

---

From the SelectedWorks of Allyson W. Haynes

---

August 9, 2013

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

Allyson Haynes Stuart



SELECTEDWORKS™

Available at: [http://works.bepress.com/allyson\\_haynes/13/](http://works.bepress.com/allyson_haynes/13/)

Finding Privacy in a Sea of Social Media and Other E-Discovery  
Allyson Haynes Stuart\*

Abstract

*This article looks at the case law governing discovery of social media, and finds several problems. First, many courts are improperly requiring a threshold showing that relevant information exists in public portions of the user's social media account before allowing such discovery. Second, they allow overbroad discovery, often requiring a litigant to turn over its username and password to the other party. At the same time, parties are seeking 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 Fed. R. Civ. P. 26(b)(1) to limit the scope of discovery based on proportionality and relevance to existing claims and defenses.*

- I. Introduction
- II. Discovery of Social Network Information: Both Overinclusive and Underinclusive
  - A. Increase in Requests and Use In All Kinds of Cases
  - B. Courts Improperly Ordering Blanket Access to Social Media
    - 1. The Threshold Approach
    - 2. Underinclusive as Well as Overinclusive
    - 3. Wasting Judicial Resources
  - C. Parties Improperly Seeking Blanket Access Directly from Social Media Sites
  - D. Movement Toward a Better Approach
- III. Finding Privacy in a Sea of E-Discovery
  - A. Putting Social Media in Context
    - 1. The Format
    - 2. The Public Nature
  - B. What Is the Implication of Using Privacy Settings?
  - C. Narrowing the Scope of Discovery
  - D. Privacy Protection Consistent With the Rules
- IV. Conclusion

## I. Introduction

Electronic discovery is one of the biggest challenges our courts face today.<sup>1</sup> Its vast scope complicates the system in which relevant information is exchanged, and its expense can be overwhelming.<sup>2</sup> Given the very low number of cases that ever actually go to trial,<sup>3</sup> pretrial discovery (and related motion practice) is the primary determinant of a case's success.<sup>4</sup> 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.<sup>5</sup> With the advent of social media, discovery now often includes information from social media sites, and its potential for misuse is high.

Courts faced with the discoverability of social media unfortunately have treated the issue differently from other discovery, giving litigants both more and less protection from such requests.<sup>6</sup> 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.<sup>7</sup> There is no basis for such a threshold requirement in the federal rules, which instead allow broad

---

\*Associate 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 and Ian Kerr, for their very helpful comments on an earlier draft; and Kelsey Brudwig, Charleston School of Law 2014, for her excellent research assistance.

<sup>1</sup> See Richard L. Marcus, Introduction, at 1, in Shira A. Scheindlin, Daniel J. Capra, *Electronic Discovery and Digital Evidence* (2d Ed. West 2012) (“Since the beginning of the 21<sup>st</sup> 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.”).

<sup>2</sup> See Scheindlin & Capra, at 56 (quoting 2008 Rand Study, *The Legal and Economic Implications of Electronic Discovery*, at 2-3) (discussing increased costs of discovery).

<sup>3</sup> Stephen C. Yeazell, *Civil Procedure* (8<sup>th</sup> Ed. 2012 Wolters Kluwer Law & Bus.), at 284 (“No sort of case goes to trial at a high rate: The national average hovers around 3 percent.”); 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, 306-307 (“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. . . .”).

<sup>4</sup> Miller, 88 N.Y.U.L. Rev. at 307 (“Cases simply do not survive until trial; they are settled or, increasingly, dismissed”).

<sup>5</sup> 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”).

<sup>6</sup> See *infra* Section II.

<sup>7</sup> *Id.*

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.

Second, and more troubling, once courts do find such a threshold showing is met, they allow overbroad discovery into the user's SNS accounts.<sup>8</sup> 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.<sup>9</sup>

Finally, parties are going directly to Facebook and other SNS providers themselves with a subpoena seeking account information and content.<sup>10</sup> Instead, parties should only resort to this tactic if unable to obtain relevant information from the party itself. 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.<sup>11</sup> In addition, there are valid arguments that direct solicitation of the information from SNS providers violates the Stored Communications Act.<sup>12</sup>

Information on social media sites should be treated like other discovery.<sup>13</sup> 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.<sup>14</sup> Only if there is a basis for showing that the responding party is withholding information should there be any issue of further compelled disclosure.

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.<sup>15</sup>

---

<sup>8</sup> See Section II.B.

<sup>9</sup> *Id.*

<sup>10</sup> See Section II.C.

<sup>11</sup> *Id.*

<sup>12</sup> *Id.*

<sup>13</sup> 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.”).

<sup>14</sup> See Fed. R. Civ. P. 26.

<sup>15</sup> See *infra* Section III.C.

## II. Discovery of Social Network Information: Both Overinclusive and Underinclusive

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

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 a billion users worldwide,<sup>16</sup> 167 million in the United States alone,<sup>17</sup> and 240 billion photographs have been uploaded onto the site.<sup>18</sup> Half of all adults in America use social networking sites.<sup>19</sup> Americans now spend more time on social networks than they do on email.<sup>20</sup>

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 SNS's, people tend to share thoughts, feelings, and information freely and often,<sup>21</sup> making such media treasure troves of admissions and impeaching evidence,<sup>22</sup> especially against individuals claiming mental and/or physical damages. Evidence from Facebook has been used in cases to show plaintiffs' exaggeration of their physical injuries,<sup>23</sup> and emotional injuries;<sup>24</sup>

---

<sup>16</sup> Facebook Financial Report, First Quarter 2013, available at <http://investor.fb.com/releasedetail.cfm?ReleaseID=761090>.

<sup>17</sup> 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](http://articles.marketwatch.com/2013-01-15/finance/36346107_1_active-users-facebook-social-media).

<sup>18</sup> Craig Smith, *By The Numbers: 32 Amazing Facebook Stats*, DIGITAL MARKETING RAMBLINGS (May 25, 2013), <http://expandedramblings.com/index.php/by-the-numbers-17-amazing-facebook-stats/>.

<sup>19</sup> PewResearch Center Publications, August 26, 2011.

<sup>20</sup> LA Times, Aug. 3, 2010.

<sup>21</sup> See Ryan A. Ward, *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>.

