

**PRIVACY IN THE WORKPLACE:
EFFECTIVE SCREENING OF
POTENTIAL EMPLOYEES**

Presented By: Debra Weiss Ford, Esquire
fordd@jacksonlewis.com

**Jackson Lewis LLP
100 International Drive, Suite 363
Portsmouth, NH 03801
603.559.2700**

March 8, 2011

Debra Weiss Ford is the Managing Partner of the Portsmouth, NH office. Ms. Ford has close to 30 years of experience representing employers in litigation matters before the state and federal courts and administrative agencies. Ms. Ford also represents employers before the New Hampshire Commission for Human Rights, the Equal Employment Opportunity Commission, the New Hampshire Department of Labor, the Massachusetts Commission Against Discrimination, and the Maine Human Rights Commission.

Ms. Ford also lectures frequently at seminars in New Hampshire and Massachusetts on issues related to employment law, including discrimination, wrongful discharge, reductions in force, termination issues, personnel issues, privacy issues, and contractual issues. She regularly advises clients on employment-related matters.

Ms. Ford received her B.A., *magna cum laude*, from Drew University in 1979 and her J.D. from Temple University of School of Law in 1982. She is an approved federal and state mediator. She is a member of the New Hampshire Bar Association, Labor and Employment Law Section, Massachusetts Bar Association, Maine Bar Association, American Bar Association, New Hampshire Trial Lawyers Association, American Arbitration Association, the American Board of Trial Advocates, and the National Association of College and University Attorneys. She is admitted to practice in the State of New Hampshire, Commonwealth of Massachusetts, State of Maine, United States Court of Appeals for the First Circuit, United States District Court for the District of New Hampshire, United States District Court for the Commonwealth of Massachusetts, United States Claims Court, and the Supreme Court of the United States. Ms. Ford was a member of the New Hampshire Board of Bar Examiners from 1993 to 2005. She was appointed by the United States District Court for the District of New Hampshire to serve on the Merit Selection Panel to consider the reappointment of the incumbent magistrate. In 2003, she was appointed to serve on the Federal Court Advisory Committee.

Ms. Ford is named as New Hampshire's Best Labor and Employment Lawyer in 2010 by *Business NH Magazine*. She is listed by *Chambers* as one of America's Leading Lawyers for Business. She is the author of the New Hampshire chapter of *Workplace Privacy*, a legal reference book for managers and human resource professionals, published by the Thompson Publishing Group, a division of West Publications. Ms. Ford was elected as a Fellow to The College of Labor and Employment Lawyers in June 2006. She is listed in *The Best Lawyers in America* by Woodward White, Inc., and has been recognized by New England Super Lawyers as one of the top 50 women lawyers in New England and one of the top 100 lawyers in New England. She is listed in Top NH Lawyers in Labor and Employment in *New Hampshire Magazine*. She is rated AV by Martindale-Hubbell. Ms. Ford serves as a board member for Family Service, Inc., New Hampshire SPCA, and Rockingham Community Action.

TABLE OF CONTENTS

| | | |
|-----|---------------------------------------------------------------------|---|
| I. | INTRODUCTION | 1 |
| II. | THE LAWS AND ISSUES IMPLICATED BY SOCIAL MEDIA | 1 |
| A. | Applicant-Screening Concerns | 1 |
| 1. | Negligent Hiring | 2 |
| B. | Discrimination Laws | 2 |
| 1. | Protected Class Information..... | 2 |
| 2. | Genetic Information Nondiscrimination Act of 2008 | 3 |
| C. | Protected Activity Laws..... | 3 |
| 1. | National Labor Relations Act | 4 |
| 2. | Lawful Activities Laws..... | 5 |
| 3. | Public Employers | 5 |
| 4. | Whistleblower Laws | 6 |
| 5. | Retaliation Laws | 7 |
| D. | Privacy Concerns | 7 |
| 1. | Invasion of Privacy | 7 |
| 2. | Surveillance or the Impression of Surveillance | 8 |
| E. | Federal Laws Applicable to Electronic Communications and Data | 8 |
| 1. | The Electronic Communications Privacy Act..... | 8 |
| 2. | Stored Communications Act | 9 |

