Social Networking in the Workplace: Are Private Employers Prepared to Comply with Discovery Requests for Posts and Tweets

Lisa Thomas

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

Recommended Citation
SOCIAL NETWORKING IN THE WORKPLACE: ARE PRIVATE EMPLOYERS PREPARED TO COMPLY WITH DISCOVERY REQUESTS FOR POSTS AND TWEETS?

Lisa Thomas*

With over five hundred million active users, Facebook is the most visited social networking site on the Internet. By the end of 2008, social networking had become more popular than e-mail. Two-thirds of the world's Internet users access social networking sites, with individuals spending, on average, ten percent of all of the time they spend on the Internet on such sites. With the strong Internet presence of social networking sites, it is no surprise that companies have begun to utilize the sites to interact with their customer base and clientele. As companies begin to use social networking for business purposes, the likelihood that such sites may contain information relevant to a lawsuit becomes quite high. For companies, problems associated with the discovery of electronically stored information may be directly applicable to the discovery of information from social networking sites. As such, the legal ramifications of the use of social networking sites as a marketing tool, and as a means of internal and external communication, must be addressed for companies to be prepared in the event of litigation.

This Comment addresses the problems related to the discovery of electronically stored information and how such problems relate to the discov-

* B.S. Bioengineering Rice University, 2005. J.D. Southern Methodist University Dedman School of Law, 2011. Many thanks to my family and friends for their love and encouragement throughout this endeavor. A special thanks to my husband, Tojo, for his support during the writing and editing process. This work is dedicated to Jeremiah.

ery of information from social networking sites. Part I addresses the history of electronic discovery, with emphasis on case law that aided the Advisory Committee in amending the Federal Rules of Civil Procedure related to electronically stored information. Part II discusses the rise of Facebook and Twitter, how such sites work, and how information can be obtained from the sites in the event of litigation. Part III discusses current case law relating to electronically stored information and analyzes how courts will likely treat discovery of information from social networking sites. Part IV addresses the steps that employers should take to ensure that they are prepared for discovery of information from social networking sites in the event of litigation. Policy guidelines regarding the use of social networking sites in the workplace are also considered.

I. ELECTRONIC DISCOVERY: A HISTORICAL PERSPECTIVE

Electronic discovery, more recently referred to as e-discovery, is now commonplace in litigation. The prevalence of computer usage in the workplace has dramatically altered the universe of discoverable information. As companies now maintain records in electronic form to save space and money, evidence relevant to litigation matters will generally be in electronic form. An early case defined electronic records to encompass:

- voice mail messages and files, back-up voice mail files, e-mail messages and files, backup e-mail files, deleted e-mails, data files, program files, backup and archival tapes, temporary files, system history files, web site information stored in textual, graphical or audio format, web site log files, cache files, cookies, and other electronically-recorded information.

This court did not intend the definition to be limited only to the terms listed. Like the Kleiner court, the Advisory Committee to the Federal Rules of Civil Procedure did not intend the term "electronically stored information" to be defined in a way that did not contemplate future technological developments. When Rule 34 of the Federal Rules of Civil Procedure was originally adopted, it contemplated the discovery of documents and things. The 2006 amendment to Rule 34 explicitly included the term "electronically stored information" and placed such documents on the same plane as traditional paper documents. Though the term is not specifically defined in the Federal Rules, the Advisory Committee acknowledged that the term "electronically stored information" is intended to be broad in order to cover types of electronically stored infor-
As electronic recordkeeping and communication became more prevalent, courts began to see discovery requests from litigants for such information. Even before the amendments to the Federal Rules of Civil Procedure in 2006, courts recognized certain legal tenets regarding the discovery of electronically stored information. First, courts acknowledged that computer records, whether deleted or not, were discoverable under Rule 34. In addition, courts were obligated under Rule 26(c) to protect the parties responding to discovery requests “from annoyance, embarrassment, oppression, or undue burden or expense.” Finally, courts could limit discovery when the burden or expense of the discovery outweighed the benefit of production. Even with these overarching principles in mind, courts have taken different approaches to the discovery of electronically stored information. Courts have been confronted with problems relating to the scope and form of production, the accessibility of the electronically stored information, and the cost of discovery. Luckily, the Federal Rules of Civil Procedure provided courts some guidance to help resolve these issues.

A. Zubulake v. UBS Warburg LLC

The landmark case regarding the accessibility of electronically stored information is Zubulake v. UBS Warburg LLC. Zubulake involved an employee’s claim under Title VII against her supervisor for sex discrimination and retaliation. Though UBS produced some of the e-mails requested by Zubulake, the dispute stemmed from Zubulake’s request for production of e-mails that she knew had not been initially produced and had been deleted by UBS. UBS had an e-mail backup system that backed up the e-mails on tapes and optical discs. To restore e-mails from backup tapes took about five days, or with the help of a vendor, the backup tapes could be restored faster at an increased cost. The optical disc backups created by UBS could not be rewritten or erased and were searchable using a language search, and UBS had kept each disc from the time of implementation of the backup system.

The court reconfirmed the presumption that even with electronic evidence, “the responding party must bear the expense of complying with

12. Id.
14. Id.
15. Id.
18. Id. at 312.
19. Id. at 313.
20. Id. at 314.
21. Id.
22. Id. at 315.
discovery requests." Under Rule 26, the cost of production only shifts to the party with electronic discovery requests when the cost of production creates an "undue burden or expense" on the responding party. Merely because the evidence is electronic does not create an undue burden or expense on the responding party. The court clarified that the primary consideration as to whether production of documents would lead to an undue burden or expense is whether the information is in an accessible ("stored in a readily usable format") or inaccessible format. The court considered that the e-mails Zubulake requested could be in one of three different places with varying levels of accessibility: active user e-mail files (accessible); e-mail archived on optical discs (accessible); and e-mail on backup tapes (inaccessible because it required processing to be placed in a readily usable format). As such, only with respect to the backup tapes did the Zubulake court find that cost shifting could be considered. In addition, the court revised the factors stated in Rowe Entertainment, Inc. v. William Morris Agency, Inc. to be assessed in determining whether the cost of discovery should be shifted to the requesting party. The seven factors included in the modified analysis are

1. The extent to which the request is specifically tailored to discover relevant information;
2. The availability of such information from other sources;
3. The total cost of production, compared to the amount in controversy;
4. The total cost of production, compared to the resources available to each party;
5. The relative ability of each party to control costs and its incentive to do so;
6. The importance of the issues at stake in the litigation; and
7. The relative benefits to the parties of obtaining the information.

These factors are not of equal weight; the first two being the most important and the last being the least important. The court recognized that the analysis is fact-based and, after considering accessibility, UBS was ordered to produce e-mails on the optical discs, active e-mail files, and e-mails from five backup discs documenting the results, time, and money spent. After this initial assessment, the court would consider the

23. Id. at 316 (quoting Oppenheimer Fund v. Sanders, 437 U.S. 340, 358 (1978)).
24. Id.
25. Id. at 318.
26. Id. at 318, 320.
27. Id. at 320.
28. Id.
31. Id.
32. Id. at 324.
33. Id.
cost-shifting analysis regarding e-mails on the backup discs. Ultimately, UBS's willful deletion of e-mails and recycling of backup tapes led to the strongest sanction—an adverse inference jury instruction.

