

2014

Finding Privacy in a Sea of Social Media and Other E-Discovery

Allyson H. Stuart
Charleston School of Law

Recommended Citation

Allyson H. Stuart, *Finding Privacy in a Sea of Social Media and Other E-Discovery*, 12 NW. J. TECH. & INTELL. PROP. 149 (2014).
<https://scholarlycommons.law.northwestern.edu/njtip/vol12/iss3/1>

This Article is brought to you for free and open access by Northwestern Pritzker School of Law Scholarly Commons. It has been accepted for inclusion in Northwestern Journal of Technology and Intellectual Property by an authorized editor of Northwestern Pritzker School of Law Scholarly Commons.

N O R T H W E S T E R N
JOURNAL OF TECHNOLOGY
AND
INTELLECTUAL PROPERTY

**Finding Privacy in a Sea of Social Media
and Other E-Discovery**

Allyson Haynes Stuart



August 2014

VOL. 12, NO. 3

Finding Privacy in a Sea of Social Media and Other E-Discovery

By Allyson Haynes Stuart*

This article looks at the case law governing discovery of social media and finds several problems. First, many courts improperly require a threshold showing that relevant information exists in public portions of the user's social media account before allowing such discovery. Second, courts allow overbroad discovery, often requiring a litigant to turn over his or her username and password to the other party. At the same time, parties seek such information directly from social media sites, attempting an end-run around the relevancy requirement and increasing motion practice. The article argues that, instead, social media discovery should be treated like other party-driven discovery where litigants are entitled to request relevant information that exists on social media accounts and are in turn responsible for providing that information just as they would other discovery in their possession, custody, or control. There is a promising new line of case law following that path. The article then looks more broadly at the emerging issue of privacy in e-discovery and sets forth the existing methods of restricting undue attempts to invade that privacy. Finally, the article argues that the scope of e-discovery dictates a new look at the way our discovery rules protect privacy and finds encouragement in the latest proposed amendments to Federal Rule of Civil Procedure 26(b)(1) to limit the scope of discovery based on proportionality and relevance to existing claims and defenses.

TABLE OF CONTENTS

I. Introduction.....	150
II. Discovery of Social Network Information: Both Overinclusive and Underinclusive ..	152
A. Increase in Requests and Use In All Kinds of Cases	152
B. Courts Improperly Ordering Blanket Access to Social Media	154
1. The Threshold Approach.....	154
2. Both Underinclusive and Overinclusive	159
3. Wasting Judicial Resources.....	161
C. Parties Improperly Seeking Blanket Access Directly from Social Media Sites ..	162
D. Movement Toward a Better Approach	163
III. Finding Privacy in a Sea of E-Discovery	166
A. Putting Social Media in Context	166
1. The Format	166

* Professor of Law, Charleston School of Law. The author would like to thank the participants of the 2013 Privacy Law Scholars Conference, in particular Amanda Conley, Ian Kerr, and Eloïse Gratton, for their very helpful comments on an earlier draft; Kelsey Brudvig, Charleston School of Law 2014, for her excellent research assistance; and the Faculty of the Charleston School of Law for their support and encouragement.

2. The Public Nature	166
B. What Is the Implication of Using Privacy Settings?	168
C. Narrowing the Scope of Discovery	171
D. Privacy Protection Under the Rules.....	173
IV. Conclusion.....	175

I. INTRODUCTION

¶1 Electronic discovery is one of the biggest challenges our courts face today.¹ Its vast scope complicates the system in which relevant information is exchanged, and its expense can be overwhelming.² Given the very low number of cases that ever actually go to trial,³ pretrial discovery (and related motion practice) is the primary determinant of a case’s success.⁴ Unfortunately, broad discovery can inhibit the search for the truth as much as it can further that search, particularly when the discovery sought is of a sensitive nature and the prospect of its disclosure is prohibitive to a litigant’s pursuit of the case, resulting in a form of discovery blackmail.⁵ With the advent of social media, discovery now often includes information from social media sites, and its potential for misuse is high.

¶2 Courts faced with the discoverability of social media unfortunately have treated the issue differently as compared with other types of discovery, giving litigants both more and less protection from such requests.⁶ First, some courts have established a “preliminary showing” requirement that a person’s public social network site (SNS) information must reveal relevant evidence before the court will allow inquiry into a party’s private SNS area as well.⁷ There is no basis for such a threshold requirement in

¹ See RICHARD L. MARCUS, *Introduction* to SHIRA A. SCHEINDLIN, DANIEL J. CAPRA & SEDONA CONFERENCE, *ELECTRONIC DISCOVERY AND DIGITAL EVIDENCE* 1 (2d ed. 2012) (“Since the beginning of the 21st century, electronic discovery has been the hottest topic in litigation By one 2011 estimate, the annual production of digital information equals 39 million times the amount of information contained in all books ever written.”).

² See James N. Dertouzos, Nicholas M. Pace & Robert H. Anderson, *The RAND Inst. for Civil Justice, The Legal and Economic Implications of Electronic Discovery*, RAND INST., 3–4 (2008), available at http://www.rand.org/content/dam/rand/pubs/occasional_papers/2008/RAND_OP183.pdf (“[T]he most frequent issue raised by those we interviewed was the enormous costs—in time and money—to review information that is produced. This is because the sheer volume of records that are identifiable and producible is greater with electronic processes, potentially relevant information that might never have been recorded previously is now being routinely retained, and because the requesting attorneys are aggressive in seeking out such information.”).

³ Marc Galanter, *The Hundred-Year Decline of Trials and the Thirty Years War*, 57 STAN. L. REV. 1255, 1257–59 (2005); Arthur R. Miller, *Simplified Pleading, Meaningful Days in Court, and Trials on the Merits: Reflections on the Deformation of Federal Procedure*, 88 N.Y.U. L. REV. 286, 306–07 (2013) (“I am increasingly concerned about procedural changes that have resulted in the earlier and earlier disposition of litigation Today, there are hardly any federal civil trials—let alone jury trials.”).

⁴ See Miller, *supra* note 3, at 307 (“Cases simply do not survive until trial; they are settled or, increasingly, dismissed.”).

⁵ See Richard L. Marcus, *A Modest Proposal: Recognizing (At Last) That the Federal Rules Do Not Declare That Discovery Is Presumptively Public*, 81 CHI.-KENT L. REV. 331, 340–41 (2006) (discussing the “strategic value of discovery into sensitive areas”).

⁶ See *infra* Section II.

⁷ *Id.*

the federal rules, which instead allow broad requests for relevant discovery. The public/private distinction suggested by SNS users' privacy settings, while relevant in some legal contexts, should not prevent SNS discovery, just as privacy of diaries or personal correspondence does not necessarily prevent disclosure in the offline context.

¶3 Second, and more troubling, once courts do find that such a threshold showing is met, they often allow overbroad discovery into the user's SNS accounts.⁸ It is as if the preliminary showing provides the key to unlocking a litigant's treasure chest of social media content. These courts order a party to turn over her username and password, allowing wholesale access to SNS accounts, despite the high likelihood that such access will reveal non-relevant and possibly highly private information as well.⁹

¶4 Finally, parties are going directly to Facebook and other SNS providers themselves with a subpoena seeking account information and content.¹⁰ Instead, parties should only resort to this tactic if unable to obtain relevant information from the other party. As with other discovery, when information is in the custody or control of a party, seeking that information from a third party is an option only when there is a showing that the party has spoliated evidence or is otherwise wrongfully refusing to produce relevant evidence.¹¹ In addition, there are valid arguments that direct solicitation of the information from SNS providers violates the Stored Communications Act.¹²

¶5 Information on social media sites should be treated like other discovery.¹³ Parties should include requests for SNS communications and other content in their discovery requests, and the responding party should bear the burden of producing responsive information.¹⁴ Only if there is a basis for showing that the responding party is withholding information should there be any issue of further compelled disclosure.

¶6 While this article stresses that social media discovery should not be treated differently from other discovery—meaning that parties should not be entitled to more *or* less privacy—it also argues that the federal rules should be reexamined in light of the magnitude of discoverable electronic information. While the federal rules have been modified somewhat to take into account the emergence of vast amounts of electronically stored information, additional restrictions on scope are appropriate to counter the potential for discovery abuse.¹⁵

¶7 Part II describes the increase in social network discovery and examines court decisions regarding discoverability of that information. Courts have largely fallen into two camps, one of which grants overbroad blanket access to social media discovery, and the other which improperly limits such discovery where there is no relevant public social network information. Part II also critiques litigants' practice of directly requesting access from the social network providers themselves, which represents an end-run around the

⁸ See Section II.B.

⁹ *Id.*

¹⁰ See Section II.C.

¹¹ *Id.*

¹² *Id.*

¹³ See Steven S. Gensler, *Special Rules for Social Media Discovery?*, 65 ARK. L. REV. 7, 13 (2012) (“[S]ocial-media discovery has not presented any issues that are not covered by the existing discovery scheme and that cannot be resolved by sound judicial application of the existing discovery scheme to this new technological context.”).

¹⁴ *Cf.* FED. R. CIV. P. 26.

¹⁵ See *infra* Section III.C.

relevancy requirement. Finally, Part II notes a promising trend of courts rejecting the all-or-nothing approach and granting discovery of properly tailored requests for relevant social network information. Part III looks more closely at the nature of social media discovery and criticizes the tendency to treat the discoverability of such information as a function of its semi-public nature. Instead, the fact that social network communications have been shared with a limited group of people does not render them automatically discoverable. Part III also discusses the proposed amendments to the Federal Rules of Civil Procedure to make discoverability a function of proportionality, and suggests that this change could also reduce overbroad social media fishing expeditions. Finally, Part III discusses the interaction between discoverability and privacy under the federal rules and how those rules may be used properly to protect against undue invasions into personal material. Part IV briefly concludes.

II. DISCOVERY OF SOCIAL NETWORK INFORMATION: BOTH OVERINCLUSIVE AND UNDERINCLUSIVE

A. *Increase in Requests and Use In All Kinds of Cases*

¶8 In less than a decade, there has been an explosion in the use of social media in society. Facebook, the most popular online social network, which launched in 2004, has over one billion monthly active users worldwide,¹⁶ including 167 million users in the United States alone,¹⁷ and 250 billion photographs have been uploaded onto the site.¹⁸ Half of all adults in America use social networking sites.¹⁹ The increase in digital devices only adds to social media use, as Americans use smartphones and tablets to access social media at all times of the day.²⁰

¶9 Not surprisingly, social media has invaded the courtroom. Litigants have found social media evidence to be very helpful in a vast array of cases. On SNSs, people tend to share thoughts, feelings, and information freely and often,²¹ making such media treasure troves of admissions and impeaching evidence,²² especially against individuals claiming

¹⁶ *Facebook Reports First Quarter 2013 Results*, FACEBOOK INVESTOR RELATIONS (May 1, 2013), <http://investor.fb.com/releasedetail.cfm?ReleaseID=761090>.

¹⁷ This is a drop from 2012, and some believe the social network may be reaching a saturation point. Quentin Fottrell, *Facebook Loses 1.4 Million Active Users in U.S.*, MARKET WATCH (Jan. 15, 2013, 5:24 PM), http://articles.marketwatch.com/2013-01-15/finance/36346107_1_active-users-facebook-social-media.

¹⁸ FACEBOOK, ERICSSON & QUALCOMM, *A FOCUS ON EFFICIENCY* 6 (Sept. 16, 2013).

¹⁹ Mary Madden & Kathryn Zickuhr, *65% of Online Adults Use Social Networking Sites*, PEWRESEARCH INTERNET PROJECT (Aug. 26, 2011), <http://pewinternet.org/Reports/2011/Social-Networking-Sites.aspx>.

²⁰ NIELSEN, *THE DIGITAL CONSUMER* 17 (2014), available at <http://www.nielsen.com/content/dam/corporate/us/en/reports-downloads/2014%20Reports/the-digital-consumer-report-feb-2014.pdf> (“Two in five (39%) Americans get digitally social while at work, and one in five (21%) have logged onto social sites while in the bathroom in the past 30 days.”).

