2011

Privacy's Role in the Discovery of Social Networking Site Information

Kelly Ann Bub

Follow this and additional works at: https://scholar.smu.edu/smulr

Recommended Citation
Kelly Ann Bub, Privacy's Role in the Discovery of Social Networking Site Information, 64 SMU L. Rev. 1433 (2011)
https://scholar.smu.edu/smulr/vol64/iss4/11

This Comment is brought to you for free and open access by the Law Journals at SMU Scholar. It has been accepted for inclusion in SMU Law Review by an authorized administrator of SMU Scholar. For more information, please visit http://digitalrepository.smu.edu.
PRIVACY’S ROLE IN THE DISCOVERY OF SOCIAL NETWORKING SITE INFORMATION

Kelly Ann Bub*

I. INTRODUCTION ........................................ 1434
II. BACKGROUND ........................................ 1435
   A. SOCIAL NETWORKING SITES ....................... 1435
   B. PRIVACY EXPECTATIONS IN THE WORLD OF SOCIAL
      NETWORKING ........................................ 1436
   C. SHOULD SNS BE CONSIDERED ELECTRONICALLY
      STORED INFORMATION UNDER THE FRCP? ......... 1436
   D. THE SCOPE OF SNS DISCOVERY: RULE 26 AND THE
      ROLE OF PROTECTIVE ORDERS ........................ 1438
   E. EARLY CASES APPLYING THE FEDERAL RULES TO
      SNS ................................................ 1439
   F. THE CANADIAN STYLE ................................ 1440
III. CURRENT STATE OF THE LAW IN THE UNITED
     STATES ................................................ 1441
     A. SOCIAL NETWORKING LOGINS AND PASSWORDS .... 1442
     B. In Camera Review .................................... 1444
     C. SNS DISCOVERABLE AS LONG AS REQUESTED IN
        NARROWLY TAILORED DISCOVERY REQUESTS ........ 1445
     D. THIRD-PARTY SUBPOENA ............................ 1446
IV. ANALYSIS ............................................. 1448
     A. PUBLIC INFORMATION ................................ 1449
     B. PRIVATE INFORMATION .............................. 1449
     1. Third-Party SNS Provider .......................... 1450
     2. Obtaining Discovery Directly from SNS User ...... 1452
        a. Discoverability: A Question of Privacy or
           Relevance? ........................................ 1453
        b. Best Method for Relevancy Determinations: In
           Camera or Self Review? ........................... 1456
        c. The Role of Protective Orders .................... 1457
     3. Who Should Provide the Content? .................. 1459
V. CONCLUSION ............................................ 1461

* J.D. Candidate 2012, Southern Methodist University Dedman School of Law;
Honors B.S.B.A. 2009, Saint Louis University. The author would like to thank her family
and friends for their support. Special thanks to my husband, Andrew, for his unending
patience, love, and encouragement and to my parents, William and Celeste, for their con-
stant love and support.
I. INTRODUCTION

In response to the recent outburst in social media usage, courts have struggled as how best to treat discovery of information contained within these sites. From pictures to wall posts to status updates, people feel a new comfort in sharing masses of intimate information within the confines of the sites—information which often would not have been shared so readily or spread so easily before the explosion of the social networking medium. Although the creators of the social networking sites (SNS) publicize that there can be no guarantee that information does not become "publicly available," many users continue to hold on to at least a subjective expectation of privacy. Perhaps the expectation of privacy has something to do with the intricate privacy settings available for site users to manipulate. Whatever the case, people's new willingness to post the intimate details of their lives on the Internet provides a large source of information that attorneys zealously try to obtain through the discovery process. In recent months, U.S. courts have issued numerous inconsistent holdings regarding the discovery of SNS information, reflecting the current high levels of confusion in the area. This Comment seeks to set forth a more coherent approach for courts to use in the future so that courts can apply the law in a consistent fashion and so that litigants and their lawyers can better ex ante understand the law. This Comment begins by discussing the nature of SNS as well as examining the historic role of the Federal Rules of Civil Procedure (FRCP) and their application to SNS information in Part II. Part III seeks to examine the current convoluted state of jurisprudence surrounding the discoverability of SNS information. Finally, Part IV determines if and how privacy expectations should play a role in the analysis of whether SNS information should be discoverable. In addition, Part IV recommends a cohesive and uniform method for courts to follow in the future to extinguish the recent, confused jurisprudence surrounding SNS discovery. The method requires courts to draw distinctions between public information and private information, scrutinize whether the information is sought from the third party SNS provider or the actual SNS user directly, and place more emphasis on the role of relevance in discovery.

1. Privacy Policy, FACEBOOK, http://www.facebook.com/policy.php (last visited Aug. 4, 2011) (stating “[a]lthough we allow you to set privacy options that limit access to your information, please be aware that no security measures are perfect or impenetrable”). Mark Zuckerberg has stated in interviews that privacy is "no longer a 'social norm'" and that “[p]eople have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people.” Emma Barnett, Facebook’s Mark Zuckerberg Says Privacy Is No Longer a 'Social Norm,' TELEGRAPH, Jan. 11, 2010, http://www.telegraph.co.uk/technology/facebook/6966628/Facebooks-Mark-Zuckerberg-says-privacy-is-no-longer-a-social-norm.html.
II. BACKGROUND

A. SOCIAL NETWORKING SITES

Social networking sites, also known as social media sites, are websites where registered users have the ability to log in and form connections both personally and professionally with other users. Through "friend-ing" others and joining interest groups, members create linkages to other users based on similar interests and connections. The sites allow people to view connections among people that might otherwise be unclear. Once a user joins a SNS, he can use the site to "search for friends, blog, discuss topics in message forums, explore new music, view film trailers and comedy clips, join groups, plan events, advertise a business, and many more activities."

In recent years, SNS usage has increased exponentially. Facebook and MySpace constitute two of the most popular SNS with more than 700 million users and 80 million users respectively. According to a recent Nielsen Report, as of June 2010, Americans spent nearly one-fourth of their total Internet time on SNS. This is a 43% increase in the amount of time spent on SNS from June 2009, just one year prior. According to Facebook, 50% of its users log in to their account at least once per day, and more than 30 billion pieces of content are shared each month on its site alone. Each user that fills out a relatively complete profile will list almost forty pieces of personal information, including everything from "name; date of birth; educational and employment history; sexual preferences and relationship status;" to "online and offline contact information; political and religious views; tastes in music, books, and movies; and of course, photos." The widespread use of the sites, combined with the large amount of content posted on the sites, creates the perfect hunting ground for discovery, especially since people often post candid, unguarded, and personal information on the sites.

---

2. Steven C. Bennett, Civil Discovery of Social Networking Information, 39 Sw. L. Rev. 413, 414 (2010).
3. Id.
5. Id. at 19.
6. Id. at 17.
9. Id.
12. Id. at 105–06.
B. Privacy Expectations in the World of Social Networking

So why is it that users feel so comfortable posting the private details of their life in such a public forum? One reason, a scholar has pointed out, is that sites like Facebook create an "intimate, confidential, and safe setting" which breeds a natural ground for socialization. Many SNS users rationalize their behavior based on the assumption that since 500 million other people have engaged in the same activities, the activities must be safe and their personal information must be protected. Furthermore, some may have a diminished fear of sharing their personal information because they feel it is unlikely they would get picked out of a crowd of over 500 million active Facebook users for their individual indiscretions, a phenomenon commonly referred to as the "safety in numbers" rationale.

