Privacy and Social Media in the Workplace

Justin G. Vaughn, Esq

THE VAUGHN LAW OFFICES, P.L.L.C.

E-MAIL: jvaughn@vaughn-law.com
www.vaughn-law.com

Privacy and Social Media in the Workplace

Social media is becoming more prevalent each year, both in and out of the workplace. People are engaging in Tweeting and Facebooking, directed toward the public and specific persons. Social media involves making of statements, posting of photographs, sharing of information, and re-posting of items submitted by others. As a result, social media poses a constant and significant impact on the workplace, ranging from ill-conceived comments to criminal harassment and cyber stalking.

The workplace impacts of social media are numerous. The implications which are widely evolving in employment law include sexual harassment claims, NLRB administrative complaints, arguments concerning privacy rights, litigation over the discovery of social media, and the implementation of social media workplace policies.

I. SOCIAL MEDIA AND SEXUAL HARASSMENT CLAIMS

Social media has become increasingly more prevalent, through formats such as Facebook, Youtube, Linkedin, Twitter, text messaging, instant messaging, and other forms of digital communication. Indeed, conduct both in and out of the office can create a hostile work environment or sexual harassment issue. The law prohibits sexually motivated or related conduct that unreasonably interferes with an individual's work performance, or creates an intimidating, hostile, or offensive working environment. Such conduct may arise from a romance among co-workers or management, or unsolicited or unwelcome advances up to and including cyber stalking.

Digital communications have increased the tendency for workplace romances to evolve into sexual harassment claims. These claims may involve not only the prior participant in the workplace romance, but also other co-employees affected by the uncomfortable work environment. Courts have historically recognized that a hostile work environment created by a prior office romance are actionable. Additionally, promotions given to employees having romantic involvement with a supervisor have long been held actionable by the Courts. As applied to social media, such information can create a higher level of visibility for workplace romances, and a higher likelihood of discrimination and harassment claims. These scenarios are becoming for prevalent, ranging from posting of derogatory materials to public disclosure of the extent of off-duty romantic activities, to Foursquare tagging and cyber stalking, to Anthony Weiner's twitter posts and pornographic photographs.

II. SOCIAL MEDIA AND THE NLRB

The National Labor Relations Board was created by the National Labor Relations Act, as an administrative entity. Section 7 of the NLRA is intended to protect union and non-union employees to engage in protected concerted activities, including discussion of wages, work conditions, and terms of employment. As such, these discussions are protected by federal law, particularly where the discussions involve a call to action.

The NLRB has already been asked to address and prosecute numerous cases concerning social media. For example, in one the more noted cases on this issue, the Connecticut Regional Office of the NLRB issued a complaint against American Medical Response, Inc. for terminating an employee who made derogatory remarks about a supervisor on Facebook. The NLRB asserted that the employer's policy and actions were unfair labor practices, where they interfered with the employee's rights to engage in

concerted activity. The AMR policy had prohibited any discussion about the employer on social media, and AMR subsequently settled the matter and adopted a new policy to expressly allow discussions about wages, work conditions, or terms of employment.

The NLRB has since stated that an employer cannot have policies that create a blanket prohibition to employee social media comments that would damage a company or the company's reputation. Further, the NLRB has stated that attempted rectifying language that suggest that "all National Labor Relations Act rights are intact" is inadequate to resolve such blanket policies. The NLRB has also stated that an employer cannot have a policy that requires the employee to obtain the employer permission in order to make a social media post. (See the NLRB statement on social media dated May 30, 2012).

As a side note, the FTC has indicated that they will discipline employers for posting of fraudulent testimonials, with a sanction of $250,000.00 per fraudulent act, pursuant to the Fair Credit Reporting Act. Further, SEC regulations pursuant to the Fair Disclosure Rule prohibit a CEO from posting information that would violate the requirement to disclose material information to all investors at the same time.

For a copy of NLRB policies on social media, go to www.nlrb.gov/node/5078

III. SOCIAL MEDIA AND PRIVACY RIGHTS

While some claim privacy rights in social media, such rights appear to be largely evaporating. The fact that social media can be electronically saved, reproduced, and/or forwarded to others is commonly seen as eroding the expectation of privacy.

Certainly, there are organizational risks with use, or lack of use, of social media. An organization can be exposed to claims of defamation, copyright or trademark infringement, interference with business relations, disclosure of third party confidential information or trade secrets, or potential malpractice based upon postings by employees. Further, an employer could be subject to negligent hiring and retention claims for failing to find information available on social media. An individual employee also faces liability for postings which may impact their employment, including claims for defamation, copyright infringement, infliction of emotional distress, harassment, or cyber stalking. Inappropriate use of social media may result in adverse action by an employer, up to and including termination.