²¹ See Ryan A. Ward, Note, *Discovering Facebook: Social Network Subpoenas and the Stored Communications Act*, 24 HARV. J.L. & TECH. 563, 564 (2011) (“Information from these sites is useful because ‘users of social network sites often ‘let their hair down’ in a way that surpasses even the thoughtless statements that all too often appear in email.’”) (quoting James Parton, *Obtaining Records from Facebook, LinkedIn, Google and Other Social Networking Websites and Internet Service Providers*, DRI TODAY (May 24, 2010, 9:40 AM), <http://forthedefense.org/post/Obtaining-Records-From-Facebook-LinkedIn-Google-and-Other-Social-Networking-Websites-and-Internet-Service-Providers.aspx>).

²² See *In the Matter of K.W.*, 666 S.E.2d 490, 494–95 (N.C. Ct. App. 2008) (holding that evidence of

mental and/or physical damages. Evidence from Facebook has been used in cases to show plaintiffs' exaggeration of their physical²³ and emotional injuries;²⁴ parents' failure to act in the best interests of their children;²⁵ spouses' infidelity;²⁶ and even a criminal defendant's alibi²⁷ or a rape victim's lack of credibility.²⁸ Practitioners recommend the aggressive use of broad interrogatories and document requests aimed at social media evidence.²⁹

¶10

Like other changes to the law wrought by the Internet, the infiltration of social media into discovery has not been seamless. Whether it is because of the online nature of social media or the candor it provokes, parties and courts have treated it differently from other forms of discovery.³⁰ This Article argues that social media should not be treated differently but should instead be given as much or as little privacy as civil discovery in general. However, the procedural rules themselves should be readdressed to put a check on the vast amount of electronic discovery of all kinds that is swallowing the courts.³¹

minor's MySpace page was admissible for impeachment purposes as prior inconsistent statement but improper exclusion was harmless, and the evidence was not admissible as substantive evidence).

²³ See *Loporcaro v. City of N.Y.*, 950 N.Y.S.2d 723 (Sup. Ct. 2012); *Trail v. Lesko*, No. GD-10-017249, 2012 Pa. Dist. & Cnty. Dec. LEXIS 194 (C.P. Allegheny County July 3, 2012).

²⁴ See *Mailhoit v. Home Depot U.S.A., Inc.*, No. CV 11-03892, 2012 U.S. Dist. LEXIS 131095 (C.D. Cal. Sept. 7, 2012) (granting defendant's motion to compel discovery where discovery request was narrowed to communications between the plaintiff and her former employer, including those via social media but denying motion for more generalized discovery); *Robinson v. Jones Lang Lasalle Ams., Inc.*, No. 3:12-cv-00127-PK, 2012 WL 3763545 (D. Or. Aug. 29, 2012) (granting in part and denying in part defendant's motion to compel, applying the same standard to social media content as to other types of discoverable materials).

²⁵ *In re S.A.*, No. 10-0203, 2010 WL 1881524, at *2 (Iowa Ct. App. May 12, 2010) (admitting child's use of inappropriate language on Facebook after midnight as proof of a lack of parental supervision).

²⁶ Stephanie Chen, *Divorce Attorneys Catching Cheaters on Facebook*, CNN (June 1, 2010, 11:04 AM), <http://www.cnn.com/2010/TECH/social.media/06/01/facebook.divorce.lawyers/>. A survey found that 81% of the members of the American Academy of Matrimonial Lawyers have used or defended against evidence from social networking sites. Christopher B. Hopkins & Tracy T. Segal, *Discovery of Facebook Content in Florida Cases*, TRIAL ADVOC. Q., Spring 2012, at 14 (citing Leanne Italie, *Divorce lawyers: Facebook Tops in Online Evidence in Court*, USA TODAY (June 29, 2010, 10:41 AM), http://www.usatoday.com/tech/news/2010-06-29-facebook-divorce_N.htm).

²⁷ Damiano Beltrami, *His Facebook Status Now? 'Charges Dropped.'* LOCAL: FORT GREEN/CLINTON HILL (Nov. 11, 2009, 11:10 AM), <http://fort-greene.thelocal.nytimes.com/2009/11/11/his-facebook-status-now-charges-dropped/>.

²⁸ Stephanie Francis Ward, *MySpace Discovery: Lawyers Are Mining Social Networks for Nuggets of Evidence*, ABA J., Jan. 2007, at 34, available at <http://www.abajournal.com/magazine/article/next/>. But see *State v. Corwin*, 295 S.W.3d 572 (Mo. Ct. App. 2009), discussed in Beth C. Boggs & Misty L. Edwards, *Does What Happens On Facebook Stay on Facebook? Discovery, Admissibility, Ethics, and Social Media*, 98 ILL. B.J. 366, 369 (2010).

²⁹ See Hopkins & Segal, *supra* note 26, at 14–15 (providing sample interrogatory seeking username and password for any social media site used by the plaintiff in the previous five years and stating that the authors “as a general practice . . . request that plaintiffs execute a consent and authorization permitting them to obtain account content directly from the social media website,” noting that such access “may lead to evidence of alteration or deletion”); see also Monique C.M. Leahy, *Pretrial Involving Facebook, MySpace, LinkedIn, Twitter, and Other Social Networking Tools*, 121 AMERICAN JURISPRUDENCE PROOF OF FACTS 3d 1, § 25 (2010).

³⁰ See *infra* Section II.B.

³¹ See *infra* Section III.C.

B. Courts Improperly Ordering Blanket Access to Social Media

1. The Threshold Approach

¶11 A majority approach to social media discovery has developed.³² The majority of courts faced with motions to compel access to a litigant’s social media require a preliminary showing by the moving party that public portions of the person’s SNS have relevant information, usually because that content somehow contradicts positions taken by the SNS user in the lawsuit. Once this threshold is met, the keys to the person’s social media are given to the moving party, which then has blanket access to the person’s SNS content.³³

¶12 One of the earliest U.S. examples of the threshold approach is found in *Romano v. Steelcase*.³⁴ In this personal injury action, the defendant sought access to the plaintiff’s current and historical Facebook and MySpace content, arguing that it was relevant to the extent and nature of the plaintiff’s injuries, including loss of enjoyment of life. The court noted that the plaintiff’s public profile page “show[ed] her smiling happily in a photograph outside the confines of her home despite her claim that she ha[d] sustained permanent injuries and [was] largely confined to her house and bed.”³⁵ Therefore, the court found “a reasonable likelihood that the private portions of her sites may contain further evidence such as information with regard to her activities and enjoyment of life.”³⁶ The court found plaintiff’s privacy concerns to be low—she knew the information may become publicly available based on the policies of the SNSs themselves—and in any event outweighed by the defendant’s need for the information.³⁷ So, the court ordered the plaintiff to execute a consent and authorization to Facebook and MySpace permitting defendants access to all of the plaintiff’s records, including ones that had been deleted or archived.³⁸

³² The forerunners of this approach were primarily New York state trial and appellate courts. *See* Tapp v. N.Y. State Urban Dev. Corp., 958 N.Y.S.2d 392 (App. Div. 2013). There are obviously more appellate decisions in states like New York that allow interlocutory appeals from discovery orders, but the trend is apparent from published orders in other jurisdictions as well. *See, e.g., infra* notes 56 and 57 (listing cases).

³³ In addition to the New York cases discussed above, courts from other states like Pennsylvania and federal courts have also followed this approach. *See* Thompson v. Autoliv ASP, Inc., No. 2:09-cv-01375-PMP-VCF, 2012 WL 2342928, at *4–5 (D. Nev. June 20, 2012) (ordering plaintiff to upload all information from her Facebook and MySpace accounts onto an electronic storage device for review by defense counsel); Largent v. Reed, No. 2009-1823, 2011 WL 5632688, at *3, *6–7 (Pa. C.P. Nov. 8, 2011); Zimmerman v. Weis Markets, Inc., No. CV-09-1535, 2011 WL 2065410, at *2–3 (Pa. C.P. May 19, 2011); McMillen v. Hummingbird Speedway, Inc., No. 113-2010 CD, 2010 WL 4403285, at *4 (Pa. C.P. Sept. 9, 2010).

³⁴ *Romano v. Steelcase Inc.*, 907 N.Y.S.2d 650 (Sup. Ct. 2010).

³⁵ *Id.* at 654. The opinion does not mention the date of the profile picture or whether it was taken after the subject accident.

³⁶ *Id.*

³⁷ *Id.* at 656.

³⁸ *Id.* at 657. One reason for the broad disclosure ordered in *Romano* may be the peculiarity of New York’s “Scope of Disclosure” rules. N.Y. C.P.L.R. 3101 requires “full disclosure of any films, photographs, video tapes or audio tapes, including transcripts or memoranda thereof, involving a [party to the action].” N.Y. C.P.L.R. 3101(i) (McKinney 2009). The commentary to that rule states that “[t]his provision generally requires production of any films, photos and videos of the plaintiff, regardless of whether the material is relevant,” N.Y. C.P.L.R. 3101 cmt. 3101:50 (McKinney 2009) (citing *Tran v. New Rochelle Hosp.*, 786 N.E.2d 444 (N.Y. 2003)). But the court in *Tran* was referring to surveillance tapes made by defendants of plaintiffs in the context of personal injury actions, for which the relevance was not

¶13

Romano relied primarily on case law from Canada, including the 2009 Ontario Superior Court of Justice case *Leduc v. Roman*.³⁹ In that case, Leduc sued for injuries sustained in an automobile accident. In a medical examination conducted for purposes of discovery, the plaintiff told the doctor that he did not have many friends in the area but had “a lot on Facebook.”⁴⁰ The defendant moved for production of all materials on the plaintiff’s Facebook site and for an updated affidavit from the plaintiff listing relevant documents.⁴¹ After the lower court refused to order production, the court of appeals “share[d the lower court’s] concern about the breadth of the defendant’s request” but thought the defendant should be permitted to cross-examine the plaintiff as to “what relevant content, if any, was posted on [his] Facebook profile.”⁴² The lower court had “correctly interpreted [Canadian law] as requiring some evidence from a moving party pointing to the omission of a relevant document in the other’s affidavit of documents” but

questioned. *Tran*, 786 N.E.2d at 444. Another commentary suggests that those materials are *not* excluded from the rules’ limitation on relevance. After noting the lack of any limitation on scope in 3101(i), the commentary states nevertheless that “[t]he relevance standard in CPLR 3101(a) has generally been understood to apply to all disclosure, regardless of the materials sought or the particular device used.” N.Y. C.P.L.R. 3101 cmt 3101:50 (McKinney 2009), citing *Kavanagh v. Ogden Allied Maint. Corp.*, 705 N.E.2d 1197 (N.Y. 1998). In any event, the statutory provision only covers photographs and videos, not written messages or comments (all of which must be disclosed under *Romano*). See NY C.P.L.R. 3101(i) (McKinney 2009). And more importantly, the *Romano* court itself did not mention, much less rely upon, any argument that the scope of 3101(i) is broader than other discovery. Instead, the court specifically states that the Facebook and MySpace postings “may contain further evidence such as information with regard to her activities and enjoyment of life, *all of which are material and relevant to the defense of this action.*” *Romano*, 907 N.Y.S.2d at 654 (emphasis added).

³⁹ *Romano*, 907 N.Y.S.2d at 654–55. The court also cited *Ledbetter v. Wal-Mart Stores, Inc.*, No. 06-cv-01958-WYD-MJD, 2009 WL 1067018 (D. Colo. Apr. 21, 2009), where defendants had subpoenaed information from Facebook, MySpace and Meetup.com. The SNSs had refused to comply with the subpoena, so the defendant sought releases from the plaintiffs, who were alleging physical and psychological injuries arising from an electrical accident. See *id.* at *1. In a brief opinion, the magistrate judge denied the plaintiffs’ motion for a protective order regarding the subpoenas. *Id.* at *2. The plaintiffs had requested that the magistrate judge review the subpoenaed information in camera for purposes of removing material protected by physician-patient and spousal privilege. *Id.* at *1. The court found the plaintiffs had waived any such physician-patient privilege by seeking damages for their physical and mental injuries, and spousal privilege had been waived when the spouse herself joined the suit seeking loss of consortium. *Id.* The court also found the existing protective order in the case adequately protected the plaintiffs’ privacy interests. *Id.* at *2. Finally, the court found that the information sought in the subpoenas was reasonably calculated to lead to the discovery of admissible evidence. *Id.* It is not clear whether the plaintiffs had ever objected to the subpoenas on grounds of relevance or otherwise. See Plaintiffs’ Response in Opposition to Defendant Wal-Mart’s Motion to Compel Production of Content of Social Networking Sites, *Ledbetter v. Wal-Mart Stores, Inc.*, No. 06-cv-01958-WYD-MJD, 2009 WL 1067018 (D. Colo. Apr. 21, 2009), 2009 WL 3061764 (arguing that the defendants had chosen to use subpoenas to obtain the information and therefore should continue to pursue the information directly from the SNS’s, not by seeking releases from the plaintiffs).