Besides the reasons explained above, people may also feel a false sense of security in the details they post on SNS due to the intricate privacy controls available on the sites. On Facebook, a user can choose whether his profile can be viewed by all 500 million users, by users age 18 and older, or by "friends only." Furthermore, the social media sites contain particularized settings that control exactly who can access specific areas of the user's profile, such as personal information, wall posts, and photos. Because of the availability of detailed privacy controls, users may feel they are effectively blocking any unwanted viewers from accessing their information, and therefore, they maintain at least some expectation of privacy. Whether this expectation is reasonable, however, is another question, especially in light of Facebook's privacy policy that expressly warns users that it cannot guarantee information posted on the site will not become "publicly available."

C. Should SNS Be Considered Electronically Stored Information Under the FRCP?

Since social media does not fit neatly into a traditional category of electronically stored information (ESI) such as e-mails or blogs, some lawyers have pointed out the difficulty in determining just how social media should be treated in the discovery process. In some respects, social media shares many common attributes with e-mail since the sites often allow users to send private messages to one another. Others argue that these

14. Id. at 1160.
15. Id. at 1161.
16. Id. at 1161–62.
17. Browning, supra note 4, at 19.
18. Id.
19. See id.
22. See Bennett, supra note 2, at 415.
23. Id.
sites operate much less like e-mails and much more like blogs or bulletin boards due to the public nature of the sites and because many messages posted are meant for multiple participants to see, "reach[ing] out to a wider array of participants than they might contact through e-mail alone." But as at least one commentator has pointed out, the technical classification of SNS may not matter when it comes to discovery of the information under the FRCP.

As early as 1970, the Advisory Committee for the FRCP recognized the need to revise the discovery rules in such a way that would keep up with ever-changing technological developments. As such, in 1970, Rule 34 was amended to include "data compilations" as an additional type of potentially discoverable information. For some time, many people, including judges, assumed that the 1970 Rules would apply to electronic discovery (e-discovery) as well as physical documents. The drafters of the 2006 amendments, however, disagreed and therefore sought to create new rules that would better reflect the differences between physical discovery and e-discovery.

In 2006, the FRCP were amended to reflect these changes, and Rule 34 was rewritten to allow a party to request any relevant "electronically stored information . . . stored in any medium from which information can be obtained." The Advisory Committee notes from the 2006 amendments further clarified that ESI was meant to be "broad enough to cover all current types of computer-based information, and flexible enough to encompass future changes and developments."

Due to the amendments' broad language as well as the Advisory Committee notes, which clearly conveyed the committee's intentions that the rules be flexible enough to cover and adapt to new and emerging technologies, there has been widespread agreement in the courts that social networking information should be treated as ESI under the FRCP. As one judge recently explained in EEOC v. Simply Storage Management, LLC, discovery of social media simply "requires the application of basic discovery principles in a novel context." Accordingly, any social networking information should qualify as ESI as long as it fits Rule 34's broad definition requiring that the data compilations be stored.

24. Id.
25. Id. at 416.
27. Id.
28. Id.
29. Id. at 1283.
30. FED. R. CIV. P. 34.
31. FED. R. CIV. P. 34 (Advisory Committee's note to the 2006 amendment).
33. EEOC v. Simply Storage Mgmt., LLC, 270 F.R.D. 430, 434 (S.D. Ind. 2010); see also Goodfried & Dawson, supra note 32.
34. Goodfried & Dawson, supra note 32.
While case law in this area is still rapidly developing, most courts have reached the conclusion that relevant information posted on SNS is discoverable.\textsuperscript{35} Interestingly, at least one scholar has fervently disagreed, pointing to the inherent differences between social networking information and traditional forms of ESI as reason that courts should not simply apply the same cookie-cutter rules to SNS, an entirely different form of technology.\textsuperscript{36} Rather, the analysis should be adapted to take into account the nuances of social networking information.\textsuperscript{37} Courts, however, have yet to demonstrate any intention to adopt such an approach.

D. THE SCOPE OF SNS DISCOVERY: RULE 26 AND THE ROLE OF PROTECTIVE ORDERS

Once courts establish that social networking information is a type of ESI, courts must then turn to Rule 26 to evaluate the scope of discoverable information in a given case. According to Rule 26, "[p]arties may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense."\textsuperscript{38} "Relevant information need not be admissible at . . . trial," but rather only needs to "appear[ ] reasonably calculated to lead to the discovery of admissible evidence."\textsuperscript{39}

The scope of discovery was changed significantly by the adoption of the FRCP in 1938.\textsuperscript{40} Prior to the adoption, discovery was limited to information that could also be admissible in trial.\textsuperscript{41} The adoption of the Federal Rules greatly increased the scope of discoverable information by merely requiring that the discoverable information be helpful in preparation for trial.\textsuperscript{42} The purpose behind the widened scope of the new discovery rules was to "ease preparation for trial, to avoid surprise at trial, and to encourage the resolution of cases on their merits."\textsuperscript{43}

With the increase in the scope of discoverable information, a greater amount of confidential and private information became accessible.\textsuperscript{44} The drafters recognized that broad discovery could cause problems and, therefore, designed protections through the advent of protection orders under Rule 30(b), the predecessor of current Rule 26(c).\textsuperscript{45} Under Rule 26(c), the court retains the power to "issue an order to protect a party or person from annoyance, embarrassment, oppression, or undue burden or

\textsuperscript{36} See Payne, supra note 20, at 842.
\textsuperscript{37} See id. at 864.
\textsuperscript{38} FED. R. CIV. P. 26(b).
\textsuperscript{39} Id.
\textsuperscript{41} Id. at 1679.
\textsuperscript{42} Id.
\textsuperscript{43} Id.
\textsuperscript{44} Id.
\textsuperscript{45} Id.; see FED. R. CIV. P. 26(c).
Discovery of SNS Information

expense” by “forbidding the disclosure or discovery,” by limiting the scope of discovery, or by specifying the terms for disclosure of the discovery, among other protective options within the court’s discretion. Even though “privacy” is not specifically mentioned in the rule, a protected privacy interest is implied if the release of the private information would result in embarrassment or oppression. Although legitimate privacy interests may provide the basis for a litigant to obtain a protective order under Rule 26(c), the order may not provide as much protection as the litigant would desire since, even if a protective order is granted, the order rarely blocks discovery of the information and often merely limits the use and distribution of the information gathered.

E. Early Cases Applying the Federal Rules to SNS

In 2007, U.S. courts first began addressing whether information contained within SNS should be discoverable. In one of the earliest and most detailed cases involving the discovery of SNS information, Mackelprang v. Fidelity National Title Agency, the District of Nevada denied the defendant’s motion to compel the plaintiff to consent to the release of her social profile information. Although the court ultimately denied the motion to compel, the ruling should not be confused with the notion that SNS information is never discoverable. Instead, the judge explicitly left open the possibility that some of the information could be discoverable in some instances. The appropriate way to obtain the information, the judge explained, was to serve the plaintiff with a narrowly tailored request for production of relevant e-mail communications. Otherwise, the judge explained, a litigant is merely engaging in a “fishing expedition” when he has no relevant basis for discovering the messages in the account.