In the fifth Zubulake opinion, Judge Scheindlin emphasized that the implementation of a litigation hold is not the end of a party's discovery obligations. The court recognized the following duties of counsel with respect to e-discovery: (1) the obligation to identify all sources of information that could be relevant and (2) the duty to preserve the information, produce it at the request of the responding party, and supplement responses when counsel has knowledge that a prior response was incorrect. With respect to the duty of preservation, the opinion sets out four steps for counsel to take: (1) issue a litigation hold and periodically reissue it to make sure that it is not placed on the backburner, (2) communicate with key employees who are likely to have relevant information and be explicit about the duty to preserve, (3) request copies from employees of relevant active files, and (4) ensure that relevant backup tapes are safeguarded. This opinion strongly warns counsel and their clients about the duty to preserve relevant electronically stored information and the penalties they both may incur for failure to do so.

B. RULE 26(b)(2)(B)'S LIMITATIONS ON ELECTRONICALLY STORED INFORMATION

The 2006 amendment to Rule 26 followed suit with the Zubulake court's decision. In pertinent part, Rule 26(b)(2)(B) provides that "[a] party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost." The party from whom discovery is sought has the burden of establishing undue burden or cost. After this burden is met, the court may still order discovery of electronically stored information if the party requesting the information shows good cause based on a balance of the costs and benefits of discovery of the information. In addition, similar factual considerations addressed by the seven Zubulake factors are also relevant to determine whether the responding party is required to produce information that is not reasonably accessible. The Advisory Committee's note makes it clear that if a party iden-

34. Id.
36. Id. at 432.
37. Id. at 432–33.
38. Id.
39. Id. at 441.
41. Id.
42. Id.
43. "Appropriate considerations may include: (1) the specificity of the discovery request; (2) the quantity of information available from other and more easily accessed sources; (3) the failure to produce relevant information that seems likely to have existed but is no longer available on more easily accessed sources; (4) the likelihood of finding relevant, responsive information that cannot be obtained from other, more easily accessed sources. The Advisory Committee's note makes it clear that if a party iden-
tifies sources of electronically stored information as not reasonably accessible, the party’s duty to preserve the evidence is not thereby relieved. As was required by the Zubulake court, sampling of the sources may be an option so the court can learn more about the costs involved in obtaining the information and the burdens of production.

C. RULE 45 AMENDMENTS

Analogous to the amendments made to Rule 26, Rule 45, regarding production of electronically stored information from nonparties, was also amended. The same issues regarding discovery of electronically stored information from parties occurs with nonparties—undue burden or cost; preservation; cost-shifting; and possession, custody, and control. The amendments to Rule 45 explicitly recognized electronically stored information could be obtained by subpoena. Once again, like the amendments to Rule 26, the production of electronically stored information is determined by the accessibility of the information. Subpoena is also available to allow for testing and sampling to determine burden or cost on the party responding to the subpoena.

But a distinction between Rule 45 and Rule 26 is that the status applied to the nonparty is different from that applied to a party-opponent. Courts have made a distinction between nonparties and litigants and have recognized that nonparties should not bear the same burden as litigants. Courts consider a number of factors to determine whether the burden to a nonparty is undue, including “how narrowly tailored the request is, cost, availability of the information, importance to the issues at stake, and the benefits to the parties.” In the factor balance, courts give nonparty status substantial weight in determining whether a subpoena imposes an undue burden. The rationale for this factor is sound: it would be unfair for nonparties to pay the “significant litigation costs of others.” In addition, if courts allowed litigants to place significant costs of litigation on nonparties, the chance that nonparties would comply with discovery requests in the future would be slim. Thus, the burden on nonparties is crucial to consider because they may potentially be a source of invaluable

*Sources:* (5) predictions as to the importance and usefulness of the further information; (6) the importance of the issues at stake in the litigation; and (7) the parties’ resources.” Fed. R. Civ. P. 26 advisory committee’s note.

44. *Id.*
45. *Id.*
48. *Id.*
49. *Id.*
51. *Id.* at 312.
52. *Id.* at 313.
53. *Id.*
54. *Id.*
information. When a court determines that the discovery requests impose an undue burden on a nonparty, it may order that the cost of discovery be shifted to the requesting party.\textsuperscript{55}

Similar to its Rule 34 counterpart, nonparties, like parties, must respond to discovery requests with information within their “possession, custody, or control.”\textsuperscript{56} Courts define control in various ways, ranging from broad expansive definitions to narrower ones. One court defined control as “the legal right to obtain documents upon demand.”\textsuperscript{57} Another court established that “documents are considered to be under a party’s control when that party has the right, authority, or practical ability to obtain the documents from a nonparty to the action.”\textsuperscript{58} Other courts found that “the practical ability to obtain the documents from another, irrespective of his legal entitlement to the documents” is controlling.\textsuperscript{59} The burden is on the requesting party to establish that the nonparty or party has such control.\textsuperscript{60}

II. THE EMERGENCE OF SOCIAL MEDIA

As courts dealt with the problems of electronically stored information in the form of e-mail, the realm of electronically stored information began to change drastically. With the advent of social media, the ability to communicate information also changed. Social media has been defined as “a group of Internet-based applications that build on the ideological and technological foundations of Web 2.0, and that allow the creation and exchange of User Generated Content.”\textsuperscript{61} Social media is an umbrella term that encompasses both Facebook and Twitter. Because of the tremendous use of Facebook and Twitter for marketing purposes, this Comment will focus on these two sites in analyzing the problems with electronic discovery that social networking sites may pose.

A. FACEBOOK

When Facebook was created by former Harvard student Mark Zuckerberg,\textsuperscript{62} there was no way that he could have known that what started out as a mere hobby would turn into a worldwide phenomenon. Zuckerberg initially began Facebook at Harvard, where it was well received by the students, and the project then spread to other universities.\textsuperscript{63} The site

\textsuperscript{55} Id.
\textsuperscript{56} \textit{FED. R. CIV. P.} 34; \textit{SEDONA CONFERENCE}, \textit{supra} note 46, at 4.
\textsuperscript{57} United States v. Int'l Union of Petroleum & Indus. Workers, AFL-CIO, 870 F.2d 1450, 1452 (9th Cir. 1989).
\textsuperscript{60} \textit{Int'l Union of Petroleum & Indus. Workers}, 870 F.2d at 1452.
\textsuperscript{63} Id.
was designed to put students in contact with one another and share photos.\footnote{Jonathan Strickland, \textit{How Facebook Works}, \textit{How Stuff Works} (Dec. 10, 2007), \url{http://computer.howstuffworks.com/internet/social-networking/networks/facebook.htm}.} Two other Harvard students, Dustin Moskovitz and Chris Hughes, joined Zuckerberg to expand the site.\footnote{Id.} Moskovitz and Zuckerberg dropped out of Harvard a few months later to run the site full-time.\footnote{Id.} They changed the name of the site to Facebook and purchased the domain name facebook.com in August 2005.\footnote{Id.} Initially, Facebook was available only to users with an e-mail address associated with an academic institution.\footnote{Id.} Today, any individual who has a valid e-mail address can join Facebook.\footnote{Id.} Facebook is considered a social networking site that provides people with an effective way to share information with others.\footnote{Id.}

