New York Law Journal
Technology Today
WWW.NYLJ.COM
©2009 INCISIVE MEDIA US PROPERTIES, LLC
An incisivemedia publication
VOLUME 241—NO. 124
TUESDAY, JUNE 30, 2009

FEDERAL E-DISCOVERY ISSUES

Social Networking Data Presents New Challenges

By **H. Christopher Boehning**
And **Daniel J. Toal**

The rapid growth of social networking Web sites in the workplace means companies can no longer ignore them. Companies should consider whether their current electronic communications policies are sufficient to cover social networking sites.

If one asked practitioners and judges to describe the type of electronically stored information (ESI) at issue in e-discovery cases, most of the time the answer would be "e-mail" or possibly "Microsoft Office files." In fact, there is a dearth of federal e-discovery decisions on other types of ESI. Whereas a decade ago e-mail was often excluded from discovery as part of an unspoken agreement between parties, today all sorts of electronic communications are potentially discoverable. User activity on social networking sites like Twitter, LinkedIn, Facebook, and MySpace warrant serious concern.

According to a recent article in The New York Times, "Time spent on social networks surpassed that for e-mail for the first time in February [2009], signaling a paradigm shift in consumer engagement with the internet."[1]

Although many people use social networking services for purely personal pursuits, the presence of these services are now being felt in the business world. Companies are beginning to take advantage of social networking sites for their marketing and business potential. And employees now use them to manage both personal and professional relationships. Like it or not, social networking has come to the office, and its arrival presents a host of challenges. Those challenges can best be met through a formal policy, which should also address how to consider this online activity when collecting ESI for discovery.

Companies have embraced the social networking arena for its marketing and business potential. These sites offer corporations and their employees opportunities to investigate job applicants, encourage community and collaboration within their businesses, "rub virtual elbows" with other professionals in their field, and communicate directly with customers and consumers.[2]

Mutual fund giant Vanguard recently launched a Facebook profile. "Facebook lets us show a more personal side of Vanguard—a side that may not always come across through our traditional communication channels," said Amy Dobra of Vanguard's retail marketing and communications department.[3]

As the Times reported, companies have even begun to hire specialists who use social media to connect the company to its customers or potential customers.[4] These specialists follow posts on Twitter called "tweets." If they find a negative tweet, they try to control the situation by "snuffing out complaints before they snowball."

Businesses that use social networking sites to interact with customers in this way will inevitably have to confront difficult legal and compliance questions.

For example, the Federal Trade Commission has recently proposed revisions to its Advertising Guidelines that would require bloggers endorsing a product to disclose their relationship to the product's company.[5] By making such sites a part of their marketing plan, companies also need to anticipate and plan for the prospect that these electronic communications may become relevant and discoverable in litigation.

Even those companies that have yet to embrace social networking sites for their marketing potential can no longer afford to ignore the fact that their employees are unquestionably using these sites.

In addition to discovery concerns, other issues arise when employees log on to these sites—whether from the office or from home—for personal or professional use. Some companies have fallen victim to malware attacks through social networking sites visited by their employees.[6]

Employers and employees need to be aware of the potential to leak confidential information on social networking sites, often inadvertently. Employers have fired employees for their tweets and posts. For example, Virgin Atlantic Airways fired employees after they posted negative comments on Facebook about the airline and its customers.[7] In fact, such incidents are common enough that there is even a term, "dooced," used to describe being

H. CHRISTOPHER BOEHNING *and* DANIEL J. TOAL *are litigation partners at Paul, Weiss, Rifkind, Wharton & Garrison LLP.* LIAD LEVINSON, *an associate at the firm, and* JENNA STATFELD, *a summer associate at the firm, assisted in the preparation of this article.*

In some jurisdictions, this reprint may be considered attorney advertising. Past representations are no guarantee of future outcomes.

fired from one's job because of postings on a personal site.[8]

Now that social networking activity exceeds e-mail usage, employers and employees would be well advised to consider whether their current policies are appropriate. That is especially true given that employers and employees do not always see eye to eye.

According to one study, the majority of business executives believe they have a right to know everything their employees are doing on social networking sites, while a majority of employees say activity on these sites is not their employers' business.[9]

Companies must confront, and reconcile this disparity in perception and expectation. They should first determine the forms and extent of office social networking use that they are willing to permit.

After considering the sites' benefits, the risks and the needs of their company, management should create a policy. Because social networking sites present unique issues for the workplace, in many cases it will not be enough to rely on existing e-mail use policies.