In the existing U.S. Supreme Court case concerning social media and the expectation of privacy, the Supreme Court declined to establish a sweeping rule. *City of Ontario v. Quon, 130 S.Ct. 2619, 560 U.S. ___ (2010).* In *Quon*, a SWAT team employee sent non-work text messages during work hours, some of which were sexually explicit. The City of Ontario, California, upon hearing of such texting, conducted a search of the phone and found the text messages, and terminated employment. The Supreme Court found that the search by the City was reasonable and did not violate Fourth Amendment expectations. However, the Court refused to define specific workplace expectations or a right to privacy, and refused to establish any rule on the expectation of privacy in social media. As such, this Supreme Court case helps employers in some respects, but does not set forth a bright line rule of law.

Questions that may bear upon the rights of privacy and reasonable expectations of privacy would likely include the question of whether the existing employer policy that prohibits the use at-issue, whether the employer in fact monitors such use, whether third parties have access to the information on computers, emails, or social media, and whether the employer is made aware of the policies and/or third party access. Further, the employer's right to review and rely upon information may include geotagging (the presence of geographical information on posts, particularly photos). At least one U.S. Court has identified that geotracking is an appropriate resource for criminal matters. *United States v. Skinner* (6th Cir. 2012) (affirming that technology can be used to track a criminal suspect through cell phone GPS location).

Further, privacy implications would include the significant question: does the individual know the privacy settings of all of their friends on social media. While some individuals claim that their social media is limited, such as Facebook limitations of purported privacy, absent any cogent argument that he individual knows all of the settings of their friends, and has control over their social media posts, it is difficult to imagine any reasonable argument of an expectation of privacy. At least one Court has recognized that there is no privacy right concerning derogatory comments about an employer on Facebook. Roberts v. Careflite, Tex.Civ.App. October 4, 2012.

While arguments have been raised concerning First Amendment issues, these are generally limited to a few scenarios. For example, the expectation of privacy can be upheld in a school setting, where a school code is determined to be unconstitutionally vague. However, sanctions upon students have been held appropriate when social media constitutes a substantial disruption of school activities. Further, public employees are protected in postings that are matters of public concern. Although at least one matter has been brought involving an argument on public versus private concern in social media postings by a firefighter, the suit was settled without decision.

Some federal laws have been used for arguments concerning social media. For example, the Stored Communications Act, 18 USC 2701 et. seq., makes it an offense for a person or entity to intentionally access without authorization an electronic communications service. The primary example of this scenario was the Houston's Restaurant litigation, which proceeded to a jury trial. In that case, Houston's managers had lied to get a password to access social media, and subsequently terminated employees who were posting complaints about management on a secured site. Interestingly, the jury determined that Houston's did not violate any common law privacy, and that the employees did not have a reasonable expectation of privacy. Instead, the jury determined that the Houston's management had violated the Stored Communications Act, in that they lied to obtain a password and access the site. Also note that one circuit has determined that cell phones do not constitute "stored" electronic communications for purposes of the Stored Communications Act. *Garcia v. City of Loredo*, 5th Cir. 2012 Pursuant to the Consumer Fraud and Abuse Act 18 USC 1030, it is unlawful to access a protected computer without authorization. If the "hacker" damages the computer or obtains information that they are not entitled to obtain, a violation of the act has occurred.

IV. SOCIAL MEDIA AND DISCOVERY

Social media is more commonly being used in investigation and discovery for litigation. For example, it is now common for investigators and divorce lawyers to review profiles on Facebook, Twitter, and Match.com. The American Bar Association has recently reported that since 2010, there have been over 1,000 reported decisions on the discoverability of social media. Many of these lawsuits involve personal injury claims, particularly pursuing a Facebook page and the photos saved and posted on Facebook. Generally, the courts have held there is no expectation of privacy, and production has been ordered. At least one court has additionally ordered disclosure of the user name and password for the other party to log in and access social media. Further, a court has recently held that the deletion of a social media website during pendency of a case is sanctionable.

V. SOCIAL MEDIA AND WORKPLACE POLICIES

It is estimated that 45% of employers look at network profiles when hiring, and that number continues to grow. In addition to policies and concerns of the NLRB, social media workplace policies are critically important for the employer.

The employer should establish policies applicable to the nature of the work performed. This may include specific policies to address posting of copyrighted material, preservation of confidentiality, a prohibition of false information, protection against professional malpractice, and certainly policies that are directed toward prevention of any hostile work environment or sexual harassment. Indeed, as early as 2005, companies were being held liable where notice was given of inappropriate conduct, and the company failed to act. *Doe v. XYC Corp*, 887 A.2d 1156 (2005) (holding company liable where company had notice of employee viewing child pornography at work, where employee posted child pornography during off work hours).

Most importantly, the employer should establish policies, implement and monitor controls, take appropriate preemptive action, and be diligent in corrective action. An employer should also implement policies that differentiate between employer provided devices, and employee's personally owed devices. Such policies should define the expectations of privacy, and the rights of the employer.

Each employer should consider employment practices liability coverage. Such coverage is not commonly found in general liability policies, but can be added to policy coverage. Such coverage helps provide indemnification and payment of counsel for lawsuits involving employment practices and decisions.