⁴⁰ *Leduc v. Roman*, [2009] O.J. No. 681, at para. 3 (Can. Ont. Sup. Ct. J.)(QL).

⁴¹ *Id.* at para. 6.

⁴² *Id.* at para. 35; see also *id.* at para. 15 (“Master Dash did not err in his articulation of the law regarding motions under Rule 30.06. He acknowledged that Mr. Leduc had an obligation to produce all relevant documents in his possession, including any information posted on his private Facebook profile demonstrating activities and enjoyment of life, ‘even if it is contrary to his interests in this action.’ Master Dash also correctly noted that where, on a Rule 30.06 motion, the defendant contends that the plaintiff has not met his obligation to produce relevant documents, then the defendant must provide some evidence that the plaintiff has relevant materials in his possession or control.”).

should have “afford[ed] the defendant an opportunity to cross-examine Mr. Leduc on that affidavit regarding the kind of content posted on his Facebook profile.”⁴³ The court did not grant a broad request for disclosure of all Facebook information.

¶14 *Romano* misread *Leduc* both in its breadth of production required and in reasoning that a threshold showing of existence of relevant information in publicly-accessible material justified disclosure of the private information as well. The *Leduc* court discussed the only previous case to consider the issue, also from Canada and also involving a claim for loss of enjoyment of life resulting from injuries suffered in a car accident. In *Murphy v. Perger*,⁴⁴ “[t]he plaintiff had posted photographs on her publicly-accessible Facebook profile showing her engaged in various social activities. The defendant moved for production of any photographs maintained on the private Facebook profile over which the plaintiff had control.”⁴⁵ The court found it reasonable to conclude that relevant photographs were posted on the private site, in part because the plaintiff had produced pictures of herself in the litigation from before the accident.⁴⁶ The court found that any invasion of privacy was minimal and outweighed by the defendant’s need to have the photographs in order to assess the case and ordered the plaintiff “to produce copies of the web pages posted on her private site, subject to the ability of plaintiff’s counsel to make future submissions in the event that any of the photographs personally embarrassed the plaintiff.”⁴⁷

¶15 The plaintiff in *Leduc* had not posted any photographs or other material in the public portion of his Facebook profile.⁴⁸ Rather than allowing this fact to insulate his Facebook account from discovery, the court found “[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.”⁴⁹ Therefore, neither case ordered blanket access to the party’s SNS material; instead, they found that relevant material should be produced.

¶16 In addition, *Romano* has been cited as precedent for applying a threshold approach to SNS evidence, but, in fact, the Canadian law applied in *Leduc* and *Murphy*—unlike U.S. law—specifically requires such a threshold showing. In what are known as “simplified rules” cases like *Leduc*, which do not permit discovery as of right, a movant is required to present evidence that the other party possesses a relevant document before the court can order production.⁵⁰ That evidence may come from “questions asked on a party’s examination for discovery about the existence and content of the person’s Facebook profile,”⁵¹ or from evidence of relevant information on the public portion of the

⁴³ *Id.* at para. 36.

⁴⁴ *Id.* at para. 24 (discussing *Murphy v. Perger*, [2007] O.J. No. 5511 (Can. Ont. Sup. Ct. J.)(QL)).

⁴⁵ *Id.*

⁴⁶ *Id.*

⁴⁷ *Id.* at para. 25.

⁴⁸ *Id.* at para. 31.

⁴⁹ *Id.* at para. 32. Instead, the court stated that “mere proof of the existence of a Facebook profile does not entitle a party to gain access to all material placed on that site.” *Id.* at para. 33.

⁵⁰ *Id.* at para. 33 (“Rule 30.06 requires the presentation of some evidence that a party possesses a relevant document before a court can order production.”).

⁵¹ *Id.* at para. 33; *see also id.* (“Where the party’s answers reveal that his Facebook profile contains content that may relate to issues in an action, production can be ordered of the relevant content.”).

Facebook profile.⁵² In *Leduc*, there was no such public information, and the defendant had not questioned the plaintiff about his Facebook profile because he only learned of its existence from the plaintiff's medical examination.

¶17 Nonetheless, the court in *Romano* cited *Leduc*, as well as several other Canadian decisions granting limited access to Facebook materials, as support for its decision to allow the defendants complete access to the plaintiff's social media accounts upon finding that the publicly available SNS evidence contradicted the plaintiff's claims.⁵³

¶18 Other courts have followed *Romano*'s approach of deciding whether a threshold showing has been met, and, if so, allowing complete access to the SNS accounts.⁵⁴ The approach has been followed by other New York state courts⁵⁵ and endorsed by its court of appeals.⁵⁶ Pennsylvania's state courts also follow the threshold approach.⁵⁷ And numerous

⁵² Simplified Rules cases do not permit discovery as of right, so other circumstances may arise where a party learns of the existence of another's Facebook profile, but cannot examine the person on the site's content. In such cases trial fairness dictates that the party who discovers the Facebook profile should enjoy some opportunity to ascertain and test whether the Facebook profile contains content relevant to any matter in issue in an action. One way to ensure this opportunity is to require the Facebook user to preserve and print-out the posted material, swear a supplementary affidavit of documents identifying any relevant Facebook documents and, where few or no documents are disclosed, permit the opposite party to cross-examine on the affidavit of documents in order to ascertain what content is posted on the site. Where the parties do not consent to following this process, recourse to the courts may be made.

Id. at para. 34.

⁵³ *Romano v. Steelcase, Inc.*, 907 N.Y.S.2d 640, 654–55 (Sup. Ct. 2010).

⁵⁴ None of these courts recognizes that *Romano* was following Canadian precedent that, unlike U.S. law, clearly required such a threshold showing.

⁵⁵ *Loporcaro v. City of N.Y.*, 950 N.Y.S.2d 723 (Sup. Ct. 2012) (ordering an in camera inspection of all Facebook postings, including deleted material, so the court may assess materiality and relevance, based on the fact that the plaintiff has posted at least some information publicly which may contradict his claims); *Winchell v. Lopiccio*, 954 N.Y.S.2d 421 (Sup. Ct. 2012) (denying a motion to compel authorization of Facebook account because the defendant failed to establish the factual predicate that Facebook information may be relevant).

⁵⁶ *Tapp v. N.Y. State Urban Dev. Corp.*, 958 N.Y.S.2d 392 (App. Div. 2013) (denying request for Facebook authorization where defendants failed to make a showing that the content would be relevant); *Nieves v. 30 Ellwood Realty LLC*, 966 N.Y.S.2d 808 (App. Term 2013) (remanding for in camera inspection of plaintiff's Facebook records because the defendant demonstrated that plaintiff's public profile contained photos probative of the extent of her injuries).

⁵⁷ *Largent v. Reed*, No. 2009-1823, 2011 WL 5632688, at *6 n.3, *7 (Pa. C.P. Nov. 8, 2011) (finding that the public portion of plaintiff's SNS profile gave a good faith basis for the defendant's request to access the private portion, and ordering the plaintiff to provide the defendant with her login and password for twenty-one days); *Zimmerman v. Weis Markets, Inc.*, No. CV-09-1535, 2011 WL 2065410, at *2–4 (Pa. C.P. May 19, 2011) (ordering disclosure of plaintiff's passwords and log-in names for SNS accounts because the public portions were inconsistent with plaintiff's claims of permanent injury and inability to enjoy life); *McMillen v. Hummingbird Speedway, Inc.*, No. 113-2010 CD, 2010 WL 4403285, at *4 (Pa. C.P. Sept. 9, 2010) (ordering the plaintiff to provide his SNS user names and passwords to the defendants because the public portion revealed comments about a fishing trip and car race attendance, while plaintiff alleged substantial injuries and loss of enjoyment of life); *see also Gallion v. Gallion*, No. FA114116955S, 2011 WL 4953451 (Conn. Super. Ct. Sept. 30, 2011) (ordering that attorneys exchange clients' Facebook and dating website passwords after husband reported seeing incriminating information on computer he shared with his wife).

federal district courts have also applied this standard, including courts in New York, Colorado, Nevada, Tennessee, and Michigan.⁵⁸

¶19 The reasoning of these courts is akin to finding that a plaintiff seeking substantial injuries has waived any right to privacy of SNS data by revealing some public content that contradicts those claims. As the court stated in *McMillen v. Hummingbird Speedway, Inc.*,

[a]ccessing only the public portion of [the plaintiff's] Facebook page, . . . the defendants have discovered posts they contend show that McMillen has exaggerated his injuries. Certainly a lack of injury and inability is relevant to their defense, and it is reasonable to assume that McMillen may have made additional observations about his travels and activities in private posts not currently available to the defendants. If they do exist, gaining access to them could help to prove either the truth or falsity of McMillen's alleged claims.⁵⁹

¶20 In addition, many courts are ordering wholesale access to a party's SNS account although it is not clear whether the court found any threshold required or met.⁶⁰ These courts treat information on private portions of SNS as being a single source, permissible or not, without any consideration of the relevance of individual aspects of the SNS account.⁶¹ In a recent case from the District of Colorado, a court granted a motion to

⁵⁸ *Potts v. Dollar Tree Stores, Inc.*, No. 3:11-cv-01180, 2013 WL 1176504, at *3 (M.D. Tenn. Mar. 20, 2013) (denying production where the defendant failed to produce "any evidentiary showing that Plaintiff's public Facebook profile contains information that will reasonably lead to the discovery of admissible evidence"); *Reid v. Ingerman Smith LLP*, No. CV 2012-0307(ILG)(MDG), 2012 WL 6720752, at *1–2 (E.D.N.Y. Dec. 27, 2012) (finding the photos and comments posted by the plaintiff on her publicly available Facebook pages probative, so private postings may likewise be relevant, but declining to require full disclosure of all SNS materials because not all will be relevant); *EEOC v. Original Honeybaked Ham Co. of Ga., Inc.*, No. 11-cv-02560-MSK-MEH, 2012 WL 5430974, at *2 (D. Colo. Nov. 7, 2012) (finding that where publicly available Facebook information from one class member was relevant, "each class member's social media content should be produced, albeit in camera in the first instance"); *Thompson v. Autoliv ASP, Inc.*, No. 2:09-cv-01375-PMP-VCF, 2012 WL 2342928 (D. Nev. June 20, 2012); *Glazer v. Fireman's Fund Ins. Co.*, No. 11 Civ. 4374(PGG)(FM), 2012 WL 1197167, at *5 (S.D.N.Y. Apr. 5, 2012) (ordering plaintiff to create a new SNS account, allowing her to access all her old and deleted chats, and turn over all chat transcripts to the defendant); *Tompkins v. Detroit Metro. Airport*, 278 F.R.D. 387, 389 (E.D. Mich. 2012) (denying defendant's motion to compel plaintiff to execute authorizations releasing Facebook account because defendant has not made a threshold showing that the requested information is likely to lead to relevant evidence).

⁵⁹ *McMillen*, 2010 WL 4403285, at *6.

⁶⁰ *Davenport v. State Farm Mutual Auto. Ins. Co.*, No. 3:11-cv-632-J-JBT, 2012 WL 555759 (M.D. Fla. Feb. 21, 2012) (limiting scope of request from "[a]ll photographs posted, uploaded, or otherwise added to any social networking sites or blogs . . . since the date of the accident alleged in the Complaint" to all such photographs *depicting the plaintiff*, regardless of who posted them); *Bass v. Miss Porter's Sch.*, No. 3:08cv1807 (JBA), 2009 WL 3724968 (D. Conn. Oct. 27, 2009); *Beswick v. North West Med. Ctr., Inc.*, No. 07-020592 CACE (03), 2011 WL 7005038 (Fla. Cir. Ct. Nov. 3, 2011).