<sup>22</sup> See *In the Matter of K.W.*, 666 S.E.2d 490 (N.C. Ct. App. 2008) (evidence of minor's MySpace page admissible for impeachment purposes as prior inconsistent statement, but improper exclusion harmless; not admissible as substantive evidence).

<sup>23</sup> See *Trail v. Lesko*, No. GD 10-017249 (Pa. Com. Pl. Jul. 3, 2012); *Loporcaro v. City of New York*, 950 N.Y.S.2d 723, 2012 Slip Op. 50617(U) (N.Y. Sup. Ct. 2012).

<sup>24</sup> See *Robinson v. Jones Lang Lasalle Americas, Inc.*, No. 3:12-cv-00127-PK, 2012 WL 3763545 (D. Ore. Aug. 29, 2012); *Mailhoit v. Home Depot USA Inc.*, 285 F.R.D. 566 (C.D. Cal. 2012).

parents' failure to act in the best interests of their children;<sup>25</sup> spouses' infidelity;<sup>26</sup> and even to show a criminal defendant's alibi<sup>27</sup> or a rape victim's lack of credibility.<sup>28</sup> Practitioners recommend the aggressive use of broad interrogatories and document requests aimed at social media evidence.<sup>29</sup>

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.<sup>30</sup> This Article argues that social media should not be treated differently, but should 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.<sup>31</sup>

---

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

<sup>26</sup> 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/index.html?hpt=C2>. A recent 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 and Tracy T. Segal, *Discovery of Facebook Content in Florida Cases*, 31 No. 2 Trial Advoc. Q. 14 (Spring 2012), citing *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](http://www.usatoday.com/tech/news/2010-06-29-facebook-divorce_N.htm).

<sup>27</sup> Ben Muessig, *Facebook Status Update Keeps Teen Out Prison*, GOTHAMIST (Nov. 11, 2009, 5:11 PM), [http://gothamist.com/2009/11/11/facebook\\_status\\_update\\_keeps\\_teen\\_o.php](http://gothamist.com/2009/11/11/facebook_status_update_keeps_teen_o.php).

<sup>28</sup> Stephanie Francis Ward, *MySpace Discovery, Lawyers are mining social networks for nuggets of evidence*, 93 ABA J 34 (Jan. 2007), available at <http://www.abajournal.com/magazine/article/next/>; but see *State v. Corwin*, 295 S.W.3d 572 (Mo. App. S.D. 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).

<sup>29</sup> See Christopher B. Hopkins & Tracy T. Segal, *Discovery of Facebook Content in Florida Cases*, TRIAL ADVOCATE QUARTERLY, Vol. 31, No. 2, at 14, 15 (2012), available at [http://www.internetlawcommentary.com/articles/2012\\_discovery\\_facebook.pdf](http://www.internetlawcommentary.com/articles/2012_discovery_facebook.pdf) (Sample interrogatory seeks username and password for any social media site used by the plaintiff in the previous five years; authors also "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, J.D., *Pretrial Involving Facebook, MySpace, LinkedIn, Twitter, and Other Social Networking Tools*, 121 Am. Jur. Proof of Facts 3d 1, § 25 (Apr. 2013).

<sup>30</sup> See *infra* Section II.B.

<sup>31</sup> See *infra* Section III.C.

## B. Courts Improperly Ordering Blanket Access to Social Media

### 1. The Threshold Approach

A majority approach to social media discovery has developed.<sup>32</sup> 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, who then has blanket access to the person's SNS content.<sup>33</sup>

#### i. Origins of the Threshold Approach

One of the earliest U.S. examples of this approach is *Romano v. Steelcase*.<sup>34</sup> 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 her injuries, including loss of enjoyment of life. The court noted that the plaintiff's public profile page "shows her smiling happily in a photograph outside the confines of her home despite her claim that she has sustained permanent injuries and is largely confined to her house and bed."<sup>35</sup> 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."<sup>36</sup> The court found plaintiff's privacy concerns to be low – she knew the information may become publicly available based on the policies of the SNS themselves – and in any event were outweighed by the defendant's need for the information.<sup>37</sup> So the court ordered the plaintiff to execute a

---

<sup>32</sup> The forerunners of this approach were primarily New York state trial and appellate courts. See *Tapp v. NY State Urban Dev., Corp.*, 102 A.D. 3d 620 (NY. App. Div 2013) (citing *Romano v. Steelcase, Inc.*, 907 N.Y.S.2d 650 (N.Y. Sup. Ct. 2010)). 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).

<sup>33</sup> Courts from other states like Pennsylvania, and federal courts, have also followed this approach. See *McMillen v. Hummingbird Speedway, Inc.*, No. 113-2010 CD, 2010 WL 4403285 (Pa. Com. Pl. Sept. 9, 2010); *Zimmerman v. Weis Markets, Inc.*, No. CV-09-1535, 2011 WL 2065410 (Pa. Com. Pl. May 19, 2011); *Largent v. Reed*, No. 2009-1823, 2011 WL 5632688 (Pa. Com. Pl. Nov. 8, 2011); *Sourdiffe v. Texas Roadhouse Holdings, LLC*, Civ. Action No. 3:10-CV-0408, 2011 WL 7560647 (N.D.N.Y. Oct. 24, 2011); *Thompson v. Autoliv ASP, Inc.*, No. 2:09-cv-01375-PMP-VCF, 2012 WL 2342928 (D. Nev. June 20, 2012).

<sup>34</sup> 907 N.Y.S.2d 650 (N.Y. Sup. Ct. 2010)

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

<sup>36</sup> *Id.*

<sup>37</sup> *Id.* at 656.

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.<sup>38</sup>

*Romano* relied primarily on case law from Canada, including the 2009 Ontario Superior Court of Justice case *Leduc v. Roman*.<sup>39</sup> *Leduc* sued for injuries sustained in an

---

<sup>38</sup> *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). 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 (McKinney). The rule commentary cites to the New York Supreme Court case of *Tran v. New Rochelle Hosp.*, 99 N.Y.2d 383, 756 N.Y.S.2d 509 (2003) as support for this position. 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 questioned. 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." Commentary, N.Y. C.P.L.R. 3101 (McKinney), citing *Kavanagh v. Ogden Allied Maint. Corp.*, 92 N.Y.2d 952, 683 N.Y.S.2d 156 (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*). 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 supplied).