The opinion also set forth a noteworthy discussion regarding the procedure surrounding relevancy determinations in the SNS context. Although the court agreed with the defendant that interested parties “cannot be the ‘final arbiter’ of relevance,” the judge pointed out each party’s duty to comply with discovery requests with a good-faith response, mandated by

46. Id.
51. Id.
52. Id.
53. Id.
54. Id. at *2.
the Federal Rules and corresponding ethical obligations. Only when a party can demonstrate that the adversary is wrongfully withholding relevant information can the information-seeking party request relief. The court also rejected the role of in camera review for relevancy determinations, stating that this type of review is ordinarily only used to resolve disputes involving privilege. Therefore, the court denied any basis to conduct an in camera review to determine whether the litigant’s SNS contained private messages that were either relevant or discoverable.

Just months after the Mackelprang opinion, a New Jersey Superior Court also denied a motion to compel the release of information from a SNS. In T.V. v. Union Township, the plaintiff, a minor, was sexually assaulted at school, and the defendant’s counsel sought production of the plaintiff’s MySpace page, arguing that the contents of the site might shed light on the plaintiff’s state of mind and therefore provide information relevant to the plaintiff’s emotional distress claims. The plaintiff’s counsel raised numerous privacy objections, and the judge granted a protective order denying production of the requested SNS content. Although, on its face, the opinion might seem to indicate that courts will bar discovery based on privacy objections, the judge notably left open the possibility for later discovery of the information if particularized relevance could be shown.

F. The Canadian Style

Although it may seem unusual to address the Canadian courts’ treatment of SNS discovery issues, a few key Canadian opinions are worth mentioning since they heavily influenced many opinions in the United States courts. Due to the limited precedent available regarding discovery of SNS information in United States courts, many courts have turned to Canadian precedent in order to analyze these issues. Canadian courts first addressed SNS privacy concerns in Murphy v. Perger. In Murphy, the judge held that any privacy concerns regarding the production of information from a private Facebook profile were minimal and totally outweighed by the defendant’s need for the information, and therefore the court ordered production. Later, in Leduc v. Roman, a Canadian ap-
pellate judge relied on some of Murphy's analysis in a case also involving
discovery of SNS. Disagreeing with the lower court's holding, the ap-
pellate judge ruled that from the existence of the social networking page,
it was "reasonable to infer that [the plaintiff's] ... social networking site
likely contains some content relevant to the issue of how [the plaintiff] ...
has been able to lead his life since the accident." The court agreed that
the rules require at least some evidence "that a party possesses a relevant
document before a court can order production." The court made clear,
however, that it has the power to infer, from the nature of the SNS ser-
vice, "the likely existence of relevant documents on a limited-access
Facebook profile," and held that the lower court erred by denying the
defendant the opportunity to question the plaintiff through an affidavit to
see what relevant information might have been available on the site.

In contrast, a recent decision in another Ontario court appeared to
reach a different conclusion. In Schuster v. Royal & Sun Alliance Insur-
ance Company, the defendant gained knowledge of the plaintiff's limited
access Facebook profile and sought production of its contents. The
court, however, denied production without the defendant demonstrating
that the site contained relevant evidence, thereby rejecting the automatic
presumption of relevance set forth earlier in Leduc.

Although it is still unclear whether courts in Canada will automatically
assume that a limited-access Facebook profile contains relevant content,
it is clear that Canadian courts allow all SNS to be potentially discovera-
able and that the courts have given little weight to the privacy concerns
raised by litigants in barring discovery.

III. CURRENT STATE OF THE LAW IN THE UNITED STATES

In the past few months alone, U.S. courts have demonstrated added
confusion regarding the discoverability of social media information, issu-
ing inconsistent holdings with slightly different analyses and results.
Recently, rather than merely turning to the precedents set forth in early opinions such as Mackelprang and Leduc for guidance, courts have issued numerous different analyses regarding when and what social media information should be discoverable. These holdings range from requiring the litigant to turn over all social networking information including logins and passwords, to enlisting the judge in the case to "friend" the litigant to obtain access to information and perform an in camera review, and to allowing discovery of any information that fulfills narrowly tailored discovery requests. When litigants seek information from the third-party social networking sites directly, rather than from the actual SNS user, courts have employed additional analyses, confusing the field even more. This Comment discusses each of these approaches in turn, and after performing a thorough examination of the law, highlights some of the biggest problems with the current methods and suggests a sustainable approach courts should use in the future.

A. SOCIAL NETWORKING LOGINS AND PASSWORDS

Requiring litigants to turn over total access to their accounts, including user names and passwords, is one of the most aggressive discovery paths a court can mandate when it comes to discovery of SNS information. Recently, however, at least two courts did just that. In McMillen v. Hummingbird, the judge ordered the plaintiff to turn over the account names and passwords for his SNS profiles to the opposing party. The plaintiff contested by arguing that the communications were shared among private friends on a social networking site, and therefore, the communications were confidential and should be protected from disclosure. The judge, however, rejected the existence of any "social networking site privilege" and clarified that new privileges should not be recognized unless four elements could be established: (1) the communication originated in confidence, (2) the confidentiality of the communication is essential to maintain the relationship between the parties, (3) there is agreement in for production of relevant email communications); Romano v. Steelcase, Inc., 907 N.Y.S.2d 650, 657 (Sup. Ct. 2010) (granting "access to Plaintiff's current and historical Facebook and MySpace pages and accounts, including all deleted pages and related information"); McMillen v. Hummingbird Speedway, Inc., No. 113-2010 CD, 2010 Pa. Dist. & Cnty. Dec. LEXIS 270, at *13 (Pa. Ct. Com. Pl. Sept. 9, 2010) (ordering plaintiff to "provide his Facebook and MySpace user names and passwords to counsel").


76. See Barnes, 2010 WL 2265668, at *1.

77. See EEOC, 270 F.R.D. at 435-36.

78. See Crispin, 717 F. Supp. 2d at 990-91.


81. Id. at *3.

82. Id.
the general community that the particular relationship needs to be fostered, and (4) the potential injury sustained due to disclosure outweighs the benefit of disclosing the particular information in litigation. The judge cited Facebook’s privacy policy as evidence that any communications made via a SNS failed to meet the first requirement since users are put on notice that, regardless of subjective intention, communications can be disseminated by friends or even by the SNS itself. So since, at a bare minimum, the SNS providers had access to the information, the confidentiality element of a potential privilege cannot exist, and the law will not protect against the sharing of these communications.

After concluding that no privilege exists, the judge held that SNS information should be discoverable whenever there is an indication that a person’s SNS contains information relevant to the prosecution or defense of a lawsuit. Puzzlingly though, the judge then ordered that the plaintiff grant the opposing party total access to the sites including login names and passwords. As rationale for his decision, the judge cited only to precedent requiring that courts use “all rational means for ascertaining the truth” and the law’s general disfavorment of privileges.