| | | |
|-------|-----------------------------------------------------------------------------------------------|----|
| F. | Other Tort Liability for Employers | 9 |
| 1. | Negligent Retention and Supervision | 9 |
| 2. | Defamation..... | 10 |
| 3. | Special Problems with References and Recommendations | 10 |
| G. | Employee Endorsements and Testimonials | 10 |
| III. | PRACTICAL STRATEGIES FOR ADDRESSING USE AND MISUSE OF SOCIAL MEDIA AT AND ABOUT WORK | 11 |
| IV. | ELEMENTS OF A SOCIAL MEDIA POLICY..... | 12 |
| V. | MAKING HIRING DECISIONS BASED ON INFORMATION FROM SOCIAL MEDIA OUTLETS | 14 |
| VI. | DRUG AND ALCOHOL TESTING | 15 |
| A. | The Americans with Disabilities Act | 15 |
| VII. | REFERENCE AND BACKGROUND CHECKS | 18 |
| 1. | Reference Checks..... | 18 |
| 2. | Fair Credit Reporting Act | 18 |
| 3. | Criminal Background Investigations | 20 |
| 4. | Motor Vehicle Background Investigations | 20 |
| VIII. | ADDITIONAL PRIVACY ISSUES..... | 20 |

I. INTRODUCTION

The process of hiring generally includes the following steps: identifying the needs, establishing the necessary qualifications for the job, advertising or using an employment agency, interviewing, testing, and making the decision of whether to hire a particular applicant. Making informed, intelligent hiring decisions is the most effective way to secure the best employees and reduce employee lawsuits and claims.

Many employers utilize a screening procedure to streamline the hiring process. The purpose of screening is to ensure that the applicant meets the minimum qualifications for the position. In today's new technological age, a potential way to screen applicants is through various social media sites and the internet. While it is important to determine whether an applicant has the qualifications for a position, as well as to assess an applicant's abilities, skills, experience, job history, professional affiliations and other factors which are essential to the job, it is also important to recognize the limitations and legal implications of utilizing online screening procedures.

The rapid growth and extensive reach of online social media sites, such as Facebook, MySpace, Twitter, YouTube, and the like, has forever changed the way people communicate. The employer-employee relationship is particularly impacted by this fundamental shift, with employers and employees struggling to define the boundaries of appropriate employee use of social media and employer-monitoring of this usage. In addition to concerns about employee productivity, social media sites create new challenges for businesses, with possible harm to corporate reputation and brands, as well as potential liability for employee behavior online. In addition to current employee issues, employers are also increasingly venturing into the world of social media themselves to market their businesses and to search for, recruit, and screen potential applicants, and this online activity also raises potential employment law risks.

Because of the relatively recent emergence and growth of social media, the legal landscape of employer obligations is still evolving, and there is little case law and legal authority specific to social media. Nevertheless, employers should be aware of some of the anticipated legal issues that could result from online applicant screening and the use of social media by current employees. These materials are a brief summary of the various laws that may be implicated in connection with the use of social media in the workplace by employees and employers.

II. THE LAWS AND ISSUES IMPLICATED BY SOCIAL MEDIA

A. Applicant-Screening Concerns

Employers are increasingly using the Web and social media sites to both identify and recruit desirable job candidates, as well as to weed out less desirable candidates. Just as there are legal limitations to screening applicants through more traditional methods, legal issues are also implicated when applicants are screened online. Depending on the circumstances, online screening may implicate background check laws, discrimination

laws, privacy and other tort laws, electronic communication statutes, and other laws. The following section summarizes some of the key laws that may be triggered by online screening of job applicants.

1. Negligent Hiring

Because employers can be held liable for negligent hiring, it is sometimes appropriate for an employer, depending on their business and particular position's duties, to do a more thorough screening of an applicant's background to try to ensure that the individual does not pose a safety or other risks to the business or third parties. Historically the doctrine of negligent hiring has resulted in employers considering whether it is appropriate to run a criminal background check on applicants. As social media becomes more common, however, it is possible, though not yet known, that the scope of an employer's duty to investigate job applicants for safety risks may extend to conducting social media or other online searches.

B. Discrimination Laws

1. Protected Class Information

Discrimination laws are also implicated by online applicant searches and screening. Federal (Title VII of the Civil Rights Act of 1964/the Age Discrimination in Employment Law) and New Hampshire (RSA 354-A) law prohibit discrimination both in hiring and employment on the basis of various legally protected class statuses, including race, color, creed, religion, national origin, sex, sexual orientation, marital status, disability, age and military service. Because of these laws, employers generally may not ask applicants about or solicit information about protected class status during the hiring process. In conducting an online search or reviewing social media sites of an applicant, however, an employer may learn information about the protected class status of an applicant that it would not otherwise know. Through standard disclosures on social media sites, or through voluntary disclosure of other personal information such as commentary and photos, applicants may reveal more information about themselves through social media than they normally would during the hiring process.