Facebook profiles are generated after users create accounts.\footnote{Id.} A Facebook profile is a web page Facebook users will see if they search for a particular person on the site.\footnote{Id.} Users can join networks on Facebook based on commonalities, such as schools, employers, or cities.\footnote{Id.} Facebook allows members of networks to see other users' profiles in the same network.\footnote{Id.} Users can connect with other users by sending "friend requests."\footnote{Id.} Unless the user adjusts his or her privacy settings, the default setting on Facebook allows anybody to view the user's profile.\footnote{Id.} The person viewing the information does not need to have a Facebook account and, in general, the information on a profile set to "everyone" is public information and can be indexed by third-party search engines as well.\footnote{Id.} This default setting furthers the purpose of a social networking site.\footnote{Id.} A user can modify the privacy settings to set limits as to who can view his or her profile.\footnote{Id.} If "everyone" content is deleted from a user's profile page, Facebook removes the information from the profile, but makes no guarantees as to the use of the information outside of the site.\footnote{Id.}

On a Facebook profile, a user can upload a profile picture, view profile pictures of Facebook friends, and modify personal information the user has opted to share with other members.\footnote{Id.} In addition, a user's friends are notified if he modifies his profile or adds new friends via the mini-feed

\begin{itemize}
    \item \footnote{Id.}
    \item \footnote{Id.}
    \item \footnote{Id.}
    \item \footnote{Id.}
    \item \footnote{Id.}
    \item \footnote{Id.}
    \item \footnote{Id.}
    \item \footnote{Id.}
    \item \footnote{Id.}
    \item \footnote{Id.}
    \item \footnote{Facebook's Privacy Policy, FACEBOOK, \url{http://www.facebook.com/policy.php} (last visited Aug. 15, 2010).}
    \item \footnote{Id.}
    \item \footnote{Id.}
    \item \footnote{Id.}
    \item \footnote{Id.}
    \item \footnote{Id.}
    \item \footnote{Id.}
    \item \footnote{Id.}
    \item \footnote{Id.}
    \item \footnote{Id.}
    \item \footnote{Id.}
    \item \footnote{Id.}
    \item \footnote{Id.}
\end{itemize}
feature. Finally, the most popular portion of the profile is the wall, where Facebook members can write messages for the user that can be seen by others when they visit the user's profile. On the Facebook homepage, a user is alerted as to the happenings in his network and is able to leave status updates, similar to a blog posting, for his friends to see, which may include what he is doing at that time or what he is feeling. The user is also able to see the status updates of his Facebook friends on his homepage. Though it may seem odd to publicly announce to all of a user's Facebook friends what he is doing, at least one user is extremely happy that he did because it provided him a verifiable alibi that placed him elsewhere at the time he allegedly committed a crime.

In addition to these features, Facebook allows users to post photos and videos to the site, send instant messages to friends while they are online, and send messages akin to e-mail. Businesses can create special profile pages that are slightly different than the typical user profile page. Users can become fans of the business, rather than friends of the business. In addition to accessing the site on computers, users can also access Facebook on their mobile phones. Due to the large number of users and the vast amount of information on Facebook, the likelihood that information on this site may be needed during discovery is quite high.

B. Twitter

Another social networking site that is gaining popularity is Twitter. Biz Stone and Jack Dorsey, co-founders of the San Francisco-based company Obvious Corporation, founded Twitter. Twitter split from Obvious and became Twitter Inc. in March 2006. Twitter allows users to post messages that are sent to a network of contacts—their followers on Twitter. It allows a user to post a single message that is distributed to all of his friends, like a mass text message or e-mail. A “tweet” is a message sent via Twitter, and users must create an account with Twitter to tweet. Twitter profiles could be used as a user's blog by keeping all of the tweets public so that any person on Twitter can view them on the user’s profile.
After a user establishes a Twitter account, the user can invite other people to join Twitter and can become followers of other users’ posts. Tweets can only contain text—not pictures or videos—and if users want to provide photos or videos in a tweet, they must send a link to the webpage that hosts the content to their Twitter network. Like Facebook, Twitter can also be accessed using mobile phones. Twitter posts not only provide users or followers the ability to keep up with a certain individual but also may form the basis of a lawsuit, as Courtney Love was quick to find out. Courtney Love was sued for libel based on her tweet about a fashion designer. A similar fate may await Facebook users who haphazardly post to their accounts.

The privacy settings on Twitter are similar to those on Facebook. The default setting on Twitter is public, which means that the information will be instantly delivered to the public. The user can modify the settings to make information more private. Public tweets are also searchable via search engines. Like the Facebook servers, the Twitter servers record information when users use the service, including the IP address, pages visited, and browser type.

C. Obtaining Information from Facebook and Twitter for Litigation

As the realm of electronic information expands, the realm of discoverable information also expands. How can electronic information from Facebook and Twitter be discovered for litigation purposes? It may be as easy as a search on the Internet, if the information is available on a profile with a privacy setting of “everyone” on Facebook or a public Twitter profile. If it is not that easy to obtain the information through a basic Internet search or search of the site, another way to obtain it is to subpoena the social networking site. Facebook has procedures in place for the preservation and the procurement of information from the site. For obtaining information in civil cases, the site requires a subpoena from California. For preservation orders, Facebook recommends that the party making the request provide specific information to the site so that

96. Id.
97. Id.
98. Id.
99. Id.
101. See Facebook’s Privacy Policy, supra note 76.
103. Id.
104. Id.
105. Id.; see Facebook’s Privacy Policy, supra note 76.
107. Id.
108. Id.
the request can be made and processed quickly. Facebook charges a processing fee per user ID. There are limitations, however, that prevent the site from producing content from a user's Facebook profile without user consent. The Stored Communications Act provides that "a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service." The Act does not apply to communications that are "readily accessible to the general public." The Act is also broad enough to encompass social networking sites. There are exceptions to the statute that allow for a party to obtain the information without consent of the user.

Likewise, Twitter has similar policies for obtaining information from the site. Twitter has no problem releasing public information, but the release of private information about users requires a subpoena. The subpoena can be mailed or faxed to Twitter and should include the web address of the Twitter profile and what specific information is requested. Twitter conducts most communications through e-mail, and if the request is sent from non-law enforcement officials, Twitter requires that the communication be sent through regular support methods. Otherwise, Twitter lists a specific e-mail address for law enforcement officials. With respect to preservation requests, the request must be accompanied by a subpoena or court order and sent by mail, fax, or e-mail. Users generally will not lose access to Twitter when their account is under a preservation order.

III. THE LAW OF ELECTRONIC DISCOVERY TODAY

Though few cases in the United States touch on the aspects of social networking and discovery that this Comment addresses, comparisons can be made to case law regarding other forms of electronically stored information, including e-mails and text messages. As social networking sites tend to be a hybrid of these means of communication, the case law that

---

109. The information Facebook requests includes the party's contact information, response due date, full name of the user, full internet address to the user's Facebook profile, the user's date of birth, email addresses, IM names, phone numbers, address, and the period of activity to be preserved. Id.
110. Id.
111. Id.
113. Id. § 2511(2)(g).
115. 18 U.S.C. § 2702(b), (c).
117. Id.
118. Id.
119. Id.
120. Id.
121. Id.
pertains to these areas may be relevant precedent in litigation relating to social networking.