Under a similar fact situation, a New York court also ordered access to all information contained on a social networking profile by granting the information-seeking defendants “access” to the plaintiff’s current and historical Facebook and MySpace pages and accounts, including all deleted pages and related information. The court held that because the public profile page of the Facebook contained a picture of the plaintiff “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,” the profile picture was enough to present “a reasonable likelihood” that the private portions of her site would shed information about her lifestyle to discredit her loss of enjoyment of life claim. The court concluded that to deny discovery of the websites would interfere with New York’s liberal discovery policies and “condone Plaintiff’s attempt to hide relevant information behind self-regulated privacy settings.” Much like McMillen, the court seemingly ignored the fact that much of the information contained within the SNS profile may not have been relevant to the case at hand. Rather than requiring the defendant to narrow the requests to specific items relevant to the case, the court inexplicably granted access to the entire social networking profile, regardless of the type of content inside. In response to the plaintiff’s privacy ob-

83. Id. at *5.
84. Id. at *6–9.
85. Id. at *9–10.
86. Id. at *12.
87. Id. at *13.
88. Id. at *12.
90. Id. at 654.
91. Id. at 655.
92. Id. at 657.
jections, the court flatly rejected the notion that people have any reasonable expectation of privacy concerning the information on their social networking pages, basing its holding on a Second Circuit opinion holding that individuals may not enjoy an expectation of privacy for Internet postings or e-mails. The court also cited Facebook and MySpace's privacy policies as further proof that users should not have any reasonable expectation of privacy since the policies make users aware the information may become publicly available. Consequently, despite the user's control over privacy settings, the court characterized any claims to privacy as "no longer grounded in reasonable expectations but, rather, in some theoretical protocol better known as wishful thinking."

B. In Camera Review

Rather than requiring access to the entire social networking site, some courts have taken a somewhat less intrusive approach by allowing the judge to determine which information is relevant to the issues at hand and therefore producible. The "in camera review" approach differs from the former since it requires the judge to assess the information on the social networking profile to determine if any of the information should be discoverable, and if so, what information on the site must be produced. In a recent federal district court case in Connecticut, Bass v. Miss Porter's School, in response to the plaintiff's objection to production of her SNS content, the court issued an order requiring the plaintiff to produce all documents that were responsive to the defendants' specified discovery requests and also required production of the plaintiff's entire profile of information to the court for in camera review. After performing the in camera review, the judge found that the set of documents produced for review contained many more relevant documents that should have been produced than the plaintiff turned over to the defendant. The court held that the relevancy of the plaintiff's Facebook usage was more "in the eye of the beholder than subject to strict legal demarcations, and production should not be limited to Plaintiff's own determination of what may be 'reasonably calculated to lead to the discovery of admissible evidence.'" Unlike the judges in McMillen and Romano, the judge devoted attention to the relevancy requirement before automatically requiring all information on the site to be produced, but the judge had a broader opinion of what met the relevancy requirement than the produc-

93. Id. at 656.
94. Id. at 656–57.
95. Id. at 657.
98. Id.
99. Id.
100. Id.
Another federal court in Tennessee chose to take a similar approach, with a fairly unique twist. In *Barnes v. CUS Nashville, LLC*, the judge innovatively offered to “friend” the plaintiff in order to see the more private aspects of the litigant’s Facebook profile to perform an *in camera* review of the information contained within the site. After the review, the judge agreed to disseminate the relevant information to the parties and then close the Facebook account he created. The *Barnes* approach placed the relevancy determination in the judge’s hands from the onset, and although it appears to be an efficient way to quickly gain access to questionable content, the method does not come without its own inherent problems. Due to the structure of Facebook, a “friend” will not immediately gain access to all of the user’s SNS content. For example, private messages sent between the user and other friends, besides the judge, would not be visible for the judge to examine. In addition, the judge would not have ready access to deleted content or any information blocked through one of the many privacy settings available to the user.

C. SNS Discoverable As Long As Requested in Narrowly Tailored Discovery Requests

Rather than requiring a judge to perform an *in camera* review of SNS content or requiring the litigant to automatically produce all information from his SNS profile, at least one court has advocated an approach like that set forth earlier in *Mackelprang*, requiring that SNS content be produced, but only to the extent it was relevant to the case and requested within narrowly tailored discovery requests. In *EEOC v. Simply Storage*, the court agreed that information found on social networking profiles should be discoverable, but limited discovery requests for SNS content only to information that could be relevant to the case. The court acknowledged the broad and permissive nature of Rule 26, but at the same time, the court noted that Rule 26 “is not without its limits.” Consequently, the court held that the discovery requests should be permitted for SNS content, but the information-seeking party needed to precisely narrow its requests to reflect the relevant legal issues in the case.

101. *Id.*
103. *Id.*
104. *Id.*
108. *Id.*
109. *Id.* at 433.
before the plaintiff would be required to turn over necessary information.\textsuperscript{110}

**D. Third-Party Subpoena**

The three approaches mentioned above included requiring the release of social networking logins and passwords, imposing an \textit{in camera} review, and mandating the release of relevant information subject to specified discovery requests. The approaches differ significantly from each other, reflecting the confusion in the courts regarding discovery of SNS content. When a third-party subpoena becomes involved, however, the analysis differs even more markedly and presents even more unanswered questions of law. Some lawyers prefer to first subpoena the third-party SNS provider, such as Facebook or MySpace, directly in order to avoid objections from the producing party and ensure they receive all relevant content, including, at times, deleted content.\textsuperscript{111} The court's analysis in cases involving third-party subpoenas differs greatly from its analysis in those cases where the information is requested directly from the litigant due to possible implications of the Stored Communications Act (SCA), which arise when a third party becomes involved.\textsuperscript{112} Basically, the SCA prevents persons or entities providing electronic communication services to the public from "knowingly divul[g]ing to any person or entity the contents of a communication while in electronic storage by that service."\textsuperscript{113} Although there is some disagreement as to whether the SCA should even apply in the social media context due to the outmoded language contained within the more than twenty-year-old act,\textsuperscript{114} at least some courts have interpreted the act to apply in the social media context and, therefore, block discovery from third parties of certain social media information.\textsuperscript{115}

In a recent federal district court case in California, \textit{Crispin v. Christian Audigier}, Judge Morrow issued a detailed opinion discussing why social networks were subject to the restrictions of the SCA.\textsuperscript{116} The judge explained that the SCA applies to both remote computing service (RCS) providers and electronic communication service (ECS) providers and limits the ability of ECS providers and RCS providers to disclose private information.\textsuperscript{117} The first step, then, was for the court to decide whether

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{110} \textit{Id.} at 437.
\item \textsuperscript{114} Alan Klein, John M. Lyons, & Andrew R. Sperl, \textit{Social Networking Sites: Subject to Discovery?}, NAT'L L.J. (Aug. 23, 2010), http://www.law.com/jsp/nlj/PubArticleNLJ.jsp?id=1202470819522&Social_networking_sites_Subject_to_discovery&sfreturn=1&hxlogin=1.
\item \textsuperscript{115} See Barnes v. CUS Nashville, LLC, No. 3:09-0764, 2010 WL 2196591, at *1 (M.D. Tenn. May 27, 2010); \textit{Crispin}, 717 F. Supp. 2d at 990–91.
\item \textsuperscript{116} \textit{Crispin}, 717 F. Supp. 2d at 976–91.
\item \textsuperscript{117} \textit{Id.} at 971–72.
\end{itemize}
\end{footnotesize}
social media sites should be classified as an ECS or RCS provider. 