<sup>39</sup> *Romano* at 654-55. The court also cited *Ledbetter v. Wal-Mart Stores*, Civ. Action 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 SNS's 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. *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 privileges 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* Opposition to



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.”<sup>40</sup> The defendant moved for production of all materials on the plaintiff’s Facebook site and for an updated affidavit from plaintiff listing relevant documents.<sup>41</sup> After the lower court refused to order production, the court of appeals “share[d its] 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.”<sup>42</sup> 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 [list of relevant] documents,” but 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.”<sup>43</sup> The court did not grant a broad request for disclosure of all Facebook information.

*Romano* misread *Leduc* both in its breadth of production and in reasoning that a threshold showing of existence of relevant information in publicly-accessed material justifies 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*,<sup>44</sup> the 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.<sup>45</sup> 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.<sup>46</sup> 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

---

Motion to Compel, *Ledbetter v. Wal-Mart Stores, Inc.*, 2009 WL 3061764 (D.Colo.) (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.).

<sup>40</sup> *Leduc*, par. 3.

<sup>41</sup> *Id.*

<sup>42</sup> *Id.*; see also *Leduc*, par. 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.”).

<sup>43</sup> *Id.*

<sup>44</sup> [2007] O.J. No. 5511 (S.C.J.).

<sup>45</sup> *Id.*

<sup>46</sup> *Id.*

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.”<sup>47</sup>

The plaintiff in *Leduc* had not posted any photographs or other material in the public portion of his Facebook profile.<sup>48</sup> 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.”<sup>49</sup> So neither case ordered blanket access to the party’s SNS material; instead, they found that relevant material should be produced.

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.<sup>50</sup> 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,”<sup>51</sup> or from evidence of relevant information on the public portion of the Facebook profile.<sup>52</sup> 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.

---

<sup>47</sup> *Leduc* at 6 ¶ 25, discussing *Murphy*.

<sup>48</sup> *Id.* at 7 ¶ 31.

<sup>49</sup> *Id.* 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 7, ¶ 33.

<sup>50</sup> *Id.* at 8 ¶ 33 (“Rule 30.06 requires the presentation of some evidence that a party possesses a relevant document before a court can order production.”).

<sup>51</sup> *Leduc*, at 8 ¶ 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.”).

<sup>52</sup> “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.” *Leduc*, at 8 ¶ 34.

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.<sup>53</sup>

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.<sup>54</sup> The approach has been followed by other New York state courts,<sup>55</sup> and endorsed by its court of appeals.<sup>56</sup> Pennsylvania's state courts also follow the threshold approach.<sup>57</sup> And numerous federal district courts have applied this standard as well, including courts in New York, Colorado, Nevada, Tennessee and Michigan.<sup>58</sup>

---

<sup>53</sup> *Romano* at 654-55.

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

<sup>55</sup> *Loporcaro v. City of New York*, 950 N.Y.S.2d 723, 2012 Slip Op. 50617 (U) (N.Y. Sup. Ct. 2012) (based on the fact that the plaintiff has posted at least some information publicly which may contradict his claims, ordering an in camera inspection of all Facebook postings, including deleted material, so the court may assess materiality and relevance); *Winchell v. Lipiccolo*, 954 N.Y.S.2d 421 (N.Y. Sup. Ct. 2012) (in a personal injury accident arising from a car accident, denying a motion to compel authorization of Facebook account because the defendant failed to establish the factual predicate that Facebook information may be relevant).

<sup>56</sup> *Nieves v. 30 Ellwood Realty LLC*, 2013 N.Y. Slip. Op. 23128, 2013 WL 1629249 (N.Y. App. Term Apr. 11, 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); *Tapp*, 102 A.D.3d at 621 (denying request for Facebook authorization where defendants failed to make a showing that the content would be relevant).

<sup>57</sup> *Largent*, 2011 WL 5632688 (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 21 days); *McMillen*, 2010 WL 4403285 (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); *Zimmerman*, 2011 WL 2065410 (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); *see also* *Gallion v. Gallion*, No. FA1141169555, 2011 WL 4953451 (Conn. Supp. 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).

<sup>58</sup> *EEOC v. Original Honeybaked Ham Co. of GA, Inc.*, Civil Action No. 11-cv-02560-MSK-MEH, 2012 WL 5430974 (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

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.*,

Accessing 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.<sup>59</sup>

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.<sup>60</sup> 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.<sup>61</sup> In

---

instance"); *Glazer v. Fireman's Fund Ins. Co.*, No. 11 Civ. 4374(PGG)(FM), 2012 WL 1197167 (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); *Reid v. Ingerman Smith LLP*, No. CV 2012-0307(ILG)(MDG), 2012 WL 6720752 (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); *Potts v. Dollar Tree Stores, Inc.*, No. 3:11-cv-01180, 2013 WL 1176504 (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"); *Tompkins v. Detroit Metropolitan Airport*, 278 F.R.D. 387 (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).

<sup>59</sup> *McMillen*, 2010 WL 4403285, at \*6.

<sup>60</sup> *Bass v. Miss Porter's School*, Civil No. 3:08cv1807 (JBA), 2009 WL 3724968 (D. Conn. Oct. 27, 2009); *Beswick v. North West Medical Center, Inc.*, No. 07-020592 CACE (03), 2011 WL 7005038 (Fla. Cir. Ct. Nov. 3, 2011); *Davenport v. State Farm Mutual Auto. Ins. Co.*, No. 3:11-cv-632-J-JBT, 2012 WL 555759 (M.D. Fla. Feb. 21, 2012); *Glazer*, 2012 WL 1197167; *Thompson v. Autoliv ASP, Inc.*, No. 2:09-cv-01375-PMP-VCF, 2012 WL 2342928 (D. Nev. June 2012).