Just as history tends to repeat itself so, too, can cases. In a recent decision, Judge Scheindlin emphasized the principles in the Zubulake decisions that she issued six years ago and defined gross negligence in the context of discovery.\textsuperscript{122} In \textit{Pension Committee of the University of Montreal Pension Plan v. Banc of America Securities}, the plaintiffs failed to implement timely litigation holds and were careless in their efforts to collect after the duty to preserve arose.\textsuperscript{123} Before the plaintiffs filed suit, the attorneys for the plaintiffs contacted them to begin preserving documents.\textsuperscript{124} The issue in the case was whether the plaintiffs' conduct merited the imposition of sanctions for the spoliation of evidence.\textsuperscript{125}

In deciding the case, Judge Scheindlin clarified four concepts which are applicable to all forms of electronically stored information:

\begin{itemize}
  \item [T]he plaintiffs' level of culpability. \ldots the interplay between the duty to preserve evidence and the spoliation of evidence. \ldots which party should bear the burden of proving that evidence has been lost or destroyed and the consequences resulting from that loss. \ldots [and] the appropriate remedy for the harm caused by the spoliation.\textsuperscript{126}
\end{itemize}

Regarding the level of culpability in the discovery context, Judge Scheindlin found that a failure to preserve evidence that causes evidence to be lost or destroyed is at least negligent and may be gross or willful depending on the particular circumstances of the case.\textsuperscript{127} As previously mentioned in her fifth Zubulake decision, "the failure to issue a written litigation hold constitutes gross negligence because that failure is likely to result in the destruction of relevant information."\textsuperscript{128} Depending on the circumstances of the particular case, the failure to take appropriate measures with electronically stored information is at least negligent.\textsuperscript{129} Examples of gross negligence include failing to collect records from key players, destroying e-mail or backup tapes after the duty to preserve has taken effect, and failing to collect information from the files of former employees still in the possession, custody, or control of the company after the duty to preserve has arisen.\textsuperscript{130} In considering the duty to preserve and spoliation, the imposition of sanctions results from the court's duty to prevent abuse of the judicial process.\textsuperscript{131} The duty to preserve arises when parties reasonably anticipate litigation, and when that duty arises, the parties have a responsibility to pause their normal document-retention-

\begin{flushright}
123. \textit{Id.} at 476.
124. \textit{Id.} at 473.
125. \textit{Id.} at 463.
126. \textit{Id.}
127. \textit{Id.} at 464.
128. \textit{Id.} at 465.
129. \textit{Id.} at 464.
130. \textit{Id.} at 465.
131. \textit{Id.} at 466.
\end{flushright}
and-destruction policies and put in place a litigation hold so that relevant evidence is not destroyed. Spoliation occurs when evidence is not preserved or is altered, affecting its evidentiary value.

With regard to burden of proof, the question is who should bear the burden of establishing the importance of information that can no longer be found due to spoliation. When the sanctions requested are fines or cost shifting, the court considers the conduct of the party that failed to preserve the evidence and the resulting prejudice that failure may have caused the other party. If more severe sanctions are requested, such as an adverse inference instruction, the court must consider in addition to the conduct of the party causing spoliation, whether the evidence lost was relevant and, as such, caused prejudice to the opposing party. Relevance in this context requires the party requesting severe sanctions to establish that the evidence would have aided in establishing its claims or defenses, which is a higher standard than mere relevance. There is a rebuttable presumption of relevance and prejudice when a party acts in bad faith or is grossly negligent. In the context of negligence, the innocent party has the burden to establish relevance of the destroyed evidence and prejudice to the innocent party as a result. Judge Scheindlin employed the following test for the shifting of the burden:

When the spoliating party’s conduct is sufficiently egregious to justify a court’s imposition of a presumption of relevance and prejudice, or when the spoliating party’s conduct warrants permitting the jury to make such a presumption, the burden then shifts to the spoliating party to rebut that presumption. If the spoliating party demonstrates to a court’s satisfaction that there could not have been any prejudice to the innocent party, then no jury instruction will be warranted, although a lesser sanction might still be required.

Finally, with respect to the remedy, the court acknowledged that it has broad discretion in determining sanctions. The types of sanctions available to the court are “further discovery, cost-shifting, fines, special jury instructions, preclusion, and the entry of default judgment or dismissal.” The court should generally impose the sanction that is the least harsh but still affords an adequate remedy.

Another general consideration with respect to production of electronically stored information is the language of Rule 34, providing that a party

---

132. Id.
133. Id. at 465.
134. Id. at 466.
135. Id. at 467.
136. Id.
137. Id.
138. Id.
139. Id. at 467–68.
140. Id. at 468–69.
141. Id. at 469.
142. Id.
143. Id.
may request production of electronically stored information "in the responding party's possession, custody, or control." Rule 34 can only be used against parties to an action. Control exists when "a party has a legal right to obtain documents," and may be established if a principal-agent relationship exists or if a contract establishes that right. A requesting party is generally not allowed to search for data in the possession of a nonparty unless that party can show that the materials requested were in the possession or are currently in possession of the party to whom the discovery request was made. With these general principles in mind, this Comment will now turn to specific decisions regarding particular types of electronically stored information.

A. E-MAIL

Courts take different approaches with production of party e-mails and nonparty e-mails. In a Title VII case out of New York, the defendants, former employers of a plaintiff, requested production of e-mails from the plaintiff's America Online account. The plaintiff contended that her supervisor and the chief financial officer of the company made unwelcome sexual advances and that she was fired in retaliation for reporting the conduct. After the employee's attorney contacted the employer by letter, the employer hacked into her America Online e-mail account, which was established before her employment but paid for by the employer during her employment, and forwarded approximately four hundred e-mails from her account to the employer's e-mail. The defendants requested production of every e-mail from the employee's America Online e-mail account during the time period the employer was paying for the account and also requested the e-mails that were relevant to her claims of sexual harassment and emotional distress. The reason the employer paid for the account was because it served as a backup e-mail system when the plaintiff's company e-mail account did not work. The plaintiff also included in her complaint a hacking claim, and the defendants contended that the e-mails that were not intercepted by the employer were relevant to establish the employer's ownership of the account for the purposes of that claim and also her claims of emotional distress. The court found that these reasons were not justifications for the production of all of the plaintiff's e-mails, as she had already produced all e-

144. FED. R. CIV. P. 34.
145. Id.
149. Id.
150. Id.
151. Id. at *2.
152. Id. at *1.
153. Id. at *2–3.
mails relating to her claim for emotional distress.\textsuperscript{154} The court astutely noted that production of the e-mail account to this extent would be a requirement for "the production of every thought she may have reduced to writing or, indeed, the deposition of everyone she might have talked to."\textsuperscript{155}

Likewise, in \textit{Mackelprang v. Fidelity National Title Agency of Nevada}, an employee sued her employer for sexual harassment based on violation of Title VII.\textsuperscript{156} The issue in the case concerned a defendant’s motion to compel production of e-mails from the plaintiff’s two MySpace accounts.\textsuperscript{157} After a defendant discovered what it believed to be the plaintiff’s accounts, it subpoenaed MySpace to obtain information from the accounts, including private e-mail communications.\textsuperscript{158} In response, MySpace only provided public information from the accounts and refused to produce any private e-mail communications absent a search warrant or consent from the plaintiff.\textsuperscript{159} The defendant attempted to gain the plaintiff’s consent for production of the e-mail messages from MySpace, but the plaintiff refused on the grounds of invasion of privacy and irrelevance.\textsuperscript{160} The court denied the defendant’s motion to compel and stated that "[t]he proper method for obtaining such information, however, is to serve upon [p]laintiff properly limited requests for production of relevant email communications."\textsuperscript{161} The court did not preclude further discovery by the defendant to determine whether the MySpace accounts were actually the plaintiff’s.\textsuperscript{162} But, the court did emphasize that if the plaintiff failed to produce relevant e-mails from her MySpace accounts, after a determination that they were her accounts, she could be subject to sanctions for such conduct.\textsuperscript{163}