According to the SCA, an ECS provider is technically defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications,"\textsuperscript{118} and an RCS is defined as "the provision to the public of computer storage or processing services by means of an electronic communications system."\textsuperscript{119} Under the SCA's definition, an ECS provider is prohibited from disclosing "the contents of a communication while in electronic storage by that service."\textsuperscript{120} On the contrary, RCS providers are prohibited from disclosing any communication received by electronic submission that is kept on the service "solely for the purpose of providing storage or computer processing services to [the] subscriber or customer."\textsuperscript{121}

The court was left to examine whether private messages or wall posts were covered by the SCA and engaged in a separate analysis for each type of communication. With regard to private messages, the court eventually concluded that due to the nature of the private messaging function, social media providers should be classified as both an ECS provider and a RCS provider, which meant that these types of communications were subject to the limitations of the SCA.\textsuperscript{122} The court held that the SNS entity was operating as an ECS provider with regards to sent but unopened messages since the messages seem to fall within the ECS definition of "temporary, intermediate storage."\textsuperscript{123} Conversely, once the messages were opened and retained, the court explained that the SNS operators were providing storage services, and therefore, the SNS providers fit under the RCS classification.\textsuperscript{124}

With regard to Facebook wall posts and MySpace comments, the court struggled much more to classify the communications. The court recognized the difficulty in interpreting and applying statutory language, written prior to the creation of the World Wide Web, to today's most modern technologies.\textsuperscript{125} Relying heavily on the legislative history of the SCA, the court held that the SCA does apply to wall postings and comments.\textsuperscript{126} In reaching its conclusion, the court gave weight to Congress's primary intentions behind enacting the SCA: to protect private electronic communications including private electronic bulletin boards.\textsuperscript{127} Therefore, the court concluded that the subpoenas related to obtaining Facebook wall posts and MySpace comments would only be quashed if the party seeking to quash the subpoena could demonstrate that the privacy settings were

\begin{footnotesize}
\begin{enumerate}
\item \textsuperscript{118} Id. at 972 (quoting 18 U.S.C. § 2510(15) (2006)).
\item \textsuperscript{119} Id. at 973 (quoting § 2711(2)).
\item \textsuperscript{120} Id. at 972 (quoting § 2702(a)(1)).
\item \textsuperscript{121} Id. at 973 (quoting § 2702(a)(2)).
\item \textsuperscript{122} Id. at 987.
\item \textsuperscript{123} Id. (quoting § 2510(17)(A)).
\item \textsuperscript{124} Id.
\item \textsuperscript{125} Id. at 988.
\item \textsuperscript{126} Id. at 989.
\item \textsuperscript{127} Id.
\end{enumerate}
\end{footnotesize}
restricted by the user so as to make the postings private, since the SCA does not protect against "electronic communication[s] [that are] readily accessible to the general public." Leaving open the question of how many users the information must be shared with before the information would not be protected by the SCA, the court impliedly indicated that if access was limited to a "few," then this particular information would be considered "private" and therefore protected by the SCA.

Similarly, but with much less explanation, in *Barnes v. CUS Nashville, LLC*, a federal court in the Middle District of Tennessee used the SCA to quash a third-party subpoena in the social media context. The court, with little other explanation, affirmed that the SCA blocks the disclosure of the information sought from Facebook by subpoena.

In stark contrast to both *Crispin* and *Barnes*, in *Ledbetter*, a federal case in the District of Colorado decided about one year prior to *Crispin* and *Barnes*, the court did not quash the subpoenas sent directly to the third-party social networking sites. Although the plaintiff in the case sought a protective order under the marital and physician-patient privileges to protect the information, the court held that these privileges were waived by bringing suit, and the court refused to grant a protective order. The court held that the information was discoverable since it was "reasonably calculated to lead to the discovery of admissible evidence," but the opinion mysteriously contained no discussion of the SCA as a potential block to the subpoenas issued to the social networking site providers.

IV. ANALYSIS

From the discussion of the current state of the law, it is clear that courts are confused as how best to treat information that comes from SNS. From misanalyzing relevancy issues to misunderstanding the role of privacy, courts have taken many analytical missteps along the way. Although some commentators argue that with the advent of SNS comes the need for the application of totally new discovery rules, this Comment argues that ideal results can best be obtained by simply following the traditional FRCP. Given the current state of the law, courts should engage in a more consistent analysis, focusing on key factors including whether the information is accessible to the general public or restricted

128. *Id.* at 991.
129. *Id.* (quoting 18 U.S.C. § 2511(2)(g)(i) (2006)).
130. *Id.* at 988.
131. *Id.* at 990–91; *Barnes v. CUS Nashville, LLC*, No. 3:09-0764, 2010 WL 2196591, at *1 (M.D. Tenn. May 27, 2010).
134. *Id.* at *1.
135. *Id.* at *2.
by privacy settings, the relevancy of the SNS content in a given case, and
finally, the source of who will be providing the information.

A. Public Information

The first step in outlining a workable guide for courts to use in deter-
mining whether SNS information should be discoverable is to determine
whether the information is accessible to the public or restricted by pri-
vacy settings. A profile that contains public information provides the eas-
est analysis for the courts. Because the information is readily available
to the public eye, any party can access this information without going
through the discovery process at all.\footnote{137} This avoids any potential objec-
tions from the producing party.

However, the question of whether information is technically “publicly
accessible” can raise issues of its own. For example, on Facebook, a regis-
tered user may choose to restrict access to the public at large but still
allow access to content on the site to the user’s “friends.”\footnote{138} In other
words, the information is not visible to the general public, but it is still
readily visible content to anyone who is “friends” with the user. Since a
lawyer could easily gain access to some private information by either
“friending” the user or having an unknown third party “friend” the user,
this issue raises important ethical considerations.

Some savvy lawyers have already realized this possibility, and as a re-
result, at least one bar association has issued an ethics opinion addressing
this type of behavior.\footnote{139} The Philadelphia Bar Association issued a re-
cent ethics opinion prohibiting attorneys from gaining access to an adver-
sary’s SNS profile by asking third parties to “friend” the adverse party or
witness in order to gain access to information restricted only to the user’s
“friends.”\footnote{140} The Bar Association held that the action would violate Rule
8.4(c) of the Pennsylvania Rules of Professional Conduct, a rule that bars
“deceptive” actions.\footnote{141} As long as the attorney does not hide his identity,
the ethics opinion recognized that the attorney can attempt to “friend”
the witness since this conduct does not involve “dishonesty, fraud, deceit,
or misrepresentation.”\footnote{142}

B. Private Information

When the information is not publicly accessible, courts should ap-
proach the question of discoverability in an entirely different manner.

\footnote{137} Russell T. Burke, Social Networking Discovery: Get Used to It, DRI, Aug. 10, 2011,
available at http://clients.criticalimpact.com/newsletter/newslettercontentshow1.cfm?con-
tentid=1865&id=316.
\footnote{138} See Privacy: Privacy Settings and Fundamentals, supra note 106.
www.philadelphiabar.org/WebObjects/PBAReadOnly.woa/Contents/WebServer
\footnote{140} Id. at 1.
\footnote{141} Id. at 2–3.
\footnote{142} Id. at 2.
The first factor courts will need to consider is whether the information is sought from the SNS third-party provider or the actual user of the SNS. Because of the potential interaction of the SCA in cases where a third-party provider is involved, the analysis will differ distinctly in these cases.143

1. Third-Party SNS Provider

When a third-party SNS provider is subpoenaed directly for information, the court will need to consider the implications of the SCA.144 As Crispin and Barnes pointed out, it is likely that the SCA might apply in these cases to block information if the courts find the information was meant to be private.145 However, since the Crispin and Barnes opinions were only district court decisions, the decision to apply the SCA to SNS information is not binding on courts of other jurisdictions.146 Nonetheless, it is likely that other courts may turn to these opinions for guidance.147