<sup>61</sup> Plaintiffs were ordered to turn over their SNS passwords and login information in *Largent*, 2011 WL 5632688; *Zimmerman*, 2011 WL 2065410; *Romano v. Steelcase Inc.*, 907 N.Y.S.2d 650, 657 (N.Y. Sup. Ct. 2010); *McMillen*, 2010 WL 4403285; *Beswick*, 2011 WL 7005038; and *Gatto v. United Air Lines, Inc.*, Civil Action No. 10-cv-1090-ES-SCM, 2013 WL 1285285 (D.N.J. Mar. 25, 2013).

a recent case from the District of Colorado, a court granted a motion to compel the plaintiff's entire Facebook history in a case alleging the use of excessive force in an arrest.<sup>62</sup> 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.<sup>63</sup>

## 2. Underinclusive as Well as Overinclusive

These cases have deservedly been criticized for ordering too much disclosure.<sup>64</sup> The blanket access to social media that is allowed to parties able to meet the threshold showing (or not required to meet a threshold) includes irrelevant and potentially very private content.

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.<sup>65</sup> These courts forbid any discovery of social media if that threshold is not met.<sup>66</sup> Instead, in the U.S., parties are entitled to relevant information from litigants

---

<sup>62</sup> Moore v. Miller, Civil Action No. 10-cv-651-JLK (D. Colo. June 6, 2013).

<sup>63</sup> *Id.* at 3.

<sup>64</sup> Mallory Allen & Aaron Orheim, *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, 149-50 (2012) (noting that in *McMillen* and *Romano*, “[n]ot only did the . . . courts find that litigants could discover social media communication, but they both ordered the litigants to turn over the credentials to their accounts, thus allowing the requesting party unrestricted access to the accounts.”).

<sup>65</sup> See Steven S. Gensler, *Special Rules for Social Media Discovery?*, 65 Ark. L. Rev. 7, 19 (2012) (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 (S.D.N.Y. 2003) (ordering defendant to restore information and produce information to plaintiff).

<sup>66</sup> *Arcq v. Fields*, Civil. No. 2008-2430 (Pa Com. Pl. Dec 8, 2011); *Brogan v. Rosenn, Jenkins, & Greenwald, LLP*, No. 08 CV 6048, 2013 WL 1742689 (Pa. Com. Pl. Apr. 22, 2013); *Fawcett v. Altieri*, 960 N.Y.S.2d 592 (N.Y. Sup. Ct. 2013); *Tapp v. NY State Urban Dev., Corp.*, 102 A.D. 3d 620 (NY. App. Div 2013); *Levine v. Culligan of Florida, Inc.*, No. 50-2011-CA-010339-XXXXMB, 2013 WL 1100404 (Fla. Cir. Ct. Jan. 29, 2013); *McCann v. Harleysville Ins. Co. of NY*, 78 A.D. 3d 1524 (N.Y. App. Div. 2010); *Potts v. Dollar Tree Stores, Inc.*, No. 3:11-cv-01180, 2013 WL 1176504 (M.D.Tenn. Mar. 20, 2013); *Tompkins v. Detroit Metropolitan Airport*, 278 F.R.D. 387 (E.D. Mich. 2012).

contained in those sites regardless of the extent to which publicly available information contradicts a plaintiff's claims.

One source of the problem, of course, is that the parties' attorneys themselves often seek all access to SNS account rather than only seeking relevant information. In such a case, the court properly finds that the party is engaging in a fishing expedition.<sup>67</sup> 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: "I think *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."<sup>68</sup>

It is true that many decisions arise out of requests for access to an entire account, and some courts do chastise the party who made the overbroad request, noting that a more tailored one would be appropriate.<sup>69</sup> But other courts who deny blanket access do not do so solely on the basis that the request is overbroad, but also stress that the showing that relevant evidence exists has not been met.<sup>70</sup>

And more importantly, courts have denied access to SNS information because of a failure to meet the threshold showing even when the request is tailored to be relevant. Recently, a Florida district court denied a 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.<sup>71</sup> The plaintiff did not seek all social media evidence from the defendants, but only social media communications "that relate in any way to the incident that is described in the Second Amended Complaint."<sup>72</sup> Certainly, were the defendants to discuss 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 court found no showing of the existence of relevant evidence had been met, denying 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

---

<sup>67</sup> See *Tompkins*, 278 F.R.D. at 389; *McCann*, 78 A.D.2d at 1525.

<sup>68</sup> *Gensler*, n. 41.

<sup>69</sup> See *Howell v. The Buckeye Ranch, Inc.*, Civil Action No. 2:11-cv-1014, 2012 WL 5265170 (S.D. Ohio Oct. 1, 2012).

<sup>70</sup> See *Arcq*, No. 2008-2430, Pa. Com. Pl. 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.").

<sup>71</sup> *Salvato v. Miley*, Case No:5:12-CV-635-Oc-10PRL (D. Fla. June 11, 2013).

<sup>72</sup> *Id.* at 3.

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.<sup>73</sup>

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

### 3. Wasting Judicial Resources

In the effort to provide an element of privacy protection, many courts have ordered *in camera* review of the SNS evidence.<sup>74</sup> While an admirable attempt to protect litigants’ privacy, this solution is untenable as a general approach because it wastes judicial resources and is not justified in the law.<sup>75</sup> In *Patterson v. Turner*,<sup>76</sup> the appellate court correctly found overbroad the lower court’s order that the plaintiff produce all Facebook information after it had conducted an *in camera* review.<sup>77</sup> 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.<sup>78</sup> So instead of counsel producing responsive information, the court itself must sift through the SNS account content and determine what is relevant.<sup>79</sup> There is no reason to trust litigants’ counsel less because of the nature

---

<sup>73</sup> *Id.* at 4.

<sup>74</sup> *Loporcaro v. City of New York*, 950 N.Y.S.2d 723, 2012 Slip Op. 50617(U) (N.Y. Sup. Ct. 2012); *Nieves v. 30 Ellwood Realty LLC*, 2013 N.Y. Slip. Op. 23128, 2013 WL 1629249 (N.Y. App. Term Apr. 11, 2013); *Offenback v. L.M. Bowman, Inc.*, Civil Action No. 1:10-CV-1789, 2011 WL 2491371 (M.D. Pa. June 22, 2011); *Richards v. Hertz*, 953 N.Y.S.2d 654 (N.Y. App. Div. 2012). Another creative solution, but also time-consuming for the judge, is illustrated by *Barnes v. CUS Nashville, LLC*, No. 3:09-cv-00764, 2010 WL 2265668 (M.D. Tenn. June 3, 2013), where the magistrate judge offered to “friend” the third parties whose SNS pictures were relevant.