As mentioned previously,\textsuperscript{164} there are limitations on the ability of third-party providers to respond to subpoenas for information from their sites. \textit{In re Subpoena Duces Tecum to AOL, LLC} reiterates the limitations placed on the ability of internet service providers to disclose information of their subscribers.\textsuperscript{165} The case surrounded a lawsuit regarding claims made by a party after Hurricane Katrina.\textsuperscript{166} State Farm, the defendant, subpoenaed America Online, requesting production of e-mails from a nonparty witness’s account.\textsuperscript{167} State Farm also requested any and

\begin{thebibliography}{167}
\bibitem{154} Id. at *3.
\bibitem{155} Id.
\bibitem{157} Id. at *2.
\bibitem{158} Id.
\bibitem{159} Id.
\bibitem{160} Id.
\bibitem{161} Id. at *8–9.
\bibitem{162} Id.
\bibitem{163} Id.
\bibitem{164} See supra Part II.C.
\bibitem{165} 550 F. Supp. 2d 606, 608 (E.D. Va. 2008).
\bibitem{166} Id.
\bibitem{167} Id.
\end{thebibliography}
all documents, for a six-week period of time, from the witness's e-mail address or account. After State Farm's refusal to withdraw the subpoena, the witness moved to quash the subpoena because it violated the Privacy Act, was overbroad, and required production of privileged e-mails.

With respect to the privacy claims, the court found that America Online could not provide the contents of the witness's emails to State Farm because there is no exception for the disclosure of such communications pursuant to civil discovery subpoenas in the Privacy Act. The court made it clear "that 'unauthorized private parties' and governmental entities are prohibited from using Rule 45 civil discovery subpoenas to circumvent the Privacy Act's protections." On the issue of whether the subpoena imposed an undue burden on the witnesses by being too broad, the court found that the request of all of the witness's e-mails for a six-week period was too broad because there was no limit on the e-mails' relevance to the suit. Because the parties requested e-mails over a six-week period, the subpoena placed an undue burden on the witness because the e-mails produced may likely include personal and privileged information unrelated to the suit. Thus, production of electronically stored information from third-party providers has certain limits that even a Rule 45 subpoena cannot overcome. Though there are limits, a party may be required to produce electronically stored information relevant to the suit from third-party providers and be subject to sanctions for a failure to do so.

B. Text Messaging

As Twitter is based on technology similar to text messaging, case law relating to the discovery of text messages may be applicable. Whether text messages are discoverable or whether obtaining such information from a third-party provider would violate the privacy interests of the user is generally an issue with such forms of communication. The Ninth Circuit decided whether employees had a reasonable expectation of privacy with respect to text messages transmitted via a two-way pager in Quon v. Arch Wireless. Though the case involved public employment, the same principles could be applied in the context of private

168. Id. at 608-09.
169. Id. at 611.
170. Id.
171. Id. at 612.
172. Id.
173. Id.
175. Strickland, supra note 91.
177. Quon, 529 F.3d at 895.
178. Id.
Social Networking in the Workplace

Arch Wireless had a contract with the City of Ontario to provide text-messaging services and to the City, which two of the plaintiffs received. The City had no policy in place regarding text messaging but had a general policy regarding computer usage applicable to all employees. The policy specifically limited the computer usage to City related business and stated that use of the equipment for personal benefit violated the policy. The policy also stated that “[u]sers should have no expectation of privacy or confidentiality when using these resources.” Plaintiffs signed an employee acknowledgement indicating that they had read the computer policy, and a few years later, one of the plaintiffs attended a meeting where he was informed that the pager messages would be considered e-mail and that the policy applied to them too. The City did not have a formal policy with respect to the pagers, but per the terms of its contract with Arch Wireless, the City was assessed overage charges whenever a user went over 25,000 characters in a month. A commander with the police department’s administration bureau was in charge of collecting the overage fees from employees when they went over their limit and had a policy of not reviewing the messages when the employee paid the overages. When officers exceeded their limit multiple times, the commander was ordered to get transcripts of the text messages from the provider to audit whether they were business-related messages or personal ones and to determine if the character limit on the pagers should be increased. The City got the messages from Arch Wireless, after Arch Wireless verified that the numbers corresponded to the pagers that belonged to the City. Upon review of the transcripts, the City found that one of the plaintiffs had exceeded his limit because he was sending personal sexually explicit messages to other plaintiffs. The police officers brought suit claiming that the disclosure of the text messages violated the Stored Communications Act and the Fourth Amendment.

On appeal, the Ninth Circuit held that the users of the services had a reasonable expectation of privacy with respect to the messages stored by Arch Wireless due to the informal policy of the official in charge of collecting the overage charges. The court also found that Arch Wireless violated the Stored Communications Act by providing the messages to the City. The Supreme Court held that the Ninth Circuit was incorrect in concluding that the department’s search of Quon’s text messages was

179. *Id.*
180. *Id.* at 896.
181. *Id.*
182. *Id.*
183. *Id.*
184. *Id.*
185. *Id.* at 896–97.
186. *Id.* at 897–98.
187. *Id.* at 898.
188. *Id.*
189. *Id.*
190. *Id.* at 906.
191. *Id.* at 903.
unreasonable. The Court explicitly failed to delineate precise guidelines as to an employee’s expectation of privacy when utilizing employer-provided communication devices. The Court also emphasized that an employer’s policy regarding communications on employer-provided communication devices will shape an employee’s reasonable expectations of privacy regarding such communications, particularly if the policy is clear. This case may provide guidance to private employers as to what degree the informal representations of employees can undermine a formal policy in place at a company. It appears that the representations of an employee with the authority or delegated authority to enforce the policies of a company may be sufficient to override the stated policy of the employer, particularly when the policy is not clearly communicated. A company that has a detailed written policy in place that is not enforced is no better off than a company that has no formal policy in place.

A recent case out of the Eastern District of Michigan also highlights the discovery issues with text messaging. In *Flagg v. City of Detroit*, the defendants tried to prevent discovery of text messages sent by city-issued text messaging devices. The City of Detroit entered into a contract with a third-party (nonparty) provider for text messaging services to city officials and employees. The City terminated its contract with the third-party provider, but the provider continued to maintain some records of the messages that were sent during the period of the contract. The plaintiff requested from the third-party provider production of “text messages sent or received by 34 named individuals, including the individual Defendants, during a number of time periods spanning over 5 years, and . . . sent or received by any City official or employee during a four-hour time period in the early morning hours of April 30, 2003.”