In making hiring decisions, employers can lawfully use information relating to an applicant's illegal drug use, poor work ethic, poor writing or communications skills, comments about previous employers, and racist or other discriminatory tendencies. Employers may also lawfully consider an applicant's general poor judgment in maintenance of his or her public online persona. While employers are not prohibited from learning protected class information, they are prohibited from considering protected class information in making hiring and employment decisions. Employers may face liability under federal, state and local laws for using any information learned from social media about an applicant's protected class status in a hiring decision. It may be difficult for the employer to prove in later litigation that it only viewed, but did not actually use, the information obtained in a social medium when making its hiring decision. As such,

having access to such information through online searches about applicants, or about current employees, can increase the risk of a discrimination claim. Special steps should therefore be taken to “wall off” the individual doing an online search from the hiring or employment decision process to ensure that protected class information is not shared or taken into account in the decision-making process.

2. *Genetic Information Nondiscrimination Act (GINA) of 2008*

The recently enacted federal GINA law also raises online considerations. GINA provides that it is an unlawful employment practice for an employer or other covered entity to “request, require, or purchase genetic information with respect to an employee or family member of the employee.” Section 202(a). GINA defines “genetic information” broadly, providing that genetic information may include an individual’s family medical history or an individual’s own disclosure of a genetic condition.

Because genetic information may be obtained through an online or social media search, employers need to take care not to violate GINA in doing online applicant screening or gathering information about employees. There are, however, some limited exceptions to GINA’s prohibition on the acquisition of genetic information that could arise in connection with online searches, including (a) inadvertent requests (often referred to as the “water cooler” exception); (b) employer-provided genetic services that keep results confidential; (c) requests related to FMLA leave; (d) information in purchased public documents such as newspaper obituaries; (e) information gained as a result of monitoring the effects of toxic substances in the workplace; and (f) DNA analysis of employees who do forensic analysis to ensure samples are not contaminated.

In addition, New Hampshire law prohibits discrimination based on genetic information. In New Hampshire, RSA 141-H:3 restricts the use of genetic testing in employment. Genetic tests may only be used as part of a worker's compensation investigation or to determine an employee's susceptibility to workplace toxins. An employee must give written, informed consent to genetic testing. Results may not lead to adverse employment consequences.

C. Protected Activity Laws

In addition to the above considerations, various federal and state laws provide that employers may not take adverse action against applicants or employees based on legally protected activities. As such, when online applicant screening or other online information about employees reveal protected activities by an individual, an employer needs to take care to ensure that it does not consider or act on such information in making its hiring or employment decisions. The following is a summary of some of the laws establishing protected activities of applicants or employees.

1. National Labor Relations Act (NLRA)

The NLRA contains several prohibitions which could apply to employers gathering information about applicants or employees through social media or other online searches. For instance, whether or not a workplace is unionized, Section 7 of the NLRA protects employees' rights to engage in concerted activity for mutual aid and protection. This can include such activities as outright union organizing, but also lesser acts such as discussing or complaining about compensation or terms and conditions of employment. Section 8(a)(1) of the NLRA further provides that it is an unfair labor practice for an employer "to interfere with, restrain, or coerce employees in the exercise of the rights guaranteed by Section 7." As such, employers need to take care not to take any adverse action against an applicant or employee due to online information about that individual's activities protected by Section 7 of the NLRA. In addition, in drafting and adopting any social media policies for current employees, a company should work with labor counsel to ensure that the policy does not infringe on NLRA rights and to determine if the policy needs to be collectively bargained in a unionized setting.

In a recent case involving workers and social media, the National Labor Relations Board ("NLRB") accused a company of illegally firing an employee after she criticized her supervisor on her Facebook page. This is the first case in which the NLRB has stepped in to argue that workers' criticisms of their bosses or companies on a social networking site are generally a protected activity and that employers would be violating the National Labor Relations Act by punishing workers for such statements.

The NLRB announced in November 2010 that it had filed a complaint against an ambulance service, American Medical Response of Connecticut ("AMR"), that fired an emergency medical technician, accusing her, among other things, of violating a policy that bars employees from depicting the company "in any way" on Facebook or other social media sites in which they post pictures of themselves. The NLRB took the position that Facebook is no different from the water cooler - employees are allowed to talk jointly about working conditions, including their supervisor.