⁶¹ Plaintiffs were ordered to turn over their SNS passwords and login information in *Largent*, 2011 WL 5632688 (Pa. C.P. Nov. 8, 2011); *Zimmerman*, 2011 WL 2065410 (Pa. C.P. May 19, 2011); *Romano v. Steelcase Inc.*, 907 N.Y.S.2d 650, 657 (N.Y. Sup. Ct. 2010) (ordering execution of a consent and authorization permitting the defendant to access the plaintiff's Facebook and MySpace accounts); *McMillen*, 2010 WL 4403285; *Beswick*, 2011 WL 7005038 (granting a motion to compel a response to an interrogatory which requested login and password information or, in the alternative, to provide a copy of all data for the previous five years, and ordering that the plaintiffs sign a consent and authorization to permit the defendants to gain access to the plaintiff's Facebook records); *Gatto v. United Air Lines, Inc.*, No. 10-

compel the plaintiff's entire Facebook history in a case alleging the use of excessive force in an arrest.⁶² The court found that the plaintiff's allegations of physical injury and emotional distress were broad enough to encompass his entire Facebook activity without limitation.⁶³

2. Both Underinclusive and Overinclusive

¶21 The cases discussed above have deservedly been criticized for ordering too much disclosure.⁶⁴ The blanket access to social media that is allowed to parties who are able to meet the threshold showing (or not required to meet a threshold) includes irrelevant and potentially very private content.

¶22 But also important is the fact that courts are on occasion ordering too *little* disclosure. There is no basis in the federal rules, or in the many state rules based on them, to require a preliminary showing that relevant discovery exists before allowing a party to request that discovery.⁶⁵ These courts forbid any discovery of social media if that threshold is not met.⁶⁶ Instead, under U.S. discovery rules, parties are generally entitled to relevant information from litigants contained in those sites regardless of the extent to which publicly available information contradicts a plaintiff's claims.⁶⁷

¶23 One source of the problem, of course, is that the parties' attorneys themselves often seek all access to SNS accounts rather than only seeking relevant information. In such a

cv-1090-ES-SCM, 2013 WL 1285285 (D.N.J. Mar. 25, 2013) (granting a request for an adverse inference instruction in a spoliation dispute arising out of the plaintiff's deletion of his Facebook account after being ordered by the court to execute an authorization for the release of documents and information from Facebook, and to change his account password to "alliedunited" to facilitate defendants' access).

⁶² Moore v. Miller, No. 10-cv-651-JLK, 2013 WL 2456114 (D. Colo. June 6, 2013).

⁶³ See *id.* at *2–3.

⁶⁴ Gensler, *supra* note 13, at 18 (noting that the court in *Romano* "effectively ordered the production of irrelevant information," and that *Largent* and *McMillen* made the same error); see also Mallory Allen & Aaron Orheim, Note, *Get Outta My Face[book]: The Discoverability of Social Networking Data and the Passwords Needed to Access Them*, 8 WASH. J.L. TECH. & ARTS 137, 150 (2012) ("Granting such sweeping access represents a break from traditional electronic discovery orders.").

⁶⁵ See Gensler, *supra* note 13, at 18–19 (questioning whether cases should be construed as requiring such a preliminary showing of relevance and stating that "if courts were to start requiring a predicate showing of relevance before allowing a party to seek discovery of *specific* content from social-media sites, that would constitute a barrier to discovery that does not exist in other contexts"). The closest analogy may be to the sampling allowed in electronic discovery cases where the parties argue that certain ESI is not reasonably accessible. Before requiring wholesale recovery of such ESI, courts may order a portion restored and base further disclosure on the relevance of that sample. See *Zubulake v. UBS Warburg LLC*, 217 F.R.D. 309, 323–24 (S.D.N.Y. 2003) (ordering defendant to restore information and produce information to plaintiff).

⁶⁶ See, e.g., *Potts v. Dollar Tree Stores, Inc.*, No. 3:11-cv-01180, 2013 WL 1176504, at *3 (M.D. Tenn. Mar. 20, 2013); *Tompkins v. Detroit Metro. Airport*, 278 F.R.D. 387, 388 (E.D. Mich. 2012); *Levine v. Culligan of Fla., Inc.*, No. 50-2011-CA-010339-XXXXMB, 2013 WL 1100404, at *6 (Fla. Cir. Ct. Jan. 29, 2013); *Tapp v. N.Y. State Urban Dev. Corp.*, 958 N.Y.S.2d 392 (App. Div. 2013); *McCann v. Harleysville Ins. Co.*, 910 N.Y.S.2d 614 (App. Div. 2010); *Fawcett v. Altieri*, 960 N.Y.S.2d 592 (Sup. Ct. 2013); *Brogan v. Rosenn, Jenkins & Greenwald, LLP*, No. 08 CV 6048, 2013 WL 1742689, at *6, *8 (Pa. C.P. Apr. 22, 2013); *Arcq v. Fields*, No. 2008-2430, slip op. at 3–4 (Pa. C.P. Dec. 8, 2011).

⁶⁷ See FED. R. CIV. P. 26(b)(1) ("Unless otherwise limited by court order, [p]arties may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense—including the existence, description, nature, custody, condition, and location of any documents or other tangible things and the identity and location of persons who know of any discoverable matter.").

case, a court would properly find that the party is engaging in a fishing expedition.⁶⁸ In a 2012 article, Professor Steven Gensler questioned whether early cases should be read as requiring a predicate showing of relevance in any cases other than those where the moving party sought blanket access to the SNS site, arguing that “*Tompkins* and *Romano* are best read as speaking to the showing required to obtain access to an entire account, not to whether a party must make a prima facie showing before it can make specific, targeted requests.”⁶⁹

¶24 Certainly, many court decisions arise out of requests for access to an entire account. Some courts do chastise the party that made the overbroad request, noting that a more tailored request would be appropriate.⁷⁰ But other courts that deny blanket access do not do so solely on the basis that the request is overbroad. Rather, they also stress that the showing that relevant evidence exists has not been met.⁷¹

¶25 More importantly, courts have denied access to SNS information because of a failure to meet the threshold showing even when the request is tailored. For instance, a Florida district court recently denied a plaintiff’s request for social media discovery from the defendants in a case for excessive force brought by the father of a deceased man who had been arrested by the defendants.⁷² The plaintiff did not seek all social media evidence from the defendants, instead requesting only social media communications “that relate in any way to the incident that is described in the Second Amended Complaint.”⁷³ Certainly, had the defendants discussed the arrest of the plaintiff’s son in Facebook postings, those communications would likely be relevant in the lawsuit concerning that arrest. But applying the threshold approach, the Florida court found no showing of the existence of relevant evidence and denied the discovery request in toto as a fishing expedition:

Here, Plaintiff simply contends that the requests are relevant because, “Plaintiff is seeking information about statements that Defendant Brown made about the incident at issue in this case, which could include admissions against interest, and could certainly lead to the discovery of admissible evidence.” The mere hope that Brown’s private text-messages, e-mails, and electronic communication might include an admission against interest, without more, is not a sufficient reason to require Brown to provide Plaintiff open access to his private communications with third parties.⁷⁴

Accordingly, the threshold approach has led courts to deny appropriate discovery in addition to granting too much discovery.

⁶⁸ See *Tompkins*, 278 F.R.D. at 389; *McCann*, 910 N.Y.S.2d at 615.

⁶⁹ Gensler, *supra* note 13, at 18 n.41.

⁷⁰ See *Howell v. Buckeye Ranch, Inc.*, No. 2:11-cv-1014, 2012 WL 5265170 (S.D. Ohio Oct. 1, 2012).

⁷¹ See *Arcq*, No. 2008-2430, slip op. at 2 (“We find that there lies one glaring, distinguishing factor that prevents us from [granting access]: Defendant’s request is not the result of viewing the public portion of Plaintiff’s profile.”); *Brogan*, 2013 WL 1742689, at *6 (“The Brogans have not established that Breault published information on the publicly viewable portion of her Facebook account which refutes or questions the veracity of her assertions in this case.”).

⁷² See *Salvato v. Miley*, No:5:12-CV-635-Oc-10PRL, 2013 WL 2712206 (M.D. Fla. June 11, 2013).

⁷³ *Id.* at *2.

⁷⁴ *Id.*

3. Wasting Judicial Resources

¶26 In the effort to provide an element of privacy protection, many courts have ordered in camera review of the SNS evidence.⁷⁵ Although this solution is an admirable attempt to protect litigants' privacy, it is untenable as a general approach. It wastes judicial resources and is not justified in the law.⁷⁶ In *Patterson v. Turner*,⁷⁷ the appellate court correctly found the lower court's order that the plaintiff produce all Facebook information after it had conducted an in camera review to be overbroad.⁷⁸ But rather than finding that the plaintiff should be ordered to produce only relevant information, the appellate court remanded for the lower court's own determination of what specific Facebook information is relevant and subject to disclosure.⁷⁹ Under this result, instead of counsel producing responsive information, the court itself must sift through the SNS account content and determine what is relevant.⁸⁰ There is no reason to trust litigants' counsel less because of the nature of social media; there is just as much risk of underproduction of other types of discovery left in the hands of counsel.⁸¹

¶27 Some courts recognize that the onus should be on counsel, not on the judge, to review discovery for relevance. As the court noted in *Fawcett v. Altieri*, "asking courts to review hundreds of transmissions 'in camera' should not be the all purpose solution to protect the rights of litigants. Courts do not have the time or resources to be the researchers for advocates seeking some tidbit of information that *may* be relevant in a tort claim."⁸²

¶28 Instead, parties should seek targeted social media discovery as part of regular discovery requests.⁸³ Just like requests for email and other communications, there will be

⁷⁵ See, e.g., *Offenback v. L.M. Bowman, Inc.*, No. 1:10-CV-1789, 2011 WL 2491371 (M.D. Pa. June 22, 2011); *Richards v. Hertz Corp.*, 953 N.Y.S.2d 654 (App. Div. 2012); *Nieves v. 30 Ellwood Realty LLC*, 966 N.Y.S.2d 808 (App. Term 2013); *Loporcaro v. City of N.Y.*, 950 N.Y.S.2d 723 (Sup. Ct. 2012). Another creative but also time-consuming solution for the judge is illustrated by *Barnes v. CUS Nashville, LLC*, No. 3:09-cv-00764, 2010 WL 2265668 (M.D. Tenn. June 3, 2010), where the magistrate judge offered to "friend" the third parties whose SNS pictures were relevant.

⁷⁶ See Gensler, *supra* note 13, at 25 ("Under standard discovery practice, a court generally should wait until the information holder makes his or her response after the initial review, and then get involved only if there is a dispute regarding objections to the request or the sufficiency of the production.").

⁷⁷ *Patterson v. Turner Const. Co.*, 931 N.Y.S.2d 311 (App. Div. 2011).

⁷⁸ See *id.* at 312.

⁷⁹ See *id.*

⁸⁰ See *EEOC v. Original Honeybaked Ham Co. of Ga.*, No. 11-cv-02560-MSK-MEH, 2012 WL 5430974 (D. Colo. Nov. 7, 2012); *Thompson v. Autoliv ASP, Inc.*, No. 2:09-cv-01375-PMP-VCF, 2012 WL 2342928 (D. Nev. June 20, 2012); *Bass v. Miss Porter's School*, No. 3:08cv1807 (JBA), 2009 WL 3724968 (D. Conn. Oct. 27, 2009).

⁸¹ See *Hubbard v. Potter*, 247 F.R.D. 27, 29 (D.D.C. 2008) ("Speculation that there is more [responsive discovery] will not suffice; if the theoretical possibility that more documents exist sufficed to justify additional discovery, discovery would never end."); Gensler, *supra* note 13, at 26 ("The last thing courts want—or have the practical ability to do—is to undertake their own search or review whenever the requesting party suspects the response might not be complete.").