In opposition to the subpoena, the defendants argued that the production of the text messages would violate the Stored Communications Act, which prohibited the production of text messages in the possession of a third party for civil discovery purposes. Though the plaintiff tried to obtain the information by means of a Rule 45 subpoena, the court clarified that the same information could have been obtained via a Rule 34 subpoena and proceeded under that assumption. The court made the

---

193. *Id.*
194. *Id.* at 2630.
198. *Id.*
199. *Id.* at 347–48.
200. *Id.* at 348.
201. *Id.*
202. *Id.* at 358.
distinction between a customer of the third party and a party outside of the relationship and determined that the information could be obtained under Rule 34 but did not answer the question as to whether the information could be obtained under a Rule 45 subpoena without a violation of the Stored Communications Act.\textsuperscript{203} Also important to the court was the fact that the city employees were informed that the sent messages should be considered public information, property of the City, and not private in nature.\textsuperscript{204} These factors indicated that the employees gave their implied consent for production of the archived messages from the third-party provider.\textsuperscript{205} As such, the court ordered plaintiffs to prepare a Rule 34 request for production so that the defendants could have the information produced from the third-party provider.\textsuperscript{206} Thus, the text messages were discoverable under Rule 34 of the Federal Rules of Civil Procedure.

In a case from the Northern District of California, the court ordered a plaintiff to produce her Sidekick mobile phone.\textsuperscript{207} The case concerned claims by the plaintiffs regarding a denial of overtime pay by the defendant.\textsuperscript{208} The plaintiff in question owned a business in addition to working for the defendant, and the Sidekick was paid for by the other business.\textsuperscript{209} The defendant requested production of communications and documents from the Sidekick, claiming that a denial of overtime relates to how the plaintiff spent her time when working for the defendant.\textsuperscript{210} The court ordered the plaintiff to produce communications and documents relating to her work for her other business during the dates and times she worked for the defendant.\textsuperscript{211} Thus, these communications could have included text messages from her Sidekick.\textsuperscript{212}

C. SOCIAL NETWORKING SITES

In 2009, the United States District Court in Colorado denied a motion for protective orders by plaintiffs when the defendant Wal-Mart sent subpoenas to social networking sites seeking information about the plaintiffs in a lawsuit related to injuries they sustained while working at Wal-Mart.\textsuperscript{213} The plaintiffs claimed that the information sought fell within patient-physician privilege and spousal privilege.\textsuperscript{214} The court found that the information sought by the subpoenas was "reasonably calculated to lead to the discovery of admissible evidence as is relevant to the issues in

\textsuperscript{203} Id. at 366.
\textsuperscript{204} Id. 364–65.
\textsuperscript{205} Id. 365.
\textsuperscript{206} Id. at 366.
\textsuperscript{207} Ho v. Ernst & Young LLP, No. C05-04867 JF (HRL), 2009 WL 2756365, at *1 (N.D. Cal. Aug. 27, 2009).
\textsuperscript{208} Id.
\textsuperscript{209} Id.
\textsuperscript{211} Id. at *1–2.
\textsuperscript{212} See id. at *1–2.
\textsuperscript{214} Id. at *1.
this case” and denied the protective order.215 The question here was how can information posted on a social networking site be considered privileged after disclosure of the information to individuals able to view the plaintiffs’ profiles?

Though there is little U.S. case law relating specifically to discovery issues and social networking sites, a recent Canadian case is worth mentioning. The plaintiff John Leduc was involved in a car accident with the defendant.216 The plaintiff claimed a loss of enjoyment of life as a result of the negligent driving of the defendant.217 Though Facebook did not come up at the discovery conference, it did come up during an evaluation by a psychiatrist for the defense.218 Upon finding out that the plaintiff had many friends on Facebook, defendant’s counsel searched the plaintiff’s Facebook profile but found that only his Facebook friends could view the plaintiff’s profile.219 The defendant requested an order to preserve and produce all information on the plaintiff’s profile.220 The lower court found that the Facebook profile was a document and that it was within the control of the plaintiff.221 However, the lower court did not require the plaintiff to produce his Facebook page because the defendant did not meet his burden of establishing that the plaintiff had relevant information on his page.222

Similar to the Federal Rules of Civil Procedure, the Ontario Rules of Civil Procedure require a party to produce “‘every document relating to any matter in issue in an action that is or has been in the possession, control or power of a party’ and to produce each such document unless privilege is claimed over it.”223 In determining whether the lower court was correct in its determination, the court considered how other courts in Canada have approached the production of Facebook profiles.224 The court made distinctions between two types of Facebook profiles—public and private.225 A user can have both a private and a public profile, and the court allowed the inference to be made that information on the public profile is also likely to be found on the private profile.226 With respect to users that only have a private profile, the court stated that based on the social networking purpose behind the site, it can be inferred that users intend to make personal information available to other people on the site.227 The court made it clear that a user with a private profile stands on

215. Id. at *2.
217. Id.
218. Id. para. 3.
219. Id. para. 5.
220. Id. para. 6.
221. Id. para. 8.
222. Id. para. 9.
223. Id. para. 12 (quoting Ontario Rules of Civil Procedure, R.R.O. 1990, Reg. 194, r. 30.0(1), (2)).
224. Id. paras. 23–24.
225. Id. para. 26.
226. Id. para. 29.
227. Id. para. 31.
equal footing as a user with a public profile. The court mentioned that based on Facebook’s Terms of Use, it is clear that the profile is within the user’s control because he can add or delete content from his profile, and the party still has the obligation to produce information from his Facebook page relevant to the suit. But the mere existence of a profile does not mandate the production of the contents of that page. The court found that the defendant should have been able to question the plaintiff to determine what relevant information was posted on the site and ordered this to occur. The court stated it best:

To permit a party claiming very substantial damages for loss of enjoyment of life to hide behind self-set privacy controls on a website, the primary purpose of which is to enable people to share information about how they lead their social lives, risks depriving the opposite party of access to material that may be relevant to ensuring a fair trial.

The court also set out a procedure to follow with respect to the discovery of Facebook profiles. When a party discovers the opposing party’s Facebook profile, the following steps should be taken to ensure that the party discovering the profile has the opportunity to determine whether the site contains information relevant to the suit. Specifically, the user should be required to preserve and maintain printouts of the materials posted on his site, produce that to the opposing party, and when few documents are produced, allow the opposing party to cross-examine the user to find out if there is relevant content on the site.

Thus, it appears that privacy controls had limited utility in preventing the exposure of a party’s Facebook profile in litigation. Though a party requesting the information still has the burden of establishing that the information is relevant before a court will order production, the permissible inferences the Canadian court allowed regarding content of the site when a user has both a public and a private profile essentially would allow the content of the site to be produced in most cases. Unless a user is particularly cautious, it is rare that the pictures available on a public profile will not in some way be relevant to a lawsuit, particularly when a user claims damages for a loss of enjoyment of life.

228. Id. para. 32.
229. Id. para. 27.
230. Id. para. 32.
231. Id. para. 36.
232. Id. para. 35.
233. Id. para. 34.
234. Id.
235. Id.
236. See id. para. 32.
237. See id. paras. 28–30.
D. Are Social Networking Sites Discoverable?