<sup>75</sup> See Steven S. Gensler, *Special Rules for Social Media Discovery?*, 65 Ark. L. Rev. 7, 25 (2012) (“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.”).

<sup>76</sup> 931 N.Y.S.2d 311, 312 (N.Y. App. Div. 2011).

<sup>77</sup> *Id.* at 316.

<sup>78</sup> *Id.*

<sup>79</sup> See also *Bass v. Miss Porter’s School*, Civil No. 3:08cv1807 (JBA), 2009 WL 3724968 (D. Conn. Oct. 27, 2009); *EEOC v. Original Honeybaked Ham Co. of GA, Inc.*, Civil Action No. 11-cv-02560-MSK-MEH, 2012 WL 5430974 (D. Colo. Nov. 7, 2012); *Kregg v. Maldonado*, 951 N.Y.S.2d 301 (N.Y. App. Div. 2010); *Thompson v. Autoliv ASP, Inc.*, No. 2:09-cv-01375-PMP-VCF, 2012 WL 2342928 (D. Nev. June 20, 2012).

of social media; there is just as much risk of underproduction of other types of discovery left in the hands of counsel.<sup>80</sup>

Some courts are recognizing 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.”<sup>81</sup>

Instead, parties should seek targeted social media discovery as part of regular discovery requests.<sup>82</sup> Just like requests for email and other communications, there will be some relevant and some irrelevant information. Counsel have the task of sorting through it and figuring out what is responsive. If they improperly withhold responsive information, the requesting party has all the normal tools at his disposal to compel production.<sup>83</sup>

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

Exacerbating the issue is the tendency of litigants to subpoena social media information from SNS’s directly.<sup>84</sup> The federal rules of civil procedure have been revised in an effort to reduce the cost and time expended in disputes related to electronic discovery,<sup>85</sup> and to

---

<sup>80</sup> 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*, 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.”).

<sup>81</sup> *Fawcett*, 960 N.Y.S.2d at 597-98; see also *Tompkins*, 278 F.R.D. at 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.’”) (citations omitted).

<sup>82</sup> See *Gensler*, at 25 (“The longstanding general rule is that people review their own records when responding to discovery requests.”).

<sup>83</sup> See *Gensler*, 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.”).

<sup>84</sup> See *Ledbetter v. Wal-Mart Stores, Inc.*, Civil Action No. 06-cv-01958-WYD-MJW, 2009 WL 1067018 (D. Colo. Apr. 21, 2009).

<sup>85</sup> 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 Cooperation Proclamation (“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



decrease the involvement of judges in unnecessary discovery disputes.<sup>86</sup> However, the approach of many litigants to social media discovery has resulted in just the opposite: counsel are often seeking the discovery not from the other party but directly from the SNS itself, guaranteeing motion practice before the court.

Seeking direct access to SNS information from the providers violates the Stored Communications Act,<sup>87</sup> which prohibits remote computing and electronic communication service providers from divulging the contents of a communication while in storage.<sup>88</sup> Some courts have quashed subpoenas on this basis.<sup>89</sup>

In addition, seeking this information directly from the SNS providers allows an end-run around the relevancy requirements of the rules, since the SNS providers will not review the discovery for relevance before complying with a subpoena. In fact, the SNS's themselves are loath to respond to such subpoenas at all without a court order.<sup>90</sup> Thus,

---

ball,' to no practical effect."); *id.* ("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.").

<sup>86</sup> "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 Cooperation Proclamation. The rules require that parties attempt to resolve any discovery dispute before moving for a protective order (26(c)(1)) or moving to compel discovery (37(a)(1)). Fed. R. Civ. P. 26(c)(1); 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.).

<sup>87</sup> See *Ward, Discovering Facebook*, *supra* note 21, at 566.

<sup>88</sup> 18 U.S.C. 2702 et seq.

<sup>89</sup> *Crispin v. Christian Audigier*, 717 F. Supp. 2d 965 (C.D. Cal. 2010); *In re Subpoena Duces Tecum to AOL, LLC*, 550 F. Supp. 2d 606 (E.D. Va. 2008); *O'Grady v. Superior Court*, 44 Cal. Rptr. 3d 72 (Cal. Ct. App. 2006).

<sup>90</sup> 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:

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 "Account 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

the issue ends up in front of the court anyway, even without the request going directly to a party. So again, too many judicial resources are being devoted to a process that should largely operate without court involvement.<sup>91</sup> 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.<sup>92</sup> Otherwise, the information is within the possession, custody or control of the party itself and should be requested from the party.<sup>93</sup>

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*,<sup>94</sup> the magistrate judge denied the defendant's request for authorizations for the release of records from the SNS hosts. 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,"<sup>95</sup> to be "persuasive and reasonable," and therefore directed that plaintiff's counsel make the appropriate relevant production.<sup>96</sup>

#### D. Movement Toward a Better Approach

An increasing number of courts are rejecting the all-or-nothing and threshold approaches and realizing that discovery of social media, like other discovery, must focus on relevance of individual content, not wholesale access.<sup>97</sup>

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.<sup>98</sup> In

---

to collect and produce the account's content. Facebook preserves user content only in response to a valid law enforcement request.

*Information on Civil Subpoenas*, FACEBOOK HELP CENTER (June 4, 2013, 9:26 PM), available at <https://www.facebook.com/help/.473784375984502/>

<sup>91</sup> 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.

<sup>92</sup> *Id.*; see also *Allied Concrete v. Lester*, 736 S.E.2d 699 (Va. Sup. Ct. 2013).

<sup>93</sup> See Fed. R. Civ. P. 34.

<sup>94</sup> CV 11- 06323 (ADS) (AKT) (E.D.N.Y. May 6, 2013).

<sup>95</sup> *Id.* at 4.

<sup>96</sup> *Id.* at 5.

<sup>97</sup> *Trail v. Lesko*, No. GD 10-017249, at 13 (Pa. Com. Pl. Jul. 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 rely on counsel to peruse the client's profile for relevant information in the first instance.").

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

*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.<sup>99</sup>

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.”<sup>100</sup> Similarly, allegations of depression, stress disorders, and like injuries do not automatically render all SNS communications relevant.<sup>101</sup>

The *Simply Storage* court also emphasized that the role of counsel in discovery of social media is no different from other contexts: “Lawyers 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.”<sup>102</sup> So the court ordered the plaintiffs’ counsel to gather relevant evidence from the SNS accounts and provide it to opposing counsel. “As 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.”<sup>103</sup>

---

<sup>99</sup> *Id.* at 434.