The National Labor Relations Act gives workers a federally protected right to form unions, and it prohibits employers from punishing workers - whether union or nonunion - for discussing working conditions or unionization. The NLRB argued that AMR's Facebook rule was "overly broad" and improperly limited employees' rights to discuss working conditions among themselves.

AMR denied the NLRB's allegations, asserting that they were without merit. AMR asserts that the employee in question was discharged based on multiple, serious complaints about her behavior and that the employee was also held accountable for negative personal attacks against a co-worker posted publicly on Facebook which the company believes were not concerted activity protected under federal law.

A confidential settlement was reached in this case in February 2011 between the parties. Although this case addressed the use of social media by an employee rather than applicant, it is nonetheless illustrative of the potential pitfalls of using social media to screen applicants and making hiring decisions based on certain information obtained online.

2. Lawful Activities Laws

Employers that use the Web or social media sites to screen applicants, or to monitor or investigate employees, may uncover information about or observe pictures of an individual engaged in alcohol use, smoking, or other lawful activities which an employer might disagree with or prefer the individual not do. Because such activities may be legally protected, employers should, however, take care to learn of and comply with any applicable lawful activity laws to avoid running afoul of these laws.

For example, New Hampshire RSA 275:37(a) prohibits employers from requiring any covered employee or job applicant, as a condition of employment, to abstain from using tobacco products outside the course of employment as long as the employee complies with any workplace smoking policy. Violations of RSA 275:37(a) trigger criminal penalties and subject the employer to liability for double the employee's unpaid wages. RSA 275:39, 40.

An important New Hampshire case on the issue of right to privacy in the workplace is O'Brien v. Papa Gino's of America, Inc., 780 F.2d 1067 (1st Cir. 1986). Papa Gino's fired O'Brien after receiving the results of a polygraph examination which indicated O'Brien had lied (the case arose prior to the enactment of the federal Employee Polygraph Protection Act of 1988). O'Brien asserted, among other defenses, that he was asked questions about his drug use which were unrelated to his employment. The jury awarded O'Brien \$398,200 in the invasion of privacy claim alone. The First Circuit Court of Appeals upheld the verdict and rejected Papa Gino's argument that O'Brien contracted away his right of privacy by consenting to the employer handbook which prohibited drug use by employees.

3. Public Employers

For public employers, the Fourth Amendment of the United States Constitution might also be implicated in connection with online searches. The Fourth Amendment protects public employees from unreasonable searches and seizures, and this prohibition extends to electronic information.

On April 19, 2010, the United States Supreme Court heard the case of City of Ontario v. Quon, and issued a written decision on June 17, 2010. The case raised questions of whether law enforcement employees had a reasonable expectation of privacy in text messages sent on employer-provided devices where the employer had a written policy allowing inspection of messages but, in practice, did not regularly monitor messages. The Court held that the employee had an expectation of privacy in the messages, but that

the warrantless review of his pager transcripts was nonetheless reasonable because it was motivated by a legitimate work-related purpose and was not excessive in scope. Therefore, there was no Fourth Amendment violation.

There are a number of practical pointers that derive from the Quon decision. First, keep in mind that the decision focuses on a governmental employer and the Fourth Amendment constraints applicable to a governmental employer. However, it is clear that the decision has ramifications for private employers as well.

Second, with respect to investigations, the intent of the search is critical. Although this has direct applicability to governmental employers' investigations of their employees, the Court's observations should be considered by any private employer conducting an investigation bearing directly or indirectly upon an employee's expectations of privacy.

Third, a company's communication policy is extremely important. As the Court observed, "employer policies concerning communications will of course shape the reasonable expectations of their employees, especially to the extent that such policies are clearly communicated." Taking guidance from the Court, public and private employers alike should develop communications policies and communicate them clearly to their employees. It is important for public and private employers to understand that supervisory or managerial employees must avoid communicating information inconsistent with the communications policies. When this occurs, there is a substantial risk that the policy will be undermined.

Further, like other aspects of employment law, cases implicating privacy considerations will be heavily influenced by their own unique fact patterns. What are the broader factual circumstances of the dispute? What is an employee's expectation of privacy as it applies to electronic communications, even on devices issued by the employer? These cases seemingly will be adjudicated on a totality of the circumstances analysis.