⁸² *Fawcett v. Altieri*, 960 N.Y.S.2d 592, 597–98 (Sup. Ct. 2013); see also *Tompkins v. Detroit Metro. Airport*, 278 F.R.D. 387, 389 n.4 ("I decline the parties' alternative suggestion that I conduct an *in camera* review of Plaintiff's private Facebook postings. Such review is ordinarily utilized only when necessary to resolve disputes concerning privilege; it is rarely used to determine relevance.") (internal quotation marks omitted).

⁸³ See Gensler, *supra* note 13, at 23 ("The longstanding general rule is that people review their own records when responding to discovery requests.").

some relevant and some irrelevant information. Counsel has the task of sorting through it and figuring out what is responsive. If responsive information is improperly withheld, the requesting party has all the normal tools at his disposal to compel production.⁸⁴

C. Parties Improperly Seeking Blanket Access Directly from Social Media Sites

¶29 Exacerbating the issue is the tendency of litigants to subpoena social media information from SNSs directly.⁸⁵ The Federal Rules of Civil Procedure have been revised in an effort to reduce the cost and time expended in disputes related to electronic discovery⁸⁶ and to decrease the involvement of judges in unnecessary discovery disputes.⁸⁷ However, many litigants' approach to social media discovery has resulted in just the opposite: counsel often seek discovery not from the other party but directly from the SNS itself, which consequently guarantees motion practice before the court.

¶30 Seeking direct access to SNS information from the providers may violate the Stored Communications Act,⁸⁸ which prohibits remote computing and electronic communication service providers from divulging the contents of a communication while in storage.⁸⁹ Some courts have quashed subpoenas on this basis.⁹⁰

¶31 In addition, because the SNS providers will not review the discovery for relevance before complying with a subpoena, seeking this information directly from the SNS providers allows an end-run around the relevancy requirements of the rules. Indeed, the SNSs themselves are loath to respond to such subpoenas at all without a court order.⁹¹

⁸⁴ See *id.* at 26 (“[In] the social media context, courts would have no reason to undertake an in camera review of a party’s social-media content unless the requesting party had some specific, non-speculative grounds to argue that the account contained responsive materials that the account holder had failed to disclose.”).

⁸⁵ See, e.g., *Ledbetter v. Wal-Mart Stores, Inc.*, No. 06-cv-01958-WYD-MJW, 2009 WL 1067018 (D. Colo. Apr. 21, 2009).

⁸⁶ See FED. R. CIV. P. 26(b)(1) advisory committee’s note (discussing reduction of scope based on concerns about cost and delay); see also THE SEDONA CONFERENCE, THE SEDONA CONFERENCE COOPERATION PROCLAMATION 1 (2008) (“Over-contentious discovery is a cost that has outstripped any advantage in the face of ESI and the data deluge. It is not in anyone’s interest to waste resources on unnecessary disputes, and the legal system is strained by ‘gamesmanship’ or ‘hiding the ball,’ to no practical effect.”); *id.* at 2 (“The 2006 amendments to the Federal Rules specifically focused on discovery of ‘electronically stored information’ and emphasized early communication and cooperation in an effort to streamline information exchange, and avoid costly unproductive disputes.”).

⁸⁷ “In addition to rising monetary costs, courts have seen escalating motion practice, overreaching, obstruction, and extensive, but unproductive discovery disputes—in some cases precluding adjudication on the merits altogether—when parties treat the discovery process in an adversarial manner.” THE SEDONA CONFERENCE, *supra* note 86, at 1. The rules require that parties attempt to resolve any discovery dispute before moving for a protective order, FED. R. CIV. P. 26(c)(1), or moving to compel discovery, FED. R. CIV. P. 37(a)(1). See *Romero v. Allstate Ins. Co.*, 271 F.R.D. 96, 109 (E.D. Pa. 2010) (“The Federal Rules of Civil Procedure, case law, and the *Sedona Principles* all further emphasize that electronic discovery should be a party-driven process.”) (internal quotation marks omitted).

⁸⁸ See *Ward*, *supra* note 21, at 566.

⁸⁹ See 18 U.S.C. §§ 2701–12 (2012).

⁹⁰ See, e.g., *Crispin v. Christian Audigier, Inc.*, 717 F. Supp. 2d 965, 991 (C.D. Cal. 2010); *In re Subpoena Duces Tecum to AOL, LLC*, 550 F. Supp. 2d 606, 614 (E.D. Va. 2008); *O’Grady v. Superior Court*, 44 Cal. Rptr. 3d 72, 89 (Ct. App. 2006).

⁹¹ Facebook has a policy of not providing information in response to civil subpoenas. In response to the question whether someone can obtain Facebook contents, Facebook states:

Thus, the issue ends up in front of the court anyway, even without the request going directly to a party. Accordingly, too many judicial resources are devoted to a process that should largely operate without court involvement.⁹² Only in the situation where a person has deleted arguably relevant information on his or her SNS account would the provider need to be involved.⁹³ Otherwise, the information is within the possession, custody, or control of the party itself and should be requested from the party.⁹⁴

¶32 A recent order in the Eastern District of New York specifically recognized the impropriety of seeking access to SNS postings from the third-party provider rather than from the party herself. In *Giacchetto v. Patchogue-Medford Union Free School District*, the magistrate judge denied the defendant's request for authorizations for the release of records from the SNS hosts.⁹⁵ The court found the decision in *Howell* "ordering plaintiff's counsel to access plaintiff's social media accounts and produce responsive information as opposed to having plaintiff provide defendant with her usernames and passwords," to be "persuasive and reasonable" and therefore directed that plaintiff's counsel make the appropriate relevant production.⁹⁶

D. Movement Toward a Better Approach

¶33 An increasing number of courts reject the all-or-nothing and threshold approaches and realize that discovery of social media, like other discovery, must focus on relevance of individual content, not wholesale access.⁹⁷

Federal law prohibits Facebook from disclosing user content (such as messages, Timeline posts, photos, etc.) in response to a civil subpoena. Specifically, the Stored Communications Act, 18 U.S.C. § 2701 et seq., prohibits Facebook from disclosing the contents of an account to any non-governmental entity pursuant to a subpoena or court order.

Parties to civil litigation may satisfy discovery requirements relating to their Facebook accounts by producing and authenticating contents of their accounts and by using Facebook's "Download Your Information" tool, which is accessible through the Settings drop down menu.

If a user cannot access content because he or she disables or deleted his or her account, Facebook will, to the extent possible, restore access to allow the user to collect and produce the account's content. Facebook preserves user content only in response to a valid law enforcement request.

May I Obtain Contents of a User's Account from Facebook Using a Civil Subpoena?, FACEBOOK, <https://www.facebook.com/help/133221086752707?sr=1&sid=0wo6y3b2rP0ejHsrD> (last visited Mar. 26, 2014).

⁹² While the advisory committee, in discussing rules changes, stresses early judicial involvement in case management, in no way does the committee encourage more discovery motion practice. *See infra* Section III. C.

⁹³ *Id.*; *see also* *Allied Concrete Co. v. Lester*, 736 S.E.2d 699 (Va. 2013).

⁹⁴ *See* FED. R. CIV. P. 34.

⁹⁵ *Giacchetto v. Patchogue-Medford Union Free Sch. Dist.*, 293 F.R.D. 112 (E.D.N.Y. May 6, 2013).

⁹⁶ *Id.* at 117 (citing *Howell v. Buckeye Ranch, Inc.*, No. 2:11-cv-1014, 2012 WL 5265170, at *1 (S.D. Ohio Oct. 1, 2012)).

⁹⁷ *See* *Trail v. Lesko*, No. GD-10-017249, 2012 Pa. Dist. & Cnty. Dec. LEXIS 194, at *20–21 (C.P. Allegheny County July 3, 2012) (describing the Pennsylvania threshold approach, and noting that other jurisdictions "have wrestled to establish a middle ground between the wholesale denial of the request on the one hand and the granting of unlimited access to the user's profile on the other. Thus, some jurisdictions, when faced with these questions, fashion more narrowly tailored discovery orders and are more likely to

¶34 In an influential decision, a federal district court in Indiana rejected the threshold showing/wholesale access approach in favor of traditional application of the rules.⁹⁸ In *EEOC v. Simply Storage*, an employment discrimination case, the employer sought broad access to the claimants' Facebook and MySpace accounts. The court found that privacy concerns themselves were not sufficient to prevent access, but neither should the defendant be entitled to rummage through the claimants' SNS accounts without limitation:

Discovery of SNS requires the application of basic discovery principles in a novel context. . . . [T]he main challenge in this case is not one unique to electronically stored information generally or to social networking sites in particular. Rather, the challenge is to define appropriately broad limits—but limits nevertheless—on the discoverability of social communications in light of a subject as amorphous as emotional and mental health, and to do so in a way that provides meaningful direction to the parties.⁹⁹

¶35 In doing so, the court rejected the approach of other decisions allowing broad access because of the nature of the damages sought: “[T]he simple fact that a claimant has *had* social communications is not necessarily probative of the particular mental and emotional health matters at issue in the case. Rather, it must be the substance of the communication that determines relevance.”¹⁰⁰ Similarly, the court reasoned that allegations of depression, stress disorders, and like injuries do not automatically render all SNS communications relevant.¹⁰¹

¶36 The *Simply Storage* court also emphasized that the role of counsel in discovery of social media is no different from other contexts: “[I]awyers are frequently called upon to make judgment calls—in good faith and consistent with their obligations as officers of the court—about what information is responsive to another party’s discovery requests. Discovery is intended to be a self-regulating process that depends on the reasonableness and cooperation of counsel.”¹⁰² Therefore, the court ordered the plaintiffs’ counsel to gather relevant evidence from the SNS accounts and provide it to opposing counsel. The court explained, “[a]s with discovery generally, *Simply Storage* can further inquire of counsel and the claimants (in their depositions) about what has and has not been produced and can challenge the production if it believes the production falls short of the requirements of this order.”¹⁰³

rely on counsel to peruse the client’s profile for relevant information in the first instance.”).

⁹⁸ *EEOC v. Simply Storage Mgmt., LLC*, 270 F.R.D. 430 (S.D. Ind. 2010).

⁹⁹ *Id.* at 434.

¹⁰⁰ *Id.* at 435; *see also* *Rozell v. Ross-Holst*, No. 05 Civ. 2936(JGK)JCF, 2006 WL 163143, at *33 (S.D.N.Y. Jan. 20, 2006) (“[While] anything that a person says or does might in some theoretical sense be reflective of her emotional state, . . . that is hardly justification for requiring production of every thought she may have reduced to writing or, indeed, the depositions of everyone she may have talked to.”).

¹⁰¹ The court also found that the plaintiffs’ position that they should produce only communications that directly reference the matters alleged in the complaint is too restrictive. *Simply Storage Mgmt., LLC*, 270 F.R.D. at 435.

¹⁰² *Id.* at 436.

¹⁰³ *Id.* at 436. *See also* *Mackelprang v. Fidelity Nat’l Title Agency of Nev., Inc.*, No. 2:06-cv-00788-JCM-GWF, 2007 WL 119149, at *8 (D. Nev. Jan. 9, 2007) (noting that it is the obligation of counsel, in responding to requests for production, to produce what is relevant: “Defendants are entitled to discover information relevant to Plaintiff’s alleged emotional distress and her mental condition, which she has

¶37 Other courts have followed this more sensible, traditional approach.¹⁰⁴ In *Brogan v. Rosenn, Jenkins, and Greenwald, LLP*, the court rejected a request for login information:

The Brogans do not request copies of Facebook messages concerning specific subjects during particular time periods. Rather, the Brogans seek to compel Breault to provide them with her Facebook username and password so that the Brogans may have unbridled access to any and all information contained on Breault's Facebook account.

....