Once a court makes the decision that the SCA should apply in a given case, the SCA still may not necessarily result in a bar to discovery. Since the SCA only bars discovery of “private” information, courts will then be tasked with deciding whether the information sought is private.148 In the social media context, the question of whether certain content deserves a privacy expectation results in a complex analysis since personal privacy settings are so versatile and will likely change based on the privacy settings of the particular communications at issue. For example, if the communication was sent using the SNS’s private message function, a court will likely protect discovery of the communication from a third party under the SCA, much like the court’s holdings in Crispin and Barnes.149 The toughest privacy analysis occurs when the information sought is shared with a limited number of people, such as the SNS user’s group of “friends.” It is unclear how many people the communication would need to be shared with before a court would fail to recognize a privacy expectation for SCA purposes. For example, if the communication was shared with all of the user’s “friends,” but the user only had three “friends” on Facebook, a court may still consider the user to have at least some expectation of privacy for the information shared and therefore quash the sub-

147. Id.
Discovery of SNS Information

poena on SCA grounds.\(^{150}\) On the other hand, if the same information was shared with a user's "friends," but the user happened to have two thousand friends, it seems that courts will be and should be much less likely to protect the communication based on any privacy grounds.\(^{151}\)

Since this issue has not been thoroughly addressed by the courts,\(^{152}\) it is unclear how the courts may rule in the future. In making future determinations, this Comment recommends that courts perform a balancing test, weighing a variety of factors to determine whether the given communication is private and subject to the protections of the SCA. Factors that courts may want to consider in their analysis include the number of people or "friends" that had access to the communication, the substance of the content (how embarrassing the content might be if released), the type of people that had access to the communication, and the inherent public nature of SNS.

The last factor, however, the public nature of SNS, would seem to be enough for at least some courts to render the SCA toothless in all cases. Although the court in Crispin asserted that at least some communications made on SNS could qualify as private communications, some courts have issued analyses implying that no matter the privacy setting, no information ever posted on a SNS should deserve an expectation of privacy.\(^{153}\) As reasoned by some courts, such as Romano, since most popular SNS do not guarantee privacy, people cannot have any reasonable expectation of privacy.\(^{154}\) In fact, the Facebook privacy policy specifically warns users that despite privacy options, "no security measures are perfect or impenetrable" and that any information shared through the site risks becoming "publicly available."\(^{155}\) It seems unlikely that courts following Romano's line of reasoning would ever find a SNS communication private and protected from discovery by the SCA.\(^{156}\)

As such, there is an enormous amount of gray area in this area of the law. Fortunately for litigants seeking discovery, much of this uncertainty can be easily avoided with proper planning. First of all, customer consent

150. See Crispin, 717 F. Supp. 2d at 991 (an expectation of privacy was an implied possibility since the court remanded the decision of whether certain wall posts were discoverable based on inadequate facts regarding the privacy settings of those posts).

151. See id.

152. Id. ("Given that the only information in the record implied restricted access, the court concludes that Judge McDermott's order regarding this aspect of the Facebook and MySpace subpoenas was contrary to law. Because it appears, however, that a review of plaintiff's privacy settings would definitively settle the question, the court does not reverse Judge McDermott's order, but vacates it and remands so that Judge McDermott can direct the parties to develop a fuller evidentiary record regarding plaintiff's privacy settings.").


154. See Romano, 907 N.Y.S.2d at 656.

155. Privacy Policy, supra note 1.

156. See Romano, 907 N.Y.S.2d at 657 (explaining "when Plaintiff created her Facebook and MySpace accounts, she consented to the fact that her personal information would be shared with others, notwithstanding her privacy settings. Indeed, that is the very nature and purpose of these social networking sites else they would cease to exist.").
constitutes one major exception to the SCA. The party seeking information should try to obtain consent from the SNS user. If consent is obtained, the SCA would no longer potentially void a subpoena to a third party, and the third-party provider would be required to comply with the subpoena request.

Obviously, in many cases, the user may not want to readily give the consent necessary to allow the opposing party to acquire his SNS information. If the user fails to consent, the information seeker can turn to the court and move for a motion to compel. As long as the information-seeking litigant can demonstrate that the third-party provider maintains information relevant to the case, the court will likely grant the motion and compel the reluctant litigant to consent. In Flagg v. City of Detroit, the court held that the producing party must give the requisite consent required under the SCA so that the information-seeking party could gain access to the information without interference by the SCA. Even when the information is sought from a non-party to the suit, the non-party may still be required to give consent to third parties when issued a subpoena under Rule 45. In Thomas v. Deloitte Consulting, the court held that subpoenas, under Rule 45, include any documents that the non-party can obtain, and therefore, the court required the non-party in the case to grant access to their bank to release records. Therefore, consent, in many cases, can effectively eliminate the possible hurdles presented by the SCA, which may render any detailed analysis regarding the convoluted state of the law surrounding the SCA and its interactions with social media simply an unnecessary headache.

2. Obtaining Discovery Directly from SNS User

If the information is not available to the general public, however, and the information-seeking litigant does not try to subpoena the third-party SNS, the litigant can also try to obtain the information from the SNS user directly. Just like a discovery request in any other context, the procedure for obtaining the SNS from a user directly includes sending a request for

159. Browning, supra note 4, at 126.
160. Bennett, supra note 2, at 422–23 (“[C]ourts have suggested that, at very least, a litigant in a dispute may be required to provide consent for access to social networking sites that contain information relevant to a dispute before the court. That is, if the litigant has the ability to obtain ‘control’ over such information by providing consent to the ISP, then the litigant must provide such consent as part of its discovery obligations.”).
164. See Browning, supra note 4, at 125–26.
production of all relevant documents to the opposing litigant. By sending a discovery request directly to the profile user, the information-seeking litigant will avoid the potential hurdles presented by the SCA, and therefore, this option may be the most strategic one for litigants. In recent years, however, courts have demonstrated difficulty in deciding how to proceed when information is requested directly, namely due to confusion about the role of relevance and privacy in discovery of SNS.

a. Discoverability: A Question of Privacy or Relevance?

One area within which courts have become increasingly confused involves the difference between privacy expectations and relevance, and the role that each factor should play in determining whether particular SNS content should be discoverable. On the whole, many courts have concluded that due to the inherently public nature of SNS, as well as the sites' stated privacy policies, there should be no expectation of privacy, and therefore, discovery should be allowed to proceed. Although many courts end up reaching the correct holding, at least some courts have portrayed fault in their reasoning. The question of discoverability should rest mostly upon relevancy, not privacy. As the court in EEOC v. Simply Storage so poignantly pointed out:


166. See, e.g., Bass v. Miss Porter's Sch., No. 3:08-CV-1807, 2009 WL 3724968, at *1 (D. Conn. Oct. 27, 2009) (noting that plaintiff obtained information from SNS by first issuing subpoena to the SNS directly and then passed on the relevant information to the defendant).


168. See, e.g., EEOC, 270 F.R.D. at 432 (“The EEOC objects to production of all SNS content . . . because they improperly infringe on claimants' privacy.”).


