *3.

[35] *Id*. at *3-4.

his communications are confidential."[36] The right of confidentiality is lost when an individual knows that a third party could overhear or intercept the information.[37]

In an assertive conclusion, the court emphasized that allowing discovery of social networking sites in anticipation of litigation is of very little detriment to society, while the benefits of proving the truth or falsity of such claims "cannot be overstated."[38]

V. *ROMANO V. STEELCASE, INC.*

Only a few weeks after *McMillen* was decided, in *Romano v. Steelcase, Inc.*, a New York trial court again allowed defendants to access private information on the plaintiff's Facebook and MySpace accounts.[39]

In her personal injury action, plaintiff Romano claimed she had sustained permanent injuries and was confined to her house because of defendant's negligence.[40] In an effort to contest the extent of the plaintiff's injuries, particularly her claims for loss of enjoyment of life, the defendant sought discovery of the plaintiff's Facebook and MySpace accounts. The defendant based his request on the fact that her public Facebook profile page showed her smiling happily outside of her home.[41]

In response to the defendant's requests, Romano argued that she held a reasonable expectation of privacy with respect to her home computer and her online postings under the Fourth Amendment.[42] The court rejected Romano's Fourth Amendment claims and found that she in fact had no reasonable expectation of privacy. The court looked to the reasonableness standard set forth by Justice Harlan in *Katz v. United States*, and asked whether plaintiff had both exhibited an actual subjective expectation of

---

[36] *Id*. at *5.
[37] *Id*.
[38] *Id*. at *6.
[39] Romano v. Steelcase, Inc., 30 Misc.3d 426, 427 (N.Y. Sup. Ct. 2010).
[40] *Id*. at 430.
[41] *Id*. at 427. Under the local court rule, Civil Practice Law and Rule (CPLR) 3101, "there shall be full disclosure of all non-privileged matter which is material and necessary to the defense or prosecution of an action."
[42] *Id*. at 434.

privacy and whether the expectation is one that society recognizes as reasonable.[43] The court concluded that an additional factor weighing against recognition of a right to privacy on social networking sites is the fact that "privacy concerns are far less where the beneficiary herself chose to disclose the information."[44] Lastly, after reviewing the privacy disclaimers on both Facebook and MySpace, the court determined that "when plaintiff created her accounts, she consented to the fact that her personal information would be shared with others, notwithstanding her individual privacy settings."[45]

Because the *public* portions of the pages contradicted her claims and deposition testimony, the court concluded that there was a "reasonable likelihood" the *private* portions of the sites could contain evidence that was "material and relevant to the defense" of the action and were therefore discoverable.[46] The court based much of its decision upon the notion that "plaintiffs who place their physical condition in controversy may not shield from disclosure material which is necessary to the defense of the action."[47]

The court further found that "[t]o deny defendant an opportunity to access these sites would not only go against the liberal pretrial disclosure and discovery policies of New York, but would condone plaintiff's attempt to hide relevant information behind self-regulated privacy settings," a result the court found unjust.[48]

VI. ACCESS GRANTED

Litigants should pay particular attention to the practical effects of these decisions. Not only did the *McMillen* and *Romano* courts find that litigants could discover social media communication, but

[43] *Id*. at 433 (quoting Katz v. United States, 389 U.S. 347, 361–62 (1967)).

[44] *Id*. at 433. (citing Beye v. Horizon Blue Cross Blue Shield of N.J., No. 06-5337 (D. N.J., Dec. 14, 2007)).

[45] *Id*. at 434.

[46] *Id*. at 430.

[47] *Id*. at 428 (citing Hoenig v. Westphal, 52 N.Y.2d 605 (1981)).

[48] *Id*. at 432.

they both ordered the litigants to turn over the credentials to their accounts, thus allowing the requesting party unrestricted access to the accounts.[49]

Granting such sweeping access represents a break from traditional electronic discovery orders. Normally, courts will not invoke FRCP 34 to grant unrestricted access to a party's electronic database.[50] Rather, the requesting party may inspect and copy the information after the producing party turns over the data in a "reasonably usable form."[51] The general rule is that courts will only allow direct access to a party's database after the court makes a factual finding that the producing party failed to comply with discovery rules and after considering the producing party's interests including the "preservation of his records, confidentiality of non-discoverable matters and costs."[52]

By allowing access to the credentials of the accounts, the courts in *McMillen* and *Romano* skipped the production step and allowed the requesting party direct access. These cases indicate that courts have concluded social media communication deserves little privacy protection. In essence, the producing parties had such a low interest in protecting the information that the courts did not need to find that the party failed to comply with a discovery rule. Not all courts grant such broad access.[53] But litigants should take notice that a court may grant complete access to a party's social networking account.

---

[49] McMillen v. Hummingbird Speedway, Inc., 2010 WL 4403285 (Pa. Com. Pl. 2010); *Romano*, 30 Misc.3d at 435 (ordering that the plaintiff grant full access to the account including the delivery "to counsel for defendant Steelcase a properly executed consent and authorization as may be required by the operators of Facebook and MySpace, permitting said defendant to gain access to plaintiff's Facebook and MySpace records, including any records previously deleted or archived by said operators.").