A discovery request seeking carte blanche access to private social networking information is overly intrusive, would cause unreasonable embarrassment and burden in contravention of Pa.R.C.P. 4011(b), and is not properly tailored "with reasonable particularity" as required by the Pennsylvania Rules of Civil Procedure If the Brogans obtain Breault's Facebook username and password, they would have an unrestricted license to peruse her entire Facebook account, and view highly sensitive information and potentially confidential communications that have no relevance to this lawsuit, including comments that were authored by third parties such as her Facebook "friends."¹⁰⁵

¶38 Of course, just as with other discovery, if disputes arise as to whether the production is appropriate, then the parties will need to get the court involved.¹⁰⁶

¶39 In a recent decision from the Eastern District of New York, discussed above in the context of direct requests to SNSs, the court specifically recognized that the approach of other courts has been both overinclusive and underinclusive. In *Giacchetto*,¹⁰⁷ the

placed at issue in this case. . . . [i]f [information relevant to assessing the credibility of her emotional distress claims] exists in the email messages, Defendant is entitled to obtain its production." But the proper method for doing so is "to serve upon Plaintiff properly limited requests for production of *relevant* email communications." (emphasis in original).

¹⁰⁴ See, e.g., *Reid v. Ingerman Smith LLP*, No. CV 2012-0307(ILG)(MDG), 2012 WL 6720752 (E.D.N.Y. Dec. 27, 2012); *Howell v. Buckeye Ranch, Inc.*, No. 2:11-cv-1014, 2012 WL 5265170 (S.D. Ohio Oct. 1, 2012); *Robinson v. Jones Lang LaSalle Ams., Inc.*, No. 3:12-cv-00127-PK, 2012 WL 3763545, at *2 (D. Or. Aug. 29, 2012) (relying on *Simply Storage*, ordering plaintiff to produce communications on SNS that "reveal, refer, or relate to: any significant emotion, feeling, or mental state allegedly caused by defendant's conduct; or events or communications that could reasonably be expected to produce a significant emotion, feeling, or mental state allegedly caused by defendant's conduct" and noting that the court "expects counsel to determine what information falls within the scope of this Court's order in good faith and consistent with their obligations as officers of the court."); *Mailhoit v. Home Depot U.S.A., Inc.*, 285 F.R.D. 566 (C.D. Cal. 2012); *Sourdiffe v. Tex. Roadhouse Holdings, LLC*, No. 3:10-CV-0408 (TJM/DEP), 2011 WL 7560647 (N.D.N.Y. Oct. 24, 2011); *Held v. Ferrellgas, Inc.*, No. 10-2393-EFM, 2011 WL 3896513 (D. Kan. Aug. 31, 2011); *Holter v. Wells Fargo and Co.*, 281 F.R.D. 340 (D. Minn. 2011); *Patterson v. Turner Const. Co.*, 931 N.Y.S.2d 311, 312 (App. Div. 2011).

¹⁰⁵ *Brogan v. Rosenn, Jenkins & Greenwald, LLP*, No. 08 CV 6048, 2013 WL 1742689, at *6-8 (Pa. C.P. Apr. 22, 2013) (internal citations omitted); see also *Mackelprang*, 2007 WL 119149 at *7 ("Ordering Plaintiff to execute the consent and authorization form for release of all of the private email messages on Plaintiff's Myspace.com internet accounts would allow Defendants to cast too wide a net for any information that might be relevant and discoverable.").

¹⁰⁶ See *Gatto v. United Air Lines, Inc.*, No. 10-cv-1090-ES-SCM, 2013 WL 1285285 (D.N.J. Mar. 25, 2013); *Allied Concrete Co. v. Lester*, 736 S.E.2d 699 (Va. 2013).

¹⁰⁷ *Giacchetto v. Patchogue-Medford Union Free Sch. Dist.*, 293 F.R.D. 112 (E.D.N.Y. May 6, 2013).

plaintiff sued for wrongful termination. The defendant sought broad access to the plaintiff’s social media accounts. The court noted the “threshold evidentiary showing” that had been required in cases like *Romano*, and stated that:

This approach can lead to results that are both too broad and too narrow. On the one hand, a plaintiff should not be required to turn over the private section of his or her Facebook profile (which may or may not contain relevant information) merely because the public section undermines the plaintiff’s claims. On the other hand, a plaintiff should be required to review the private section and produce any relevant information, regardless of what is reflected in the public section. The Federal Rules of Civil Procedure do not require a party to prove the existence of relevant material before requesting it. Furthermore, this approach improperly shields from discovery the information of Facebook users who do not share any information publicly.¹⁰⁸

Therefore, the court followed the traditional approach and ordered disclosure of “specific references to the emotional distress she claims she suffered or treatment she received” in connection with her claim, as well as references to alternative causes of her distress.¹⁰⁹

III. FINDING PRIVACY IN A SEA OF E-DISCOVERY

A. Putting Social Media in Context

1. The Format

¶40 One argument for seeking wholesale access to SNS accounts, either from the party or from the sites themselves, is that ordinary discovery of this material is not adequate to show its functionality or changes to its content. For example, producing hard copies of a page showing a person’s “status update” will not reveal the names of all the friends who “liked” that update, nor will it reveal deleted content. But parties are capable of obtaining this information (if it is relevant) with a variety of interrogatories, document requests, and deposition questions. Facebook itself directs its users on how to download all of their content.¹¹⁰ If there is a specific need for relevant SNS metadata in a particular case, that need would give a party a basis for seeking additional material.

2. The Public Nature

¶41 Underlying many courts’ reasoning in allowing wholesale access to social media discovery is a fundamental misunderstanding of social media sites. Rather than treating those sites as simply another location for relevant discoverable information, these courts treat them like a single treasure chest to which litigants are given the keys or not.¹¹¹ They

¹⁰⁸ *Id.* at 114 n.1.

¹⁰⁹ *Id.* at 116.

¹¹⁰ *See In re White Tail Oilfield Services, L.L.C.*, No. 11-0009, 2012 WL 4857777, at *3 (E.D. La. Oct. 11, 2012); *see also May I Obtain Contents of a User’s Account from Facebook Using a Civil Subpoena?*, *supra* note 91.

¹¹¹ *See supra* note 61 (listing cases).

consider the format in which SNS information is communicated as being tantamount to a waiver of any of the ordinary protection against irrelevant discovery. As one court put it,

Facebook, MySpace and their ilk are social network computer sites people utilize to connect with friends and meet new people. That is, in fact, their purpose, and they do not bill themselves as anything else. Thus, while it is conceivable that a person could use them as forums to divulge and seek advice on personal and private matters, it would be unrealistic to expect that such disclosures would be considered confidential.¹¹²

Therefore, the court held that the defendant was entitled to access to that content, regardless of its relevance.

¶42 Similarly, the *Zimmerman*¹¹³ court noted:

[b]y definition, a social networking site is the interactive sharing of your personal life with others; the recipients are not limited in what they do with such knowledge. With the initiation of litigation to seek a monetary award based upon limitations or harm to one's person, any relevant, non-privileged information about one's life that is shared with others and can be gleaned by defendants from the interest is *fair game* in today's society.¹¹⁴

¶43 While these observations might be relevant to whether litigants have a blanket privacy argument for protection of SNS information, they are not pertinent in a discoverability context. Our rules have never allowed blanket access to a person's email account simply because those emails might have multiple recipients or otherwise are not "confidential."¹¹⁵

¶44 The analogies used by these courts further complicate the analysis of social media as a source of discovery. *Fawcett* likens production of Facebook information to production of a diary¹¹⁶—in other words, privacy is not a barrier to production since courts order disclosure of private materials like diaries.¹¹⁷ The court in *EEOC v. Honeybaked Ham Co.* analogized social media content to a file folder titled "Everything About Me" which the plaintiffs have shared with others:

¹¹² *McMillen v. Hummingbird Speedway, Inc.*, No. 113-2010 CD, 2010 WL 4403285 (Pa. C.P. Sept. 9, 2010).

¹¹³ *Zimmerman v. Weis Mkts., Inc.*, No. CV-09-1535, 2011 WL 2065410 (Pa. C.P. May 19, 2011).

¹¹⁴ *Id.* at *3 (emphasis added); *see also* *Mazzarella v. Mount Airy #1, LLC*, No. 1798 Civil 2009 (Pa. C.P. Nov. 7, 2012) ("Those who elect to use social media, and place things on the internet for viewing, sharing and use with others, waives [sic] an expectation of privacy.").

¹¹⁵ *See* FED. R. CIV. P. 26(b)(1) (limiting the scope of discovery to "nonprivileged matter that is relevant to any party's claim or defense" or, upon a showing of good cause to "any matter relevant to the subject matter involved in the action"); *see also* *Seattle Times Co. v. Rhinehart*, 467 U.S. 20, 35 (1984) ("The Rules do not distinguish between public and private information.").

¹¹⁶ *Fawcett v. Altieri*, 960 N.Y.S.2d 592, 597 (Sup. Ct. 2013); *see also* *Patterson v. Turner Const. Co.*, 931 N.Y.S.2d 311, 312 (App. Div. 2011) (noting that personal diaries are not shielded from discovery just because they are private, but reversing a blanket order of production in favor of a more specific identification of relevant Facebook information).

¹¹⁷ This leaves aside the fact that the diary as a whole must have been found likely to lead to the discovery of relevant evidence; otherwise, only parts of it should be produced.

If there are documents in this folder that contain information that is relevant or may lead to the discovery of admissible evidence relating to this lawsuit, the presumption is that it should be produced. The fact that it exists in cyberspace on an electronic device is a logistical and, perhaps, financial problem, but not a circumstance that removes the information from accessibility by a party opponent in litigation.¹¹⁸

¶45 The problem is that these analogies may explain why social media is free game for discovery, but they make no distinction among the many disparate contents of a social media account, some of which may be relevant and many of which may not.

¶46 In fact, SNS content is better analogized to a file cabinet containing many different materials, including a diary and personal files, any of which is discoverable only if it is relevant.¹¹⁹ A better approach can be found in *Howell*,¹²⁰ where the court denied a broad SNS request, reasoning that “[t]he fact that the information defendants seek is in an electronic file as opposed to a file cabinet does not give them the right to rummage through the entire file.”¹²¹

B. What Is the Implication of Using Privacy Settings?

¶47 A primary source of the confusion underlying social media discovery is the conflation of concepts of privacy with traditional discovery. The public or private nature of SNS content is irrelevant to whether such content is subject to discovery. But the fact that content is subject to discovery does not mean there are no privacy protections.

¶48 When an SNS user chooses to limit the audience with whom she shares her content, that choice should matter.¹²² The problem is whether, and to what extent, this affirmative limitation matters in the discovery context as opposed to others. Under current law, privacy settings should influence the level of Fourth Amendment protection given SNS content in the face of government and law enforcement searches, as well as the user’s reasonable expectation of privacy in the tort context.¹²³ If a person has restricted her privacy settings, she is more likely to have a reasonable expectation of privacy in those communications. But in the civil discovery context the rules make little distinction between private and public information.¹²⁴ The most salient distinction is an obvious one:

¹¹⁸ *EEOC v. Original Honeybaked Ham Co. of Ga., Inc.*, No. 11-cv-02560-MSK-MEH, 2012 WL 5430974, at *1 (D. Colo. Nov. 7, 2012).

¹¹⁹ The New York Appellate Court has recognized this. In *Patterson*, 931 N.Y.S.2d at 312, the court noted that personal diaries are not shielded from discovery just because they are private, and reversed a blanket order of production and remanded “for a more specific identification of plaintiff’s Facebook information that is relevant, in that it contradicts or conflicts with plaintiff’s alleged restrictions, disabilities, and losses, and other claims.”

¹²⁰ *Howell v. Buckeye Ranch, Inc.*, No. 2:11-cv-1014, 2012 WL 5265170 (S.D. Ohio Oct. 1, 2012).

¹²¹ *Id.* at*1.

¹²² See Allyson W. Haynes, *Virtual Blinds: Finding Online Privacy in Offline Precedents*, 14 VAND. J. ENT. & TECH. L. 603, 647 (2012) (arguing that, in analyzing whether a person has a reasonable expectation of privacy in an online disclosure, the court should consider that person’s use of privacy settings limiting disclosure in online social networks).