170. Bennett, supra note 2, at 420 (“The Federal Rules, and equivalent state rules, do not recognize any 'privacy' exception to the requirements of discovery (much less a 'social networking privacy' exception.)."; see also EEOC, 270 F.R.D. at 434 ("Although privacy concerns may be germane to the question of whether requested discovery is burdensome or oppressive and whether it has been sought for a proper purpose in the litigation, a person's expectation and intent that her communications be maintained as private is not a legitimate basis for shielding those communications from discovery.").
Although privacy concerns may be germane to the question of whether requested discovery is burdensome or oppressive and whether it has been sought for a proper purpose in litigation, a person's expectation and intent that her communication be maintained as private is not a legitimate basis for shielding those communications from discovery.\textsuperscript{171}

At least some courts have seemed to confuse these two issues.\textsuperscript{172}

Often, at least some information in a SNS will be relevant to the case at issue due to the broad and unrestrictive standards of Rule 26.\textsuperscript{173} The scope of discovery under Rule 26 includes "any non-privileged matter that is relevant to any party's claim or defense."\textsuperscript{174} As long as discovery requests are narrowly tailored so as to only include "relevant" information of non-privileged matter, discovery should be permitted.

Privacy concerns, on the other hand, should play little role in comparison to relevancy when determining whether the SNS content in contention should be discoverable. As even the Supreme Court recognized,

The Rules do not differentiate between information that is private or intimate and that to which no privacy interests attach. Under the Rules, the only express limitations are that the information sought is not privileged, and is relevant to the subject matter of the pending action. Thus, the Rules often allow extensive intrusion into the affairs of both litigants and third parties.\textsuperscript{175}

Mere privacy concerns, without more, do not create privilege,\textsuperscript{176} and therefore private information has, for decades, been discoverable.\textsuperscript{177} In \textit{Leon v. IDX Systems}, for example, the court held that although certain information may have been private, the information was still subject to discovery and the private nature of the information was no defense to destroying the information that should have otherwise been produced.\textsuperscript{178} Consequently, the litigant suffered spoliation charges after knowingly de-
Since the determination of whether SNS content should be discoverable depends first and foremost on relevancy of the content to a specific dispute and not privacy concerns, at least some courts have misconstrued the roles that relevancy and privacy should play. In cases such as Romano and McMillen, the courts held that since there was no reasonable expectation of privacy with respect to the content posted on SNS, all content available on the sites should be turned over for production. That method, however, disregards the scope of discovery set forth in the FRCP. According to Rule 26, the scope of discovery is limited to relevant information, not any information, so long as the court finds there was no reasonable expectation of privacy.

By requiring that total access to a person's account be turned over to the opposing party, the court demonstrated profound neglect of the very sensitive nature of much of the content stored on a user's SNS profile as well as abandonment of the routine discovery procedures that have been followed by attorneys for years. A typical discovery procedure requires the information-seeking litigant to issue a production request so that the producing party can gather the evidence, cull it for relevance and privilege, and then produce the relevant non-privileged materials. As one scholar has already realized, "[i]t would be a highly intrusive system if the normal procedure was, instead of a party producing its own documents, the other party's attorneys entering your house or business, looking through all your papers and effects, and taking away the material that in their judgment was relevant and non-privileged." Because of the broad array of information stored on a SNS profile, to allow the opposing party free access to SNS content would almost always result in the release of at least some non-relevant and potentially very private information.

Some courts, on other hand, have correctly recognized the importance of requiring production to be limited to relevant information. These courts require litigants to issue narrowly tailored discovery requests to obtain access to the relevant portions of the SNS. In Mackelprang, for example, the judge explicitly recognized the problems inherent in forcing the production of all SNS content by noting that "[o]rdering [p]laintiff to

179. Id.
183. Id.
185. Id.
187. See id.
execute the consent and authorization form for release of all of the pri-
vate . . . messages . . . would allow [defendants] to cast too wide a net for
any information that might be relevant and discoverable. It would, of
course, permit Defendants to also obtain irrelevant information.”

Therefore, the court correctly recommended that the information-seeking
litigant rewrite any discovery request to seek only relevant
information.

Sometimes, however, it will be difficult for an attorney to prove there
is relevant content contained within a site if the entire site is made private.
To solve this problem, courts should follow the approach set forth in Leduc,
allowing interrogatories or affidavits about the SNS content. As
the court seemed to correctly recognize, the party otherwise has the abil-
ity to hide behind “self-set privacy controls,” so an affidavit will allow
attorneys to determine whether there might be relevant information hid-

den behind the possible privacy settings barring public access.

From there, information-seeking litigants can use the knowledge gained to issue
particularized requests for certain relevant information from the sites, but
ultimately, the producing party should be the one to cull for relevancy
and turn over relevant information to the information seeker.

b. Best Method for Relevancy Determinations: In Camera or Self
Review?

Besides exhibiting confusion between the role of privacy and relevancy
in SNS discovery, courts have also demonstrated disagreement on the
most appropriate method for making relevancy determinations. For
instance, some courts have required an in camera review of all SNS con-
tent to determine what SNS information is relevant and therefore poten-
tially discoverable while others simply leave the relevancy determination
to the producing party. Using in camera review to make relevancy de-
terminations should not be advocated for several reasons. First of all, in
camera review is extremely costly and time-consuming, creating addi-
tional strain on already limited judicial resources. Although the informa-
tion-seeking party may have legitimate concerns that the producing

---

188. See id. at *7.
189. See id. at *8.
190. Leduc, 2009 CarswellOnt 843, para. 35 (Can. Ont. Sup. Ct. J.) (WL); see also
North, supra note 26, at 1300–01.
191. See Leduc, 2009 CarswellOnt 843 at para. 35.
192. See, e.g., Barnes v. CUS Nashville, LLC, No. 3:09-CV-00764, 2010 WL 2265668, at
*1 (M.D. Tenn. June 3, 2010) (noting that the judge would “friend” the information pro-
ducing party on Facebook to perform in camera review of relevant information); Mackel-
prang v. Fidelity Nat'l Title Agency of Nev., Inc., No. 2:06-cv-00788-JCH-GWF, 2007 WL
119149, at *8–9 (D. Nev. Jan. 9, 2007) (rejecting in camera review as an appropriate
method to determine relevancy); Bass v. Miss Porter's Sch., No. 3:08-CV-1807, 2009 WL
3724968, at *1 (D. Conn. Oct. 27, 2009) (performing an in camera review to determine
relevancy).
194. John Calvin Conway, Self-Evaluative Privilege and Corporate Compliance Audits,
party may have a biased sense of relevance, "counsel for the producing party is the judge of relevance in the first interest." Indeed, in Bass, after the performance of an in camera review, the judge admittedly found a much broader set of documents that he deemed relevant than the producing party had originally produced. However, the producing party must be trusted to give good-faith responses to any demands of production since the complying attorney is bound by the Federal Rules as well as professional and ethical obligations. As Mackelprang pointed out, "in camera review is ordinarily used when necessary to resolve disputes regarding privilege and is rarely used to determine relevance." As more and more information merges onto SNS platforms, SNS discovery will continue to increase. It will not be a sustainable practice for courts to continue to require judges to review entire SNS for relevance in every case, and therefore, these reviews must be reserved for cases where information-seeking parties can demonstrate beyond a mere suspicion that the producing party might be withholding relevant information.

c. The Role of Protective Orders

Since Rule 26 permits such liberal discovery, opposing parties often have the ability to gain access to private and confidential information. Protective orders are granted to limit the production of private and confidential materials during discovery. While Rule 26(c) does not explicitly mention privacy as an interest deserving a protective order, the Rule does protect against the disclosure of information that would cause "annoyance, embarrassment, oppression, or undue burden or expense," from which courts have implied a protected privacy interest. Many courts have refused to recognize any expectation of privacy in the SNS context, and as a result, it seems less likely that courts will be enthusiastic about granting protective orders in the SNS context.