Technology continues to evolve, and this evolution will continue to affect workplace norms and employees' privacy expectations. Variations on these issues are ripe for further adjudication in the future.

4. *Whistleblower Laws*

Employers also need to take care not to take adverse action based on protected whistleblowing activities that they learn about through online searches. In New Hampshire, an employer may not take adverse employment action against an employee based on the employee making a good faith report of a violation or suspected violation of law or refusing to participate in any activity that the employee in good faith believes is illegal. Some employees may use the Web or social media sites to complain about actual or suspected legal violations of a company. Because such complaints may, depending on the circumstances, be legally protected, employers should take care to assess legal risks before taking any adverse action in response to such information.

5. *Retaliation Laws*

A number of federal and state employment laws (including, but not limited to, anti-discrimination, wage and hour, leave, and workers' compensation laws) prohibit retaliation against an individual for asserting rights under the law, assisting someone else to assert their rights, or participating in an investigation or legal proceeding. Just as employers may learn of whistleblowing through online sources, employees may also learn of other protected activities that an individual may claim gives rise to anti-retaliation rights. An employer who learns of such activities through online sources must take care not to engage in unlawful retaliation.

D. Privacy Concerns

Another legal consideration for employers engaged in online searches about applicants or employees is these individuals' potential privacy rights. Because of the public nature of the Web and many social media sites, privacy laws may, at first blush, seem inapplicable. In fact, though, the law regarding online privacy rights is unsettled, and some of the few cases involving the issue have raised the possibility of legal risks for employers, at least when online data comes from a source, such as Facebook, with some privacy restriction settings. While privacy law is still unsettled and evolving, the following is a summary of some of the legal issues that might arise in the social media and other online contexts.

1. *Invasion of Privacy*

New Hampshire recognizes invasion of an individual's privacy as a tort action. The most common privacy claims raised by employees against employers are intrusion upon seclusion claims or claims for publication of private facts. To prove both types of privacy claims, however, the plaintiff must demonstrate a reasonable expectation of privacy. When online data is publicly available through a Web search engine, such as through a Google search, it may prove difficult for an individual to establish any expectation of privacy in the data at issue.

It is less clear, however, whether individuals might claim some reasonable expectation of privacy in social media sites with some privacy settings, such as Facebook, which allows users to limit access to the site to only individuals who have been approved by the user. While arguments can be made that data posted on such sites is not private because the user has already published the data or because an employer may have been appropriately granted access to the site by an authorized user, the law is not yet settled.

In addition, in at least one case involving a restricted MySpace chat room used by current employees, an employer was found liable for accessing the restricted site even though an employee participating in the site had given the employer permission to access the site. See Pietrylo v. Hillstone Restaurant Group, No. 06-5754, 2009 WL 3128429 (D.N.J. Sept. 25, 2009). While true permission to access the site might have given the employer a viable legal defense, in Pietrylo, the employee granting access later claimed to have felt

coerced into giving access and claimed the employer's review went beyond the scope of the employee's consent.

In the case of Stengart v. Loving Care Agency, 990 A.2d 650 (N.J. 2010), plaintiff exchanged emails with her lawyer using a personal Yahoo account. However, the emails were sent from her company-issued laptop. During discovery in an employment discrimination suit she initiated, the company reviewed the emails. The New Jersey Supreme Court ruled that the company violated plaintiff's reasonable expectation of privacy because the messages were exchanged using a password-protected account. Therefore, the Court credited plaintiff's belief that the emails were privileged and thus not subject to review. The Court noted, nonetheless, that an employer can regulate the use of its computer systems. However, an employer does not have a license to read its employees' privileged emails.

2. Surveillance or the Impression of Surveillance

Another online privacy consideration is that it is an unfair labor practice under Section 8(a)(1) of the NLRA for an employer to engage in the surveillance of, or create an impression of surveillance of, union activity. For example, in Magna International, Inc. 7-CA-43093(1), 2001 NLRB LEXIS 124 (March, 9, 2001), an administrative law judge held that it was a violation of Section 8(a)(1) of the NLRA for a supervisor to tell an employee that he liked a picture of her the day after the photo was posted to a union blog, because this suggested to the employee that her union activities were being monitored. In reviewing online data about applicants and employees, both unionized and nonunionized employers should take care to not inappropriately surveil or create the impression of surveillance of union activities.