Approaches to social networking in the marketplace will vary. Some businesses have blanket bans on the use of social networking sites at the office, while others deal with this new media in a more nuanced way.

Companies should tailor policies that fit their needs; there is no one-size-fits-all answer. IBM, for example, requires its employees to identify themselves when discussing the company online, ensuring that readers know that they are speaking in an individual capacity, and not on behalf of IBM.[10]

Companies should train employees to think before they click, tweet or post. For example, while investment bankers and lawyers often are trained to guard confidential information about deals, are they trained to think about the tweets from each stop on their deal-specific due diligence tour? Policies should encourage personal responsibility and treat employees like adults, while also explaining and underlining the risks for the company and the consequences of wrongful social networking behavior.

The policy should be well publicized, and should be as consistent as possible with other existing media policies. Doing so will provide the opportunity for companies to embrace new social media technology, use it in a productive way to enhance business, and still ensure that both the company and the employees are protected and prepared for any legal issues that might arise.

Discovery, Preservation Issues

Before companies embrace social networking technology and roll out a new policy, they would be well advised—as with any new technology—to first ensure that they are prepared to deal with the discovery and preservation obligations that may flow from corporate or employee use of social networking sites.

If these Web sites are used for business, has the company taken steps to ensure that the data can be preserved, retrieved and produced if requested?

For example, if a company uses Twitter to reach its customers, is it prepared to preserve and produce those postings if relevant to a litigation? How would this data be preserved and collected, when it is not in the custody or control of an employer?

Like it or not, social networking has come to the office, and its arrival presents a host of challenges. Those challenges can best be met through a formal policy, which should also address how to consider this online activity when collecting ESI for discovery.

These are especially tricky issues given the scant guidance on preservation obligations for ephemeral data of the type associated with most social networking activity. Although some courts have considered ephemeral data within the context of the duty to preserve, courts have yet to determine specific obligations for preservation and production of social networking activity.[11]

Even if such information is deemed discoverable, courts will still have to wrestle with novel admissibility and evidentiary issues.

Conclusion

As with any new technology, companies need to think about preservation and collection before they adopt the technology.

Companies that already have embraced social networking should ensure that they are prepared to preserve, collect, and produce social networking data for an appropriate case and that their electronic communications policy is ready for the new social networking reality.

1. Teddy Wayne, Social Networks Eclipse E-mail, N.Y. Times, May 18, 2009. The number of users of these sites grows each day. Currently, 35 percent of adult Internet users in the United States have an online social networking profile, a figure that has more than quadrupled since 2005. Amanda Lenhart, Social Networks Grow: Friending Mom and Dad, Pew Research Center Publications, Jan. 14, 2009.

2. Jessica E. Vascellaro, Social Networking Goes Professional, Wall Street Journal, Aug. 28, 2007.

3. "Introducing Vanguard's Facebook Page, available at, https://personal.vanguard.com/us/news?article=/freshness/News_and_Views/news_ALL_facebook_05272009_ALL.jsp."

4. Laura M. Holson, Tweeting Your Way to a Job, New York Times, May 21, 2009.

5. WOMMA Submits Comments on FTC's Proposed Revisions to Advertising Guidelines on Testimonials and Endorsements, Reuters, March 5, 2009.

6. Two Thirds of Businesses Fear That Social Networking Endangers Corporate Security, Sophos Research Reveals, Sophos Website, April 28, 2009.

7. Losing Face, Economist, Nov. 6, 2008.

8. This term was coined by a person who was fired for her personal blog posts about her coworkers. See http://en.wikipedia.org/wiki/Heather_Armstrong. Many of the concerns that apply to social networking sites will also apply to blogs.

9. Andrew LaVallee, Bosses and Workers Disagree on Social Network Privacy, Wall Street Journal, May 19, 2009.

10. IBM Social Computing Guidelines, available at http://www.ibm.com/blogs/zz/en/guidelines.html.

11. See, e.g., *Columbia Pictures v. Bunnell*, 2007 U.S. Dist. LEXIS 46364 (C.D.Ca. 2007). See also *Arista Records LLC v. Usenet.com Inc.*, 2009 WL 185992 (SDNY 2009); *Convolve Inc. v. Compaq Computer Corp.*, 223 F.R.D. 162 (SDNY 2004).

Reprinted with permission from the June 30, 2009 edition of the NEW YORK LAW JOURNAL. © 2009 Incisive Media US Properties, LLC. All rights reserved. Further duplication without permission is prohibited. For information, contact 877-257-3382 or reprintscustomerservice@incisivemedia.com. # 070-06-09-10