<sup>100</sup> *Id.* at 435.

<sup>101</sup> The court also found that the plaintiffs’ position they should produce only communications that directly reference the matters alleged in the complaint is too restrictive. *Id.* See also *Rozell v. Ross-Holst*, No. 05-Civ.2936(JGK)JCF, 2006 WL 163143, at \*7 (S.D.N.Y. Jan. 20, 2006) (“[While] anything 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.”).

<sup>102</sup> FED. R. CIV. P. 37(a)(1).

<sup>103</sup> *Simply Storage Mgmt.*, 270 F.R.D. at 436. See also *Mackleprang v. Fidelity Nat’l Title Agency of NC, Inc.*, No. 2106-cv-00788-JCM-GWF, 2007 WL 119149, \*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

Other courts have followed this more sensible, traditional approach.<sup>104</sup> 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 PaRCP. . . . 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.’<sup>105</sup>

---

relevant to Plaintiff’s alleged emotional distress and her mental condition, which she has placed at issue in this case. If [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.”)

<sup>104</sup> *Held v. Ferrellgas, Inc.*, No. 10-2393-EFM, 2011 WL 3896513 (D. Kan. Aug. 31, 2011); *Mailhoit v. Home Depot USA Inc.*, 285 F.R.D. 566 (C.D. Cal. 2012); *Patterson v. Turner Const. Co.*, 931 N.Y.S.2d 311, 312 (N.Y. App. Div. 2011); *Howell v. The Buckeye Ranch, Inc.*, Civil Action No. 2:11-cv-1014, 2012 WL 5265170 (S.D. Ohio Oct. 1, 2012); *Reid v. Ingerman Smith LLP*, No. CV 2012-0307(ILG)(MDG), 2012 WL 6720752 (E.D.N.Y. Dec. 27, 2012); *Holter v. Wells Fargo*, 281 F.R.D. 340 (D. Minn. 2011); *Sourdif v. Texas Roadhouse Holdings, LLC.*, Civ. Action No. 3:10-CV-0408, 2011 WL 7560647 (N.D.N.Y. Oct. 24, 2011); *Robinson v. Jones Lang Lasalle Americas, Inc.*, No. 3:12-cv-00127-PK, 2012 WL 3763545, \*2 (D. Ore. 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.”).

<sup>105</sup> *Brogan v. Rosenn, Jenkins, & Greenwald, LLP*, No. 08 CV 6048, 2013 WL 1742689 (Pa. Com. Pl. Apr. 22, 2013). *See also Mackleprang*, 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.”).

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.<sup>106</sup>

In a recent decision from the Eastern District of New York, the court specifically recognizes that the approach of other courts has been both overinclusive and underinclusive. In *Giacchetto*,<sup>107</sup> the 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.<sup>108</sup>

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.<sup>109</sup>

### III. Finding Privacy in a Sea of E-Discovery

#### A. Putting Social Media in Context

##### 1. The Format

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. In fact, 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

---

<sup>106</sup> See *Gatto v. United Air Lines*, Civil Action No. 10-cv-1090-ES-SCM, 2013 WL 1285285 (D.N.J. Mar. 25); *Allied Concrete v. Lester*, 736 S.E.2d 699 (Va. Sup. Ct. 2013).

<sup>107</sup> *Giacchetto*, *supra* note 94.

<sup>108</sup> *Id.* at 3 n. 1.

<sup>109</sup> *Id.* at 7.

all of their content.<sup>110</sup> If there is a specific need for relevant SNS metadata in a particular case, that would give a party a basis for seeking additional material.

## 2. The Public Nature

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, the courts treat them like a single treasure chest to which litigants are given the keys or not.<sup>111</sup> They treat 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.<sup>112</sup>

Therefore, the defendant was entitled to access to that content, regardless of its relevance. Similarly, the *Zimmerman*<sup>113</sup> court noted: "By 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."<sup>114</sup>

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."

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

---

<sup>110</sup> See *In re White Tail Oilfield Services*, Civil Action No. 11-0009, 2012 WL 4857777 (E.D. La. Oct. 11).

<sup>111</sup> See *supra* note 61 (listing cases).

<sup>112</sup> *McMillen v. Hummingbird Speedway, Inc.*, No. 113-2010 CD, 2010 WL 4403285 (Pa. Com. Pl. Sept. 9, 2010).

<sup>113</sup> *Zimmerman v. Weis Markets, Inc.*, No. CV-09-1535, 2011 WL 2065410 (Pa. Com. Pl. May 19, 2011).

<sup>114</sup> *Id.* (emphasis added). See also *Mazzarella v. Mount Airy #1, LLC*, No. 1798 Civil 2009 (Pa. Com. Pl. 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.").

a diary<sup>115</sup> – in other words, privacy is not a barrier to production since courts order disclosure of private materials like diaries.<sup>116</sup> 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: “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.”<sup>117</sup> 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.

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.<sup>118</sup> A better approach can be found in *Howell v. Buckeye Ranch*,<sup>119</sup> where the court denied a broad SNS request: “The 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.”<sup>120</sup>

#### B. What Is the Implication of Using Privacy Settings?

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.

---

<sup>115</sup> *Fawcett v. Altieri*, 960 N.Y.S.2d 592, 597 (N.Y. Sup. Ct. 2013). *See also* *Patterson v. Turner Const. Co.*, 931 N.Y.S.2d 311, 312 (N.Y. 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).

<sup>116</sup> 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.

<sup>117</sup> *EEOC v. Original Honeybaked Ham Co. of GA, Inc.*, Civil Action No. 11-cv-02560-MSK-MEH, 2012 WL 5430974, \*1 (D. Colo. Nov. 7, 2012)

<sup>118</sup> The New York Appellate Court has recognized this. In *Patterson v. Turner Const. Co.*, 931 N.Y.S.2d 311, 312 (N.Y. App. Div. 2011), 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.”

<sup>119</sup> Civil Action No. 2:11-cv-1014, 2012 WL 5265170 (S.D. Ohio Oct. 1, 2012).

<sup>120</sup> *Id.* at\*1.