E. Federal Laws Applicable to Electronic Communications and Data

In addition to the above privacy laws, there are also two federal electronic communication laws that might be implicated by an employer's search of social media sites or other online data : (1) the Electronic Communications Privacy Act; and (2) the Stored Communications Act. These laws are briefly summarized below.

1. The Electronic Communications Privacy Act ("ECPA" or "the Wiretap Act"), 18 U.S.C. § 2510 et seq.

The federal Wiretap Act prohibits the unlawful "interception" of an electronic communication contemporaneously with the communication being made. As such, employers that monitor and intercept employees' online communications through social media or other online sources could, depending on the circumstances, be liable under the Act. Most employers do not, however, monitor employee communications in real time as they are occurring. When there is no real-time, contemporaneous "interception" of an electronic communication, the Wiretap Act should not be implicated.

2. *Stored Communications Act (“SCA”), 18 U.S.C. § 2701 et seq.*

The SCA prohibits knowing or intentional unauthorized access to “a facility through which an electronic communication service is provided.” 18 U.S.C. § 2701, 2707. This includes unauthorized access to a password-protected email account or social-networking site. Key exceptions exist, however if the person accessing the communication is the provider of the service, a user of the service, and the communication is from or intended for that user, or has been granted access to the site by an authorized user. 18 U.S.C. § 2701(c)(2).

Three notable cases have applied the SCA to electronic communications and social media. In Konop v. Hawaiian Airlines, Inc., 302 F.3d 868 (9th Cir. 2002), the Ninth Circuit Court of Appeals held that there were fact questions warranting a trial on the question of whether an employer’s secret monitoring of a password-protected Website could be a violation of the SCA. In Konop, the employer gained access to the site by submitting an eligible employee’s name and creating a password to enter, after accepting terms and conditions that prohibited viewing by management.

In the Pietrylo case noted above, the District Court of New Jersey upheld a jury verdict imposing liability under the SCA. Again, in that case, the Court found sufficient evidence that a company supervisor accessed the password-protected employee chat room with a password provided by an employee coerced into providing access.

Finally, in the Quon case noted above, the Supreme Court overturned the ruling of the Ninth Circuit Court of Appeals that the SCA did not allow an employer to view the content of text messages sent by employees through third-party pager services, holding that although the employee had a privacy interest in the texts, the search in this instance did not violate the Fourth Amendment because it was for a legitimate work purpose and reasonable in scope.

F. Other Tort Liability for Employers

As briefly summarized below, if not handled carefully, information an employer might obtain online or an employer’s own use of online information may lead to tort liability for an employer.

1. *Negligent Retention and Supervision*

As in the hiring context, employers can be held responsible for the actions of employees who are known to be a danger to others. An employer may be liable under the doctrine of negligent retention when an employer becomes aware, or should have become aware, that an employee poses a threat and fails to take remedial action to ensure the safety of others. Under the doctrine of negligent supervision, on the other hand, employers have a duty to control employees and prevent them from intentionally or negligently inflicting personal injury in the scope of their employment. The torts of negligent retention and

supervision both require a threat of physical injury or harm (as opposed to economic harm) to be actionable.

Because social media is still too new and the law is still sufficiently unsettled, it is likely not yet the standard of care for employers to regularly monitor employees' social media postings for signs of danger. Should an employer learn, however, of online data that could suggest a safety risk, the employer may be obligated, due to negligent retention and supervision laws, to investigate and take appropriate action to address and try to limit any safety risks.

2. *Defamation*

As with other more traditional forms of communications, employers may face liability under defamation law if an employee defames another employee, customer, or others in social media, blog, or other online posts. In addition, employers may face liability if they defame their own employees through social media or publicize defamatory information about an individual that they have obtained online. The plaintiff in a defamation action must usually prove: (1) a defamatory statement, (2) published to third parties, and (3) which the speaker or publisher knew or should have known was false. To avoid defamation claims, employers should take care in how they communicate about employees, in how they handle online data, and should consider policies and training designed to prevent their employees from engaging in defamation.

3. *Special Problems with References and Recommendations*

One social media site, LinkedIn, allows employees to ask their "connections" to provide recommendations for them. Most employers, however, due to defamation, privacy and other legal considerations, typically provide very limited reference information on former employees. Employers may want to make sure that employees are aware that any limited reference policies an employer may have in place extend to provide references on social media sites, such as LinkedIn.