[50] U & I Corp. v. Advanced Med. Design, Inc., 251 F.R.D. 667, 674 (M.D. Fla. 2008) (citing In re Ford Motor Co., 345 F.3d 1315, 1316 (11th Cir. 2003)).

[51] *Id*. (citing *In re Ford Motor Co*., 345 F.3d at 1316–17).

[52] *Id*.

[53] Tompkins v. Detroit Metro. Airport, 278 F.R.D. 387, 389, (E.D. Mich. 2012) (holding that a plaintiff to a civil suit need not turn over login information to Facebook account at the defendant's request, because that request was overly broad).

VII. COUNTERPOINT—*MCCANN V. HARLEYSVILLE INSURANCE CO.*

Not all courts allow access to social media communication. Less than two months after *Romano*—in a factually similar case—another New York court came to an opposite conclusion and affirmed the lower court's denial of a motion to compel disclosure of a Facebook account.

In *McCann v. Harleysville Insurance Co.* plaintiff McCann was injured in an automobile accident and filed a suit seeking the supplementary underinsured motorist coverage from her own insurance carrier after claiming the entire insurance policy of the other driver involved in the collision.[54] During discovery, the defendant, McCann's insurance company, sought access to the plaintiff's Facebook account and photographs posted on the site.[55] The defendant claimed that the plaintiff's account was relevant to the question of whether she had in fact sustained a serious injury.[56] Aside from this assertion, the defendant could not point to anything in particular that her Facebook account would reveal.

The Supreme Court Appellate Division determined that the defendant's motion to compel disclosure of photographs and seeking access to Plaintiff's account information was properly denied by the lower court as overly broad, but could be revisited upon the service of a "new, proper discovery demand" at a future date.[57] The denial was based on the fact that the defendant's request was insufficient because it "failed to establish a factual predicate with respect to the relevancy of the evidence."[58] This was, in the words of the court, simply a "fishing expedition."[59]

---

[54] McCann v. Harleysville Ins. Co. of N.Y., 78 A.D.3d 1524, 1524 (2010).
[55] *Id*.
[56] *Id*.
[57] *Id*.
[58] *Id*. at 1525 (citing Crazytown Furniture v. Brooklyn Union Gas Co., 150 A.D.2d 420, 421 (1989)).
[59] *Id*. at 1525.

CONCLUSION

Opponents of social networking discovery requests will likely face an uphill battle in their attempt to challenge such requests. While the *McCann* court did deny the discovery requests aimed at social networking information, it did so based on the overbroad nature of the discovery request, not because social networking communications deserve privacy protection. Therefore, while the legal grounds for preventing or allowing social networking discovery are unclear, courts that have considered social networking discovery requests have sent a clear message: social networking communications are discoverable. Advocates of broad social media discovery have two important factors on their side: first, the judicial consensus that courts should permit litigants to utilize "all rational means for ascertaining the truth;" and second, courts' established resistance to creating new evidentiary privileges.

Moreover, *McMillen* and *Romano* show that litigants can gain direct access to a party's social networking accounts by obtaining login and password information via discovery requests. Some courts have determined that these accounts are so undeserving of protection that they will skip the normal production step and allow direct access to the accounts themselves. Attorneys and litigants should take notice of this important development. However, remember that fishing expeditions—like the one in *McCann*—are never permitted. Social networking data is an easy target, but courts still refuse to declare "open season" on irrelevant data. In sum, while discovery of social networking information is a developing body of jurisprudence, the takeaway for the time being is that social networkers should proceed with caution when disclosing information on the web.

PRACTICE POINTERS

- Some courts have granted unrestricted access to social networking accounts by requiring disclosure of usernames, passwords, and deleted posts stored by the sites.
- *McCann v. Harleysville Insurance Co.* may merely address overbroad discovery requests and should not be interpreted

as a decision on the contours of protecting private personal information. The importance of *McCann* is that litigants seeking access to social networking information should clearly specify the "factual predicate" upon which they seek access to social networking information.

- Because data use and privacy policies on social networking sites are constantly evolving to comply with changing regulatory law and public opinion, litigants should be careful when relying on the precedential value of previous decisions. There very well may have been a wholesale upheaval of the social networking sites' policies since a prior decision. For example, since the above cases were decided, both Facebook and MySpace have made changes to their privacy policies.
- Blocking social networking communication may not be as futile as the above cases make it seem. The best approach may be to make a more nuanced argument than those that were made in the above cases. While factually and legally quite different than the above cases, in *Crispin v. Christian Audigier, Inc.*, a copyright infringement and breach of contract action, the California District Court used a more nuanced approach.[60] The court found *certain* aspects of plaintiff's Facebook and MySpace accounts were discoverable, while others were not. Messaging systems were sufficiently private and exclusive in nature such that under the Stored Communications Act, defendants could not insist upon their disclosure. Instead, defendants could discover only limited aspects of the plaintiff's social networking pages.[61] The court determined that the requests for Facebook and MySpace data that sought private messages should be quashed, but remanded to determine the degree of privacy present in Facebook "wall posts" and

[60] Crispin v. Christian Audigier, Inc., 717 F.Supp.2d 965 (C.D. Cal. 2010).
[61] *Id*. at 991.

MySpace "comments," as the degree of privacy of these functions were less apparent than the private messages.[62]

[62] *Id*.