When an SNS user chooses to limit the audience with whom she shares her content, that choice should matter.<sup>121</sup> 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.<sup>122</sup> 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.<sup>123</sup> The most salient distinction is an obvious one: if privacy settings are set to "public," litigants can obtain the information without the necessity of filing any discovery request at all.<sup>124</sup>

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.<sup>125</sup> In *Seattle Times v. Rhinehart*,<sup>126</sup> 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. 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

---

<sup>121</sup> See Allyson W. Haynes, *Virtual Blinds: Finding Online Privacy in Offline Precedents*, 14 Vand. J. Ent. & Tech. Law 603, 647 (2012) (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).

<sup>122</sup> *Id.*

<sup>123</sup> See *Seattle Times v. Rhinehart*, 467 U.S. 20 (1984).

<sup>124</sup> See Facebook Data Use Policy ("Choosing to make something public is exactly what it sounds like. It means that anyone, including people off of Facebook, will be able to see or access it."), at <https://www.facebook.com/about/privacy/#!/about/privacy/your-info-on-fb>.

<sup>125</sup> See FED. R. CIV. P. 26.

<sup>126</sup> 467 U.S. 20 (1984).



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.<sup>127</sup>

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.”<sup>128</sup> 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.”<sup>129</sup>

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*,<sup>130</sup> “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.’”<sup>131</sup>

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),<sup>132</sup> confidentiality orders, and the use of *in camera* inspections.<sup>133</sup> The types of personal information that have been recognized as deserving protection under

---

<sup>127</sup> *Id.* at 36 (emphasis supplied).

<sup>128</sup> *Id.* at n.20, (quoting *Herbert v. Lando*, 441 U.S. 153, 176-77 (1979)).

<sup>129</sup> *Seattle Times*, 467 U.S. at n. 21, (citing *Whalen v. Roe*, 429 U.S. 589 (1977)); *Cox Broad. Corp. v. Cohn*, 420 U.S. 469 (1975).

<sup>130</sup> *Hassan v. United States*, No. C05-1066C, 2006 WL 681038 (W.D. Wash. Mar. 15, 2006).

<sup>131</sup> *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. *Hassan*, 2006 WL 681038, n.5.

<sup>132</sup> See *Bennett v. Kingsbridge Heights Rehabilitation Care Center*, No. 07 Civ. 9456(LAK), 2009 WL 3294301 \*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.’”).

<sup>133</sup> 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).

these measures include medical<sup>134</sup> and psychiatric<sup>135</sup> records, police personnel files,<sup>136</sup> prison files,<sup>137</sup> information presenting a threat to physical security,<sup>138</sup> and information that otherwise invades a person's privacy without a showing of need.<sup>139</sup>

### C. Narrowing the Scope of Discovery

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.<sup>140</sup> 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

---

<sup>134</sup> *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.”).

<sup>135</sup> *Soto v. City of Concord*, 162 F.R.D. 603 (N.D. Cal. 1995) (considering privacy concerns raised by production of psychiatric evaluations, psychological and physical health records of police officers).

<sup>136</sup> *Id.*; *Rogers v. G.J. Giurbino*, 288 F.R.D. 469 (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) (in dispute over discovery of police personnel files in civil rights action, 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).

<sup>137</sup> *Labrew v. City of New York*, No. 07 Civ. 4641 (DAB)(DFE), 2009 WL 3747165 (S.D.N.Y. Nov. 5, 2009) (denying under Fed.R.Civ.P. 26(b)(2)(C)(iii) production of prison log sheet based on privacy rights of prisoners whose names would be disclosed).

<sup>138</sup> *Bennett v. Kingsbridge Heights Rehabilitation Care Center*, 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).

<sup>139</sup> *Stampf v. Long Island R.R. Co.*, No. 07-CV-3349 (SMG), 2009 WL 3628109, \*2 (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.”).

<sup>140</sup> Ralph Losey refers to this phenomenon as “TMI.” See Ralph C. Losey, *Rethinking Relevance: A Call to Modify the Rules of Discovery*, e-Discovery Team blog (Jan. 24, 2011), available at <http://e-discoveryteam.com/2011/01/24/rethinking-relevancy-a-call-to-change-the-rules-to-narrow-the-scope-of-ESI-relevance>.

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.

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.<sup>141</sup> 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.”<sup>142</sup> 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.”<sup>143</sup> Those sentences would be replaced by the following: “Information within this scope of discovery need not be admissible in evidence to be discoverable.”<sup>144</sup>

The changes arise out of the conference held at the Duke Law School in May, 2010.<sup>145</sup> The subcommittee from Duke Conference noted that:

[S]erious, even grave, problems persist in enough cases to generate compelling calls for further attempts to control excessive discovery. The geometric growth in

---

<sup>141</sup> Memorandum to the Committee on Rules of Practice and Procedure (May 8, 2013), 9-11, at [http://www.uscourts.gov/uscourts/RulesandPolicies/rules/Reports/CV05\\_2013.pdf](http://www.uscourts.gov/uscourts/RulesandPolicies/rules/Reports/CV05_2013.pdf). (“Advisory Committee Report”); see Henry Kelston, *Are We on the Cusp of Major Changes to E-Discovery Rules?*, LAW TECH. NEWS (Apr. 17, 2013), available at [http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202596362366&Are\\_We\\_on\\_the\\_Cusp\\_of\\_Major\\_Changes\\_to\\_EDiscovery\\_Rules&slreturn=20130420162952](http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202596362366&Are_We_on_the_Cusp_of_Major_Changes_to_EDiscovery_Rules&slreturn=20130420162952).

<sup>142</sup> Advisory Committee Report at 11, 30.

<sup>143</sup> Advisory Committee Report 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 Advisory Committee Report 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 Ralph C. Losey, *Rethinking Relevance: A Call to Modify the Rules of Discovery* (“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.”).

<sup>144</sup> Advisory Committee Report at 11, 30.

<sup>145</sup> Advisory Committee Report at 1.

potentially discoverable information generated by electronic storage adds still more imperative concerns.<sup>146</sup>

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 the 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.<sup>147</sup> It also deletes from that scope discovery into the “subject matter involved in the action.”<sup>148</sup> The Committee states that “[d]eleting the ‘reasonably calculated’ phrase will further the purpose of the 2000 amendment that revised this sentence out of concern that . . . ‘it might swallow any other limitation on the scope of discovery.’”<sup>149</sup>

These limitations could go a long way towards reducing fishing expeditions on the part of counsel seeking damaging admissions and character evidence from SNS’s, not to mention alternative causes of action.<sup>150</sup> 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.