Courts have explained their hesitation to recognize any legitimate privacy interests using various rationales. First, some courts have argued that there should not be a privacy expectation for any of the content posted on a SNS partly because the main purpose behind SNS is to share information with others. Even after conceding that "it is conceivable that a person could use [SNS] as forums to divulge and seek advice on

---

198. Id. (emphasis added).
199. What Americans Do Online, supra note 8.
201. Id.
203. Kim, supra note 47, at 865.
personal and private matters,” one court concluded that “it would be un-realistic to expect that such disclosures would be considered confidential.”

Second, courts also argue that SNS users cannot have a reasonable expectation of privacy due to the SNS’s terms and privacy policies, which put users on notice that communications can be disseminated by friends or even the SNS itself. The court argues that these “policies should dispel any notion that information one chooses to share, even if only with one friend, will not be disclosed with anybody else.”

Third, as cited by the Romano court, there is at least some precedent which has held that e-mail and letter writers lose any expectation of privacy upon delivery of the message. The court relied on the precedent to argue that in the SNS context, once information is posted for someone to see, any expectation of privacy is lost.

A distinguishing factor in the aforementioned cases, however, was that the courts were often refuting privacy expectations in response to arguments that the information’s private nature rendered it completely outside the scope of discovery. In deciding whether to grant a protective order, courts should be more willing to take privacy interests into account, especially when the protective order will be used merely to limit the use and dissemination of the information. Otherwise, the result leaves litigants highly vulnerable to the very problems protective orders were designed to protect against—annoyance, embarrassment, and oppression.

By failing to recognize any privacy interests at all, courts are insensitive to the realities of SNS. SNS have versatile uses and intricate privacy settings. It seems likely that reasonable people may share very intimate details of their life through the private messaging function or through some other function that limits their communication to only a few people. Consequently, such a blanket rejection of all privacy interests would be incorrect when deciding whether to issue a protective order. Instead, courts should engage in a case by case balancing test to determine whether a certain piece of SNS information deserves protection.

Information culled from SNS discovery potentially deserves the protections from a protective order for several reasons. First, SNS bring with them a “perceived sense of privacy.” The act of “participat[ing] in social networking encourages the revelation of intimate details about the participant’s life” such that “[d]espite the warnings and potential privacy dangers, users reveal intimate personal information through social networks to fulfill their innate human social needs.” Second, SNS allow
for complex privacy setting options that act as a set of controls to help limit access to information. Since users have the ability to limit access to specific types of information to specific users, courts should analyze privacy expectations on a case by case basis, taking into account the privacy settings of the information at issue to make a more precise determination about whether that user could have a reasonable expectation of privacy. Although the terms and use policies may try to warn users that there is potential for their information to be made publically available, even reasonable people may end up being misled since the site’s privacy settings make statements such as “conversations within Facebook [messages] are absolutely private.”

Instead of wholeheartedly rejecting the expectation of any privacy interests in the SNS context, judges should take advantage of their wide judicial discretion available to issue protective orders in cases that are most appropriate. When determining whether a protective order should be issued, courts should weigh the hardship that would be caused to the litigant trying to restrict access against the hardship caused by the restrictions on the party seeking the information. In making this determination, courts should consider such factors as how many people the information is shared with, the nature of the information (how embarrassing or private the information seems), the type of people the information was shared with, and the public nature of social media itself. Since protective orders often simply limit the way certain information may be used or disclosed in the trial, rather than completely barring discovery, judges should be more open to issuing protective orders, especially since “[t]he federal rules recognize the value in protecting intimate information under Rule 26(c)."

3. Who Should Provide the Content?

In addition to relevancy and protective order issues, a final consideration involves deciding who should provide the SNS content. There are two basic methods to obtain SNS information. Either the producing party can obtain the information by downloading his information from the SNS or the producing party can request the information directly from the third-party site. In most cases, the producing party should be required to produce relevant information directly since this is the fastest, easiest, and least expensive method to obtain the information.

However, in some instances, it may be best for the court to require the producing party to authorize the SNS third-party provider to turn over the information. For example, if the opposing party fears that not all relevant information is being released to them or if the opposing party

213. Id. at 869–70.
214. Id. at 870.
216. Payne, supra note 20, at 855.
217. See id. at 870.
218. Id. at 869.
wants access to information that is no longer readily available on the user’s SNS profile (i.e., deleted content). Although SNS have not specified with exactitude how long they will maintain deleted information, by obtaining the information through a request to the third party, there is at least a chance that some deleted content might be available, although probably difficult to obtain.\(^{219}\)

If for some reason, it is necessary to gain access to the information through the third-party SNS provider, the user will need to issue a subpoena to the SNS provider. The subpoena process is not easy and is likely to be met with some resistance, and thus, it is usually best to seek the information directly if possible.\(^{220}\) In fact, Facebook even states that they “urge[ ] parties to civil litigation to resolve their discovery issues without involving Facebook.”\(^{221}\) According to Facebook’s subpoena policies, “if you are or represent a party to a civil case and believe basic subscriber information is indispensable and is not within the possession of a party, you must personally serve a valid California or Federal subpoena on Facebook. Out-of-state civil subpoenas must be domesticated in California.”\(^{222}\) Furthermore, Facebook charges a processing fee of $500 per account as well as an additional $100 for each notarized declaration from the records custodian.\(^{223}\) In addition, since Facebook only guarantees that they will release “basic subscriber information,” it is unclear how much information they will actually turn over.\(^{224}\)

Luckily for litigants, at least one SNS, Facebook, has created a way to make the process easier for all involved.\(^{225}\) Now, with just a click of a button, Facebook users can download their entire account, which will document anything they have ever posted on their account.\(^{226}\) Other SNS may soon realize the value in this method and potentially come up with similar functions.

\(^{219}\) See Privacy Policy, supra note 1 (“Removed and deleted information may persist in backup copies for up to 90 days, but will not be available to others.”); see also Help Center, Safety for Law Enforcers, FACEBOOK, http://www.facebook.com/help/?safety=law (last visited Feb. 2, 2010) (“If a Facebook user deletes content from their account, Facebook will not be able to provide that content. Effectively, Facebook and the applicable Facebook user have access to the same content. To the extent a user claims it does not have access to content (e.g., the user terminated their account), Facebook will restore access to allow that user to collect and produce the information to the extent possible.”).

\(^{220}\) See id.

\(^{221}\) Id.


\(^{223}\) Id.

\(^{224}\) Id.


\(^{226}\) Id.
V. CONCLUSION

In recent years and months, a slew of different decisions have arisen from the lower courts in the United States involving the discoverability of social media information. From these holdings, it is clear that future courts should adopt a more uniform and sustainable approach to discovery of social media information by borrowing the best practices from some of these decisions. First, if possible, information should always be sought first from the litigant, not the third-party SNS, to avoid possible run-ins with the SCA. However, even if the information is sought from the third party directly, the SCA concerns can usually be avoided by requiring the SNS user to provide consent to the release of information. Next, based on the discovery rules set forth in the FRCP, courts should place more emphasis on the question of relevancy in determining whether information is discoverable and less emphasis on privacy expectations in their initial determinations. In deciding which information is relevant, courts should leave the determination to the information-producing litigant, not resort to in camera review due to the large burden it places on judges. Finally, in general, courts should be more sensitive to the private subject matter shared on SNS and give these privacy concerns more weight when using their discretion to decide whether protective orders are appropriate.