¹²³ *Id.*

¹²⁴ See *Seattle Times Co. v. Rhinehart*, 467 U.S. 20, 30 (1984).

if privacy settings are set to “public,” litigants can obtain the information without the necessity of filing any discovery request at all.¹²⁵

¶49 Under the federal rules and the many state systems modeled thereon, information in the possession or control of others is fair game for discovery requests as long as it is not privileged and is relevant.¹²⁶ In *Seattle Times Co. v. Rhinehart*, a suit brought by a religious group leader against publishers and authors for defamation, the defendants sought discovery of the group’s donors and members.¹²⁷ The trial court noted that the plaintiffs had a recognizable privacy interest in the financial affairs of their organization, and so issued a protective order prohibiting the media parties from publishing, disseminating or using the information except in that case. In considering the appeal by those parties based on their First Amendment rights, the Supreme Court stressed that protective orders under Rule 26(c) are an important check on the liberal scope of pretrial discovery:

Because of the liberality of pretrial discovery permitted by Rule 26(b)(1), it is necessary for the trial court to have the authority to issue protective orders conferred by Rule 26(c). It is clear from experience that pretrial discovery by depositions and interrogatories has a significant potential for abuse. This abuse is not limited to matters of delay and expense; discovery also may seriously implicate privacy interests of litigants and third parties. *The Rules do not distinguish between public and private information.* Nor do they apply only to parties to the litigation, as relevant information in the hands of third parties may be subject to discovery.

There is an opportunity, therefore, for litigants to obtain—incidentally or purposefully—information that not only is irrelevant but if publicly released could be damaging to reputation and privacy. The government clearly has a substantial interest in preventing this sort of abuse of its processes.¹²⁸

¶50 The Court recognized that there was concern about undue and uncontrolled discovery, “[b]ut until and unless there are major changes in the present Rules of Civil Procedure, reliance must be had on what in fact and in law are ample powers of the district judge to prevent abuse.”¹²⁹ Rule 26(c) represents one of those powers: “[a]lthough the Rule contains no specific reference to privacy or to other rights or interests that may be implicated, such matters are implicit in the broad purpose and language of the Rule.”¹³⁰

¶51 Even if information is forbidden from disclosure by the Privacy Act, it is potentially discoverable. As the district court noted in *Hassan v. United States*,¹³¹

¹²⁵ See *Information We Receive and How It is Used*, FACEBOOK, <https://www.facebook.com/about/privacy/your-info> (last visited Mar. 26, 2014) (“Choosing to make something public is exactly what it sounds like: anyone, including people off Facebook, will be able to see it.”).

¹²⁶ See FED. R. CIV. P. 26.

¹²⁷ See *Seattle Times*, 467 U.S. 20.

¹²⁸ *Id.* at 34–35 (emphasis supplied) (internal citations omitted).

¹²⁹ *Id.* at 34 n.20 (quoting *Herbert v. Lando*, 441 U.S. 153, 176–77 (1979)).

¹³⁰ *Id.* at 20 n.21.

¹³¹ *Hassan v. United States*, No. C05-1066C, 2006 WL 681038 (W.D. Wash. Mar. 15, 2006).

“general concerns of privacy are insufficient to justify the refusal to answer Plaintiffs’ discovery requests. The scope of discovery in federal court is very broad. . . . Even where information is subject to the protections of the Privacy Act of 1974, ‘a party can invoke discovery of materials protected by the Privacy Act through the normal discovery process and according to the usual discovery standards, and the test of discoverability is the relevance standard of Rule 26(b)(1) of the Federal Rules of Civil Procedure.’”¹³²

¶52

Thus information arguably deemed private is not immune from discovery under our rules, but instead is capable of protection based on protective orders under Rule 26(b)(2)(C)(iii) or Rule 26(c),¹³³ confidentiality orders, and the use of in camera inspections.¹³⁴ The types of personal information that have been recognized as deserving protection under these measures include medical¹³⁵ and psychiatric¹³⁶ records, police personnel files,¹³⁷ prison files,¹³⁸ information presenting a threat to physical security,¹³⁹ and information that otherwise invades a person’s privacy without a showing of need.¹⁴⁰

¹³² *Id.* at *2 (quoting *Laxalt v. McClatchy*, 809 F.2d 885, 889 (D.C. Cir. 1987)). In *Laxalt*, the court of appeals did note that a court might have a heightened responsibility to utilize devices such as protective orders and in camera inspection where information might be protected by the Privacy Act. *Id.* at 2 n.5.

¹³³ See *Bennett v. Kingsbridge Heights Rehabilitation Care Ctr.*, No. 07 Civ. 9456(LAK), 2009 WL 3294301, at *3 (S.D.N.Y. Oct. 8, 2009) (“When discovery is sought by a party in a civil case, the Federal Rules of Civil Procedure authorize a judge to preclude certain discovery if ‘the burden . . . of the proposed discovery outweighs its likely benefit’ The word ‘burden’ also includes ‘risks to . . . physical security and privacy.’”) (internal citations omitted).

¹³⁴ See *Laxalt*, 809 F.2d at 889 (finding that material protected by the Privacy Act was not immune from pretrial disclosure, but a court might have a heightened responsibility in that situation to utilize devices such as protective orders and in camera inspection).

¹³⁵ *Barker v. Barker*, 909 So.2d 333, 338 (Fla. Dist. Ct. App. 2005) (“By failing to provide for an in camera inspection of Hugh’s medical records to prevent disclosure of information that is not relevant to the litigation, the discovery order departed from the essential requirements of the law.”).

¹³⁶ *Soto v. City of Concord*, 162 F.R.D. 603, 618–19 (N.D. Cal. 1995) (considering privacy concerns raised by production of psychiatric evaluations, psychological and physical health records of police officers).

¹³⁷ *Id.* at 616–17; *Rogers v. G.J. Giurbino*, 288 F.R.D. 469, 484–85 (S.D. Cal. 2012) (finding privacy claims in response to discovery request in prisoner 1983 claim outweighed by need for the discovery); *King v. Conde*, 121 F.R.D. 180, 190 (E.D.N.Y. 1988) (finding that a showing of need must be made before placing the burden of in camera inspection on the magistrate, and recommending the use of protective orders restricting disclosure to the plaintiff and the plaintiff’s attorney, or to the plaintiff’s attorney alone, and suggesting redaction by the magistrate of “sensitive bits of information not useful to the plaintiffs,” such as officers’ home addresses, in a dispute over discovery of personnel files in a civil rights action).

¹³⁸ *Labrew v. City of N.Y.*, No. 07 Civ. 4641 (DAB)(DFE), 2009 WL 3747165 (S.D.N.Y. Nov. 5, 2009) (denying under Federal Rule of Civil Procedure 26(b)(2)(C)(iii) production of prison log sheet based on privacy rights of prisoners whose names would be disclosed).

¹³⁹ *Bennett v. Kingsbridge Heights Rehabilitation Care Ctr.*, No. 07 Civ. 9456(LAK), 2009 WL 3294301 (S.D.N.Y. Oct. 8, 2009) (protecting from disclosure names of employees who complained about threats constituting unfair labor practices).

¹⁴⁰ *Stampf v. Long Island R.R. Co.*, No. 07-CV-3349 (SMG), 2009 WL 3628109, at *2 (E.D.N.Y. Oct. 27, 2009) (granting protective order against production of witness’s claims, grievance, arbitration and litigation files with his employer: “the nature of the material is such that its production would invade the privacy of Mr. Jackson, who is not a party to the action and finds himself enmeshed in it only because he happened to be present when certain events in dispute took place. In contrast, the importance of the discovery at issue to resolving the issues in the case is, at best, minimal.”).

C. Narrowing the Scope of Discovery

¶53 Discovery has grown by leaps and bounds given the fact that so much more of our communications are recorded and stored. Conversations that would have taken place on the telephone, remembered only by the parties to it, are now recorded as chat sessions, text messages, or email messages.¹⁴¹ The changes in discovery that have been wrought by the Internet, cloud computing, social media and other electronic discovery necessitate that we re-think our rules. Privacy should be a basis for limiting discovery, although it should be balanced against a litigant's right to seek relevant documents. And it should not be based solely on privacy settings, which could lead to misuse of those settings. Instead, we need to balance intrusiveness against the permissible search for the truth.

¶54 One potential solution to overbroad discovery in general that has been proposed by the Advisory Committee on Civil Rules is to contain the scope of discovery in two ways.¹⁴² First, the revised rule would restrict the defined scope of discovery to information that is “proportional to the needs of the case considering the amount in controversy, the importance of the issues at stake in the action, the parties’ resources, the importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit.”¹⁴³ Second, the proposal would delete the following two sentences currently in Rule 26(b)(1): “For good cause, the court may order discovery of any matter relevant to the subject matter involved in the action. Relevant information need not be admissible at the trial if the discovery appears reasonably calculated to lead to the discovery of admissible evidence.”¹⁴⁴ Those sentences would be replaced by the following: “Information within this scope of discovery need not be admissible in evidence to be discoverable.”¹⁴⁵

¶55 The changes arise out of the conference held at Duke University School of Law in May 2010.¹⁴⁶ The subcommittee from the Duke Conference noted that:

¹⁴¹ Ralph Losey refers to this phenomenon as “TMI.” See Ralph Losey, *Rethinking Relevance: A Call to Modify the Rules of Discovery*, E-DISCOVERY TEAM (Jan. 24, 2011, 8:08 PM), <http://e-discoveryteam.com/2011/01/24/rethinking-relevancy-a-call-to-change-the-rules-to-narrow-the-scope-of-ESI-relevance>.

¹⁴² Memorandum from Hon. David G. Campbell, Chair, Advisory Committee on Federal Rules of Civil Procedure to Hon. Jeffrey S. Sutton, Chair, Standing Committee on Rules of Practice and Procedure 9–11 (May 8, 2013), available at <http://www.uscourts.gov/uscourts/RulesAndPolicies/rules/Reports/CV05-2013.pdf>. [hereinafter Advisory Committee Report]; see Henry Kelston, *Are We on the Cusp of Major Changes to E-Discovery Rules?*, LAW TECH. NEWS (Apr. 17, 2013), http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202596362366&Are_We_on_the_Cusp_of_Major_Changes_to_EDiscovery_Rules&slreturn=20130420162952.

¹⁴³ Advisory Committee Report, *supra* note 142, at 10, 30.

¹⁴⁴ *Id.* at 10–11, 30. The rules were changed in 2000 to require a court order for the broader “subject matter” scope of discovery, but have been largely ineffective at limiting the scope of discovery. See *id.* at 11 (“Despite the 2000 amendment, many cases continue to cite the ‘reasonably calculated’ language as though it defines the scope of discovery, and judges often hear lawyers argue that this sentence sets a broad standard for appropriate discovery.”); see also Losey, *supra* note 141 (“It was a big mistake to think this minor change would do anything to stem the tide of discovery cost inflation. In fact, this minor revision had no impact whatsoever, and most practitioners today are unaware of the slight change to a two-step good-cause process.”).

¹⁴⁵ Advisory Committee Report, *supra* note 142, at 11, 30.

¹⁴⁶ *Id.* at 1.

serious, even grave problems persist in enough cases to generate compelling calls for further attempts to control excessive discovery. The geometric growth in potentially discoverable information generated by electronic storage adds still more imperative concerns.¹⁴⁷

These changes have the potential for being very helpful in containing the scope of electronic discovery into areas that are only marginally relevant. In its Report to the Standing Committee, the Advisory Committee noted that its proposals “seek to promote responsible use of discovery proportional to the needs of the case,” by transferring the proportionality provision currently in Rule 26(b)(2)(C)(iii) to 26(b)(1)’s limit on scope of discovery.¹⁴⁸ It also deletes from that scope discovery into the “subject matter involved in the action.”¹⁴⁹ The Committee asserted that limiting the “reasonably calculated” phrase will further the purpose of the 2000 amendment, especially in light of subsequent misinterpretation that has “obliterate[d] all limits on the scope of discovery.”¹⁵⁰

¶56 These limitations could go a long way towards reducing fishing expeditions on the part of counsel seeking damaging admissions and character evidence from SNSs, not to mention alternative causes of action.¹⁵¹ Privacy considerations, including privacy settings, could be weighed as part of the “burden” of proposed discovery under Rule 26 (b)(1) that could outweigh the negligible benefit of that information.