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

---

<sup>146</sup> Duke Conference Subcommittee Rules Sketches, Meeting Materials of the Advisory Committee on Civil Rules, Washington DC (Nov. 1-2, 2012), 19 (“Duke Rules Sketches”), <http://www.uscourts.gov/uscourts/RulesAndPolicies/rules/Agenda%20Books/Civil/CV2012-10.pdf>.

<sup>147</sup> Advisory Committee Report at 9-10.

<sup>148</sup> *Id.* at 10-11.

<sup>149</sup> Advisory Committee Report at 11. *See also* Duke Rules Sketches, *supra* note 146, at 20 (“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.”).

<sup>150</sup> *See* Losey, *Rethinking Relevance*:

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.

distinction in the rules on voluntary disclosures.<sup>151</sup> Most of the “fishing expeditions” sought by litigants in the social media realm are in the hopes of finding contradictory 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.

One interesting example of a court restricting potential discovery based on privacy interests is *Coates v. Mystic Blue Cruises Inc.*<sup>152</sup> 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.<sup>153</sup> The well-reasoned restrictions on admissible evidence represented in the federal rules could be translated into restrictions on pretrial discovery as well.<sup>154</sup>

#### D. Privacy Protection Under the Rules

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 log<sup>155</sup>). Second, discovery requests should not be overbroad – and any blanket request for access to SNS accounts is likely overbroad.<sup>156</sup> Third, the producing party has the burden of seeking protection against production of information that is covered by a proper discovery request but that would invade the privacy of the party or of a non-party.<sup>157</sup> That protection can

---

<sup>151</sup> 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”) (emphasis supplied).

<sup>152</sup> No. 11 C 1986, 2012 WL 3860036 (N.D. Ill. Aug. 9, 2012).

<sup>153</sup> *Id.*; see also *Mackleprang v. Fidelity Nat’l Title Agency of NC, Inc.*, No. 2106-cv-00788-JCM-GWF, 2007 WL 119149 (D. Nev. Jan. 9, 2007).

<sup>154</sup> See also *Losey, Rethinking Relevancy* (advocating that discovery be limited not only to relevant evidence but to admissible evidence only).

<sup>155</sup> Fed. R. Civ. P. 26(c)(1)(A).

<sup>156</sup> See *Howell*, 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).

<sup>157</sup> 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

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.<sup>158</sup> The burden for the party seeking this motion is high: the party must show that her privacy 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.<sup>159</sup> Lesser remedies include motions for a protective order restricting the divulgence of materials outside the confines of the litigation.<sup>160</sup> 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.<sup>161</sup> The *in camera* review should not be used every time social media evidence is disclosed, but only in circumstances where specific private information is subject to disclosure.<sup>162</sup> The court has broad discretion in ordering these protective measures.<sup>163</sup>

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

---

character of the information sought by deposition or interrogatory weighed in the balance of the factual issues involved in each action.”

8A Fed. Prac. & Proc. Civ. § 2035 (3d ed.) (citations omitted).

<sup>158</sup> To obtain a protective order, the party seeking protection must make a particularized and specific demonstration of fact under Fed. R. Civ. P. 26 (c)(1). *Autotech Technologies Ltd. P’ship v. Automationdirect.com, Inc.*, 235 F.R.D. 435, 440 (N.D. Ill. 2006).

<sup>159</sup> *See 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.”); *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.”).

<sup>160</sup> Fed. R. Civ. P. 26(c)(1)(F) & (G); *see Layne Christensen Co. v. Purolite Co.*, 271 F.R.D. 240, 242-43 (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”).

<sup>161</sup> *See Soto v. City of Concord*, 162 F.R.D. 603 (N.D. Ca. 1995) (“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.”).

<sup>162</sup> *Id.*

<sup>163</sup> *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.”) (citing *C. Wright and A. Miller*, 8 Federal Practice and Procedure, s 2043, at 305 (1970)).

information,<sup>164</sup> information about sexual relations,<sup>165</sup> personal information about a minor,<sup>166</sup> personal information about a victim of sexual assault,<sup>167</sup> and other potential embarrassing personal information.<sup>168</sup> The more relevant the discovery to a specific issue in the case, the less likely the discovery will be protected.

#### IV. Conclusion

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 SNS's themselves. Instead, SNS information should be part of regular discovery

---

<sup>164</sup> See *Whalen v. Roe*, 429 U.S. 589, 599-600 (1977) (recognizing a limited privacy interest in the confidentiality of medical records).

<sup>165</sup> See *Coates*, *supra* note 145.

<sup>166</sup> See *Breed v. United States Dist. Ct. for Northern District*, 542 F.2d 1114, 1116 (9<sup>th</sup> Cir. 1976) (minors' privacy interests in ward files).

<sup>167</sup> See *United States v. Bd. of Cnty. Comm'rs*, CIV 08-0501 JB/ACT, 2010 WL 1141362, \*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).

<sup>168</sup> See *Flagg ex rel. Bond 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' 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); *Star Scientific, Inc. v. Carter*, 204 F.R.D. 410 (S.D. Ind. 2001) (tobacco company established good cause for entry of a protective order to secure trade secrets); *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); *Melendez v. Primavera Meats, Inc.*, 270 F.R.D. 143 (E.D.N.Y. 2010) (noting that courts are reluctant to compel their 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); *Keyes v. Lenoir Rhyne College*, 552 F.2d 579 (4th Cir. 1977), cert. denied, 434 U.S. 904, 98 S. Ct. 300, 54 L. Ed. 2d 190 (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).

requests, and given no less – and no more – protection than other private communications.

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.<sup>169</sup> The Advisory Committee notes:

[D]iscovery 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.<sup>170</sup>

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 relevant issues, as opposed to marginally relevant information.

---

<sup>169</sup> See Summary of the Report of the Judicial Conference Committee on Rules of Practice and Procedure (Sep. 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); Duke Conference: Initial Rules Sketches at 19.

<sup>170</sup> Advisory Committee Report, at 10.