The case law regarding e-mail and text messaging could be equally applicable to the use of Facebook accounts with privacy settings in place in the private employment context. If there is a question as to whether the information on a social networking site may be discoverable, by analogy to third-party providers of e-mails and text messaging, it appears that the information on such sites would be discoverable in civil litigation. Though a private employer does not pay for access to a Facebook account, the account is hosted by a third party and could be used for both business and personal use.238 Thus, applying the principles from Rozell v. Ross-Holst, a judge would have discretion to limit production of the information posted to a Facebook account to the extent of the parties’ initial disclosures.239 The use of a social networking site at work thus would not give the defendants or plaintiffs free reign to discover anything and everything posted on the site when privacy controls are in place on the account.240 Allowing discovery of a Facebook profile just because a party has an account would create the situation where counsel would just be fishing for information on the site without any basis.241 Moreover, considering the networks and numerous friends that a person has on the site, it is economically unfeasible to require production of every posting, e-mail, or conversation on the site for an extended period of time because sorting through the information would take too much time to justify the value of the information. It is for this very reason that a request for production from such social networking sites may be used strategically against a party to drive up the cost of discovery and push the case toward settlement.242 Also, because companies likely have not encountered numerous requests for production regarding the sites and are unfamiliar with them, it is likely that such requests can be used to distract the party from the real issues of the case, in addition to driving up the costs of discovery.243

If a party to a suit has a Facebook account or a Twitter account, a court would likely find that such an account is in the possession, custody, or control of the party, and as such, a party would need to produce relevant information from the site under Rule 34 based on the user agreements in place with Facebook and Twitter.244 An additional concern is the ability to procure the information for discovery purposes. A recent virtual

240. See id.
243. Id.
244. See Leduc, 308 D.L.R. 4th, para. 27.
Social Networking in the Workplace

roundtable by Symantec addressed the problems with obtaining a record of the information from Facebook or Twitter in a useable, understandable format. When users view their profile page on Facebook, it appears to them to be a consolidated page with all information in one place. However, when such user content is archived, information is located in different databases and does not appear in the same format as it appears on a Facebook page. Thus, to pull all the information together and decipher how a page appeared takes more time than if the information on a page at any given time were stored as a discrete package of information, like a word document or an e-mail. This will likely create the biggest e-discovery hassle with respect to compliance with discovery requests.

Another consideration is the Stored Communications Act and the degree that the Act may affect the ability of a party to a suit to obtain information from a third-party provider. It appears that Rule 45 subpoenas issued to third-party providers have limitations that Rule 34 requests for production can overcome. Thus, in the initial interrogatories stage, a party should question whether relevant information is present on a Facebook or Twitter page and request that the opposing party produce the information under Rule 34. By going through the party itself to obtain the information, the issues with consent and the Stored Communications Act may be avoided if the information is from the party’s own profiles.

IV. SOCIAL NETWORKING AND THE WORKPLACE

Considering the problems that may arise with the use of social networking in the workplace, private employers and their counsel must consider the benefits and the costs associated with the use of such sites in the workplace. Twitter and Facebook market to employers that they can use the sites to connect with their clients or consumers. But the legal implications of the use of such sites and the need to preserve the sites in the anticipation of litigation may lead to headaches for employers, their IT groups, and their counsel. As such, employers who decide to use social networking sites for marketing purposes, for internal communications, or for communications with their clients need to take steps to ensure that if the information is ever needed for discovery, they are well-prepared.

245. See Wendt, supra note 4.
246. Id.
247. Id.
248. Id.
251. See id.
253. See Wendt, supra note 4.
The first decision to be made by employers is whether to allow their employees the use of social networking during business hours while at work. The use of social networking in the workplace may be beneficial but may also be problematic due to a loss of productivity in the workplace, the potential for theft of data, liability for the contents of the sites in lawsuits, and damage to the employer’s image. Due to these risks, many companies have banned the use of Facebook and Twitter in the workplace, including certain investment banks and law firms. Some employers that do not completely ban the use of Facebook have taken a middle-ground approach to the posting of information on the site. For example, ESPN prohibits its employees from posting onto Facebook or Twitter any content related to sports without its permission. The Associated Press takes an even stronger approach and requires its employees to monitor what they and their friends say on Facebook, and to delete certain posts on their Facebook pages. Assuming that employers allow social networking in the workplace, certain steps can be taken to minimize their risk, both with respect to the company’s fan page and the employees’ personal profiles.

A. COMPANY FAN PAGES

The creation of a company fan page may seem like an easy task, but the employer must consider whether the page can be archived or preserved in anticipation of litigation and who has access to the page to act as its administrator. The first issue to consider in creating a company’s Facebook page or Twitter account is who is responsible for maintaining and monitoring the site. It has been suggested that a separate e-mail account should be created for all social networking site endeavors and account information should be available to all “stakeholders.” It is important that the company’s Facebook page is viewed as a company-controlled page, rather than any kind of individual asset. As such, the company should limit who posts on these sites as the face of the company. In addition, the individuals in charge of the page should monitor the postings and comments.

An additional consideration regarding who should have access to the page is how to limit access once the employee is terminated or leaves employment. Suppose that an employee in charge of postings on a company’s social networking page is fired. Assuming that person is the

255. Id.
256. Id.
257. Id.
258. Id.
260. Id.
261. Id.
262. Id.
administrator of the company's Facebook page, that employee could still maintain access despite the fact that he is no longer with the company.263 Because the individual could post to the page and damage the company's reputation, there must be a limit in place to prevent such an occurrence.264 One source suggests that a company can create a profile page akin to a personal profile page.265 Once that page is created, a page for the company can be created and additional administrators to the page can be added.266 These administrators can be readily changed so that when an employee who was in charge of the page leaves the company, he can be deleted as an administrator.267 Thus, when a company page is created, an employer must decide who will administer the social media sites and transmit information from the company to the public and ensure that upon termination, the ability of the terminated employee to access the sites as an administrator is prevented.

In addition, employees in charge of the site should have clear guidelines as to what can and cannot be posted on the company's Facebook page. Also, it should be clear that the monitoring of social media and postings on such sites are within the scope of employment of the individual and subject to any limitations and restrictions that the company imposes on such postings. There should be an approval process in place before a posting is made so that upper management in marketing has some oversight in the process. By doing so, the employer maintains a level of control over the postings such that it will be accountable for the content. Because the page should be viewed as a company-controlled asset, it is likely that a court would find that the site is within the company's "possession, custody, or control" and as such, information pertinent to suit must be disclosed to the opposing party and produced by the party in custody of the material.268 As mentioned previously, there are many problems with the way that social networking sites are archived that could lead to problems in obtaining the information.269

There are a few steps that employers can take to make sure that they do not suffer spoliation sanctions for destruction of information relevant to suit on their social networking pages. First, if a company has a reasonable anticipation of litigation, it should issue a litigation hold and a preservation order and contact Facebook and Twitter to make sure they are aware of the preservation order. The preservation order should be specific, relate to the company page for a set period of time, and advise administrators not to delete the postings from the page. In addition to contacting Facebook and Twitter, the administrators of the site for the company should be aware of the holds. Luckily, with Facebook, as long

---

263. See id.
264. Id.
265. Id.
266. Id.
267. Id.
268. FED. R. CIV. P. 34.
269. Wendt, supra note 4.
as posters and administrators have not deleted postings on a company's page, older posts can be seen with mere clicks on the company page. But, Facebook does not guarantee that such information will always be available by this method. With Twitter, however, there is approximately a one-and-a-half-week window in which the tweets can be retrieved by searching for them using the search engine on Twitter, though they never disappear from a user's Twitter stream. Thus, once again, with a litigation hold, the administrators of a Twitter site should not delete content from the Twitter page during the relevant time period to avoid the extra step of having to retrieve the information from Twitter itself.