¶57 In particular, courts could distinguish between relevance to the claims and defenses themselves and relevance to potential impeachment in weighing intrusive discovery against the importance of that discovery to the issues at stake. We already make this distinction in the rules on voluntary disclosures.¹⁵² Most of the “fishing expeditions” sought by litigants in the social media realm are in the hopes of finding contradictory

¹⁴⁷ *Report of the Advisory Committee on Civil Rules, in* COMMITTEE ON RULES OF PRACTICE AND PROCEDURE AGENDA BOOK 226 (2013), available at <http://www.uscourts.gov/uscourts/RulesAndPolicies/rules/Agenda%20Books/Standing/ST2013-01.pdf>.

¹⁴⁸ Advisory Committee Report, *supra* note 142, at 9–10.

¹⁴⁹ *Id.* at 10–11.

¹⁵⁰ *Id.* at 14 (internal quotation marks omitted); see also *Report of the Advisory Committee on Civil Rules, supra* note 147, at 227 (“Too many lawyers, and perhaps judges, understand the rule to mean that there are no limits on discovery, because it is always possible that somehow, somewhere, a bit of relevant information may be uncovered.”).

¹⁵¹ Ralph Losey argues:

The scope of discovery should be constricted in two ways. First, relevance should be limited to the claims and defenses raised. It should not be extended to the general subject matter of the case. It should not allow fishing expeditions into other possible causes of action. The good cause exception should be eliminated. That is a signal that the Bench and Bar will hear.

Secondly, if ESI is not relevant or trustworthy enough to be admissible evidence, it should not be discoverable. Period. ESI directly relevant to claims and defenses is already voluminous. The additional grey areas of ESI that *appears* to someone as *reasonably calculated to lead to discovery of admissible evidence*, is inherently excessive and burdensome. It is a luxury we can no longer afford.

Losey, *supra* note 141.

¹⁵² See FED. R. CIV. P. 26(a)(1)(A)(i) (requiring initial disclosure of individuals likely to have discoverable information “that the disclosing party may use to support its claims or defenses, unless the use would be solely for impeachment”).

impeachment evidence. Such evidence could be considered “disproportional to the needs of the case” if the privacy concerns are not outweighed by the relevance to the issues and limited scope of the information.

¶158 One interesting example of a court restricting potential discovery based on privacy interests is *Coates v. Mystic Blue Cruises Inc.*¹⁵³ There, the District Court for the Northern District of Illinois considered the argument of a plaintiff in a sexual harassment suit that social media discovery requested by the defendant violated the restriction on use of other sexual relations embodied in Federal Rule of Evidence 412. The court ordered a limited production of messages and allowed redaction of personal information.¹⁵⁴ The well-reasoned restrictions on admissible evidence represented in the Federal Rules of Evidence could be translated into restrictions on pretrial discovery as well.¹⁵⁵

D. Privacy Protection Under the Rules

¶159 Apart from a reduction in scope of discovery or other change in the rules, the place for privacy protection under the traditional approach is as follows. First, privacy is not an argument for immunity from discovery. As the Supreme Court has made clear, discovery encompasses all relevant material, whether public or private, confidential or privileged (although privileged material may be withheld if listed in a privilege log¹⁵⁶). Second, discovery requests should not be overbroad—and any blanket request for access to SNS accounts is likely overbroad.¹⁵⁷ Third, the producing party has the burden of seeking protection against production of information that is covered by a proper discovery request but would invade the privacy of the party or of a non-party.¹⁵⁸ That protection can take several forms. The more difficult to obtain would be a motion for a protective order asking that the party be allowed to withhold the material from production altogether.¹⁵⁹ The burden for the party seeking this motion is high: the party must show that her privacy

¹⁵³ *Coates v. Mystic Blue Cruises*, No. 11 C 1986, 2012 WL 3860036 (N.D. Ill. Aug. 9, 2012).

¹⁵⁴ *Id.*; see also *Mackelprang v. Fidelity Nat'l Title Agency of Nev., Inc.*, No. 2:06-cv-00788-JCM-GWF, 2007 WL 119149 (D. Nev. Jan. 9, 2007).

¹⁵⁵ See *Losey*, *supra* note 141 (advocating that discovery be limited not only to relevant evidence but to admissible evidence only).

¹⁵⁶ FED. R. CIV. P. 26(c)(1)(A).

¹⁵⁷ See *Howell v. Buckeye Ranch, Inc.*, No. 2:11-cv-1014, 2012 WL 5265170 (denying requests for user names and passwords for all SNS as overbroad; defendants should request relevant information from the plaintiff, who can then provide it).

¹⁵⁸ FED. R. CIV. P. 26(c)(1). As stated in *Wright & Miller*,

The rule requires that good cause be shown for a protective order. This puts the burden on the party seeking relief to show some plainly adequate reason therefore. The courts have insisted on a particular and specific demonstration of fact, as distinguished from stereotyped and conclusory statements, in order to establish good cause. This recognizes that the existence of good cause for a protective order is a factual matter to be determined from the nature and character of the information sought by deposition or interrogatory weighed in the balance of the factual issues involved in each action.

8A CHARLES ALAN WRIGHT, ARTHUR R. MILLER & RICHARD L. MARCUS, *FEDERAL PRACTICE AND PROCEDURE* § 2035 (3d ed. 1998) (internal quotation marks and citations omitted).

¹⁵⁹ To obtain a protective order, the party seeking protection must make a particularized and specific demonstration of fact under Federal Rule of Civil Procedure 26 (c)(1). *Autotech Techs. L.P. v. Automationdirect.com, Inc.*, 235 F.R.D. 435, 440 (N.D. Ill. 2006); see *Gulf Oil Co. v. Bernard*, 452 U.S. 89, 102 n.16 (1981).

interest is not outweighed by the relevance of the discovery to a specific issue in the case and that the privacy cannot be adequately protected by other means.¹⁶⁰ Lesser remedies include motions for a protective order restricting the divulgence of materials outside the confines of the litigation.¹⁶¹ Also appropriate are requests that the court conduct *in camera* review of the material to assist in identifying private material, which can then be withheld from production or redacted.¹⁶² The *in camera* review should not be used every time social media evidence is disclosed; instead, it should only be utilized in circumstances where specific private information is subject to disclosure.¹⁶³ The court has broad discretion in ordering these protective measures.¹⁶⁴

¶160 The type of information properly subject to restriction from discovery based on privacy interests deserves further attention but at the least should include certain medical information,¹⁶⁵ information about sexual relations,¹⁶⁶ personal information about a minor,¹⁶⁷ personal information about a victim of sexual assault,¹⁶⁸ and other potential embarrassing personal information.¹⁶⁹ The more relevant the discovery to a specific issue in the case, the less likely the discovery will be protected.

¹⁶⁰ See *A. Farber & Partners, Inc. v. Garber*, 234 F.R.D. 186, 191 (C.D. Cal. 2006) (“Here, plaintiff’s need for defendant Garber’s financial documents outweighs defendant Garber’s claim of privacy, especially when the ‘impact’ of the disclosure of the information can be protected by a ‘carefully drafted’ protective order.”) (citations omitted); *Soto v. City of Concord*, 162 F.R.D. 603, 616 (N.D. Cal. 1995) (“Resolution of a privacy objection or request for a protective order requires a balancing of the need for the information sought against the privacy right asserted. A carefully drafted protective order could minimize the impact of this disclosure.”) (internal citations omitted).

¹⁶¹ FED. R. CIV. P. 26(c)(1)(F) & (G); see *Layne Christensen Co. v. Purolite Co.*, 271 F.R.D. 240, 242–43, 247–48 (D. Kan. 2010) (granting a two-tier protective order limiting the disclosure of confidential information produced during discovery and allowing the parties to designate some materials as limited to “Attorneys’ Eyes Only”).

¹⁶² See *Soto*, 162 F.R.D. at 619 (“Due to the highly sensitive nature of [Defendant police officers’ medical records], this Court will conduct an *in camera* review of the medical records requested in Requests 6, 7 and 8.”).

¹⁶³ *Id.*

¹⁶⁴ *Aluminum Co. of Am. v. U.S. Dep’t of Justice, Antitrust Div.*, 444 F. Supp. 1342, 1347 (D.D.C. 1978) (“It is well established that a court has broad discretion under Rule 26(c)(7) in determining both whether a protective order is warranted and the specific restrictions to be imposed.”) (internal citations omitted).

¹⁶⁵ See *Whalen v. Roe*, 429 U.S. 589, 599–600 (1977) (recognizing a limited privacy interest in the confidentiality of medical records).

¹⁶⁶ See *Coates v. Mystic Blue Cruises, Inc.*, No. 11 C 1986, 2012 WL 3860036 (N.D. Ill. Aug. 9, 2012).

¹⁶⁷ See *Breed v. U. S. Dist. Ct. for N. Dist. of Cal.*, 542 F.2d 1114, 1116 (9th Cir. 1976) (minors’ privacy interests in ward files).

¹⁶⁸ See *United States v. Bd. of Cnty. Comm’rs*, No. CIV 08-0501 JB/ACT, 2010 WL 1141362, at *3 (D.N.M. Mar. 8, 2010) (granting motion for a protective order to the extent that it seeks to limit how and with whom the defendant can use any evidence of the victims’ alleged sexual behavior or sexual predisposition).

¹⁶⁹ See *Keyes v. Lenoir Rhyne Coll.*, 552 F.2d 579 (4th Cir. 1977) (upholding trial court’s refusal to require college to produce confidential evaluations of each faculty member because confidentiality is necessary to encourage honest and candid appraisals); *Melendez v. Primavera Meats, Inc.*, 270 F.R.D. 143 (E.D.N.Y. 2010) (noting that courts are reluctant to compel disclosure of income tax returns because of the private nature of sensitive information contained in them and the public interest in encouraging complete and accurate returns); *Flagg v. City of Detroit*, 268 F.R.D. 279 (E.D. Mich. 2010) (finding good cause for a protective order where disclosure of materials placed under seal, including police department’s murder investigation file, depositions of law enforcement officers, and material produced by nonparty police officers, had the potential to interfere with the ongoing murder investigation and to threaten nonparties’

IV. CONCLUSION

¶61 Social media is apparently here to stay, and it will continue to play a large part in pretrial discovery in a broad range of cases. Courts need to put this discovery in context and treat it like other potentially relevant information. Particularly in cases alleging emotional damages and severe physical damages, courts have been too willing to allow blanket access to a person's SNS information given the barest showing that the account may contain relevant information (including information relevant only to impeachment). And parties have too often sought that blanket access both from each other and from the SNSs themselves. Instead, SNS information should be part of regular discovery requests, and given no less—and no more—protection than other private communications.

¶62 A broader issue is containment of discovery in general. The participants at the Duke Conference in 2010 noted the myriad of issues in our civil litigation system, particularly with respect to discovery.¹⁷⁰ The Advisory Committee notes:

discovery runs out of proportion in a worrisome number of cases, particularly those that are complex, involve high stakes, and generate particularly contentious adversary behavior. The number of cases and the burdens imposed present serious problems. These problems have not yet been solved.¹⁷¹

The costs outweigh the benefits and threaten the pursuit of justice in a substantial number of cases. Limitations on discovery are necessary to ensure a more level playing field, the protection of litigants' privacy, and an increased focus on the actual issues, as opposed to marginally relevant information.

privacy interest); *Duling v. Gristede's Operating Corp.*, 266 F.R.D. 66 (S.D.N.Y. 2010) (finding possible harm from disclosure of personal information in employers' personnel files demonstrated a particular need for protection); *Flaherty v. Seroussi*, 209 F.R.D. 300 (N.D.N.Y. 2002) (granting protective order against disclosure of medical, educational, and other inherently private information concerning individual employees of the city, particularly those who were not parties to the action); *Star Scientific, Inc. v. Carter*, 204 F.R.D. 410 (S.D. Ind. 2001) (finding that tobacco company established good cause for entry of a protective order to secure trade secrets).

¹⁷⁰ See SUMMARY OF THE REPORT OF THE JUDICIAL CONFERENCE COMMITTEE ON RULES OF PRACTICE AND PROCEDURE (2012) (describing its project to study issues relating to ESI prompted by the May 2010 Conference on Civil Litigation held at Duke University School of Law and noting that it is considering potential rules amendments aimed at reducing the costs and delay in civil litigation); *Report of the Advisory Committee on Civil Rules*, *supra* note 147, at 19.

¹⁷¹ Advisory Committee Report, *supra* note 142, at 10.