Companies that want to be extra cautious with their Facebook or Twitter pages may want to archive the pages themselves and save them locally. There are programs in circulation for archiving tweets that a company's IT department would be able to implement successfully, but this is a task for IT to undertake. The same archiving possibility may exist for Facebook as well, and it is a good idea for IT to consider whether locally archiving a company's Facebook page would be a viable option. But once again, a company's IT group should formulate the policy regarding the archiving of such sites after discussion with upper management and counsel.

B. EMPLOYEE-SPECIFIC SOCIAL NETWORKING PAGES

A harder aspect to address is whether a company should permit employees to use social networking sites for business purposes, including communications with clients and internal communications with coworkers. If employers allow access to social networking sites or employees circumvent controls that limit their access, employees may be using the sites to conduct the business of their employers or collaborate with colleagues. As such, the information that relates to the employment of the individual may be relevant to a potential suit. The policy that an employer takes with respect to the use of social networking must be specific and detailed but at the same time, cannot be so constraining that the purpose for using the sites to reach clients, consumers, and colleagues is defeated.

IBM has taken the reigns and developed guidelines specific to social

271. Id.
273. There are many options for people who want to archive their tweets or other user's tweets that may be good for preservation purposes. See id.
274. See McCOWN & NELSON, supra note 270, at 252–54.
computing. The company places some responsibility on its employees for monitoring what is said on social networking sites and reporting conduct that strays from its guidelines. This would be an important part of any policy relating to social networking to ensure that the policy has an enforcement mechanism. Particularly unique to IBM's policy is the requirement that when employees discuss matters related to the company, employees have to identify themselves by name and their role at the company and make it clear that they are speaking for themselves and not on behalf of the company. In addition to this, the company requires employees who post to blogs to use a disclaimer that the views posted do not represent the company's views. The guidelines require employees to be thoughtful with respect to dispersing internal, confidential communications externally via social networking sites. Also, the employee may not comment on the business performance of the company or affirm or deny rumors related to the company's business performance. The company makes users personally responsible for the information that is posted on these sites and emphasizes that employees cannot alter previous posts without making it clear that the post has been altered. The policy also requires employees to be respectful with their postings and gently reminds employees not to let their social networking activities interfere with their work-related commitments and duties.

In addition to the IBM guidelines, there are a few additional steps that employers can take with respect to an employee's use of social networking in the workplace that may avoid the problems associated with obtaining the information for litigation purposes and maintain a company's reputation on social networking sites. First, like IBM has done, companies should make sure that they create a social networking policy that is specific and that employees are educated about the policy and the repercussions in the case of violations of the policy. The policy should also be enforced. An umbrella computer usage policy may not be sufficient to encompass the specific concerns related to social networking, especially if social networking is not mentioned. With respect to enforcement, the company should be consistent and actually follow its own policy guidelines for the policy to have any meaning.

In contrast to a general e-mail policy that usually advises employees that their business e-mail communications should not be considered private, social networking sites are usually not viewed in this way because they are personal accounts. A step that employers could take is to re-
quire employees who would like to use social networking for business purposes to create a separate business account, based on their business e-mail address, as a condition to use the sites in the workplace and on the employer's equipment, including mobile phones, desktops, and laptops. In addition, the company could require that the employee link to the company's fan page or website on his own business page. The employees should also be made aware that the information they post on social networking sites, their e-mails, and conversations may be discoverable. The employer should formulate a written agreement stating that in exchange for the employee's access and use of social networking in the workplace, the employee will grant consent for the disclosure of the information from his business profile page, including e-mail, posts, notes, and all features of Facebook or Twitter used for communication purposes, in the event the information is needed for litigation or general auditing purposes. The policy must also make it clear that the employee has no expectation of privacy with respect to communications on social networking sites made through the employee's business account, on the employer's computer network, or on the employer's hardware, including desktop computers, laptop computers, and mobile phones.284

In addition to implementing a detailed policy with respect to social networking, employees who use the sites must be educated that the same rules that apply with respect to business conversations and communications apply to the use of social networking in the workplace. Though social networking users generally do not adhere to the rules of formality associated with business communications, it is imperative that employees are educated that communications for business purposes on social networking sites should adhere to the same level of formality as e-mail communications and other written communications for business purposes. Thus, employees should be mindful of what they say on such sites and should be educated that what they say could lead to liability, not only for them but also for their employers.285

Employers should also include in their policy the degree of privacy that the employee account should maintain at a minimum.286 It is unlikely that an employer would want their employees' profiles set to public so that an Internet search would reveal information about the employer's business contacts and clients. Depending on the nature of the information and the business of the company, the employer must be explicit regarding what privacy settings the employees' profiles should maintain so that the employers and employees are protected from the unwanted viewing of business profiles on social networking sites. Also, the employer should require employees who want to modify their privacy set-

286. See Facebook’s Privacy Policy, supra note 76; Twitter Privacy Policy, supra note 102.
tings to contact the employer for any modifications in deviation of the employer's social networking policy.

By using a contract where the employee agrees to consent to disclosure of the information in exchange for use of social networking sites at work for business purposes, a company will be able to ensure that it has the ability to access information so that it retains control of its employees' reluctant actions on social networking sites. If a company decides to allow employees to communicate for business purposes on social networking sites, it is imperative that the guidelines be clear with respect to what the employees can and cannot say on the site, the employees' expectations of privacy regarding the communications, the employer's expectations of professionalism, and the penalties for failure to follow the guidelines. And once again, the policy should be enforced to have any merit.

C. DATA RETENTION POLICIES AND LITIGATIONS HOLDS

From a discovery standpoint, employees' use of social networking for business purposes will greatly increase the realm of discoverable information that a company has to control, and as such, modifications to data retention procedures must be made. If litigation is anticipated, a company and its counsel should issue a litigation hold that encompasses information posted on social networking sites—no information should be deleted from the employer's page, the employee's business pages, or archives thereof. As mentioned in Zubulake, a litigation hold does not end the counsel's duty of preservation. The litigation hold with respect to the information on social networking sites must be reissued periodically to make sure that employees are aware of their obligations. In addition, employers and counsel must request the information from social networking sites or gain access to it from employees who likely have relevant information and be particularly explicit with those employees' obligations of preservation. To save time, employers may also request that employees locally archive their social networking site pages to ensure that the data is not lost. There is a caveat with this approach—the stronger the data retention policy, the more data there will be to mine in the event of a discovery request. Companies should be mindful that a policy should be implemented but should also be cautious that in the event of litigation, spoliation does not occur that results in discovery sanctions. Ultimately, companies should be educated about media their employees are using to collaborate with each other, contact clients, conduct business, and should work with their IT groups to formulate reten-

289. See id. at 433.
290. See id.
291. See McCown & Nelson, supra note 270.
tion and archiving policies that are suited for their specific business needs.

V. CONCLUSION

Though social networking sites are great marketing tools for companies, their use in the workplace must be guided by specific guidelines to protect employers and their employees from liability. Companies must take into consideration their ability to obtain the information in the event that it is needed for discovery purposes and revise their computer usage and data retention policies to account for these needs. There is no cookie-cutter policy that applies to all employers and companies; a company must create a policy to meet the customized needs of its business. Social networking is now the norm, and it is time for employers to recognize that their use in the workplace is happening, whether or not it is specifically condoned or guided by policy. Before companies post links on their websites to find them on Facebook or follow them on Twitter, they should consider the legal implications of such solicitations and ensure that they have adequate policies in place so that they are well prepared in the event of litigation.