G. Employee Endorsements and Testimonials

While there is currently little legal authority that has been specifically enacted with respect to social media and other online data, the Federal Trade Commission ("FTC") has taken the position that false advertising legal requirements apply to online postings by a company's employees. Federal and state laws generally prohibit companies from engaging in false and misleading advertising. Until recently, it was not clear that these laws applied to social media. The FTC has, however, published a recent "Guides Concerning the Use of Endorsements and Testimonials in Advertising" that provides that: (1) both endorsers and advertisers are subject to liability for false or unsubstantiated statements made in endorsements; and (2) advertisers are subject to liability for failing to disclose material connections between themselves and endorsers. The Guides also provide illustrative examples of how the FTC Act would apply to endorsements and

testimonials made through social media, including both paid advertisements and provision of product samples for review.

Employers may, therefore, find themselves liable if employees offer endorsements or testimonials of the company's products or services online without disclosing their connection to the company. This potential liability has led some to argue that employers should engage in at least minimal monitoring of employees' use of social media. It may also be wise to adopt a social media and online posting policy for employees that makes clear the appropriate and inappropriate uses of social media and advises employees of the need to comply with FTC guidelines.

Given the wide array of legal issues that may arise in connection with social media and other online data, there are a host of practical considerations and steps employers should consider taking to try to minimize legal risks when doing online screening of applicants or dealing with online communications of current employees.

III. PRACTICAL STRATEGIES FOR ADDRESSING USE AND MISUSE OF SOCIAL MEDIA AT AND ABOUT WORK

Employee use of social media can result in external business generation and internal creation of a collegial atmosphere through less formal interaction and shared experiences between co-workers. On the other hand, employee use of social media can create awkward and potentially harassing situations when such use turns inappropriate.

For example, when a supervisor wants to be a subordinate's friend on a social networking site, it can create awkwardness between the supervisor and subordinate. If the subordinate accepts the invitation, the supervisor can access the subordinate's potentially inappropriate or revealing nonpublic profile. If the subordinate does not accept the invitation, he or she may be concerned that his or her employment opportunities may suffer or that the supervisor will be offended. In more extreme cases, misuse of such sites can give rise to claims of co-worker or supervisor sexual harassment or hostile work environment.

The most obvious hazard regarding the use of social media during employment is internal to the organization: Employees may spend so much time using social media during working hours that productivity decreases. Further, there is a significant risk of external employee misuse: Employees can easily make unauthorized disclosures of confidential company information, such as trade secrets, proprietary information and personnel matters. Employees may disparage the company or its customers in ways that lead to public relations problems or damage to the employer's brand or image.

To address these risks, employers must first consider the proper level of encouragement of social media use in the workplace. For some industries or positions, the use of social media might be appropriate for business development. For others, an outright ban may be appropriate because the workforce has no business reason to use social media at work or

while using the company networks, facilities or equipment. There are several best practices considerations that an employer can address in order to address social media in the workplace:

- Make employees aware that they are subject to the same privacy laws as employers;
- Place employees on notice regarding appropriate use of the internet’
- Ensure that employees understand that posting equals world-wide publication;
- Make employees aware of the privacy rights of others;
- Be proactive;
- Adopt a clear policy;
- Train employees on the proper use of the internet;
- Consider a total ban on the internet during working hours;
- Place employees on notice regarding potential monitoring;
- Be consistent in disciplining for violations;
- Understand the risk inherent in using the internet, and develop policies to manage potential pitfalls.

IV. ELEMENTS OF A SOCIAL MEDIA POLICY

With the increasing pervasiveness of social media, we recommend that companies consider carefully the business, legal, and HR issues raised and take steps to maximize business opportunities while minimizing potential risks.

As an important first step, employers should develop a social media policy, coordinating it with any existing policies on email, internet and electronic media usage, and codes of business conduct. The policies should include language reserving the company’s right to monitor employee use while at work or using company electronic devices, and while off-duty using the employee’s personal electronic devices where the employer’s business interests are implicated. At a minimum, employers must insert broad language encompassing social media into existing information technology, code of conduct, harassment and confidentiality policies. Employers should consider adding the following features, if appropriate, to such policies:

- A clear statement that misuse of social media can be grounds for discipline, up to and including termination.

- A prohibition on disclosure of the employer's confidential, trade secret or proprietary information.
- An instruction that employees keep company logos or trademarks off their blogs and profiles and not mention the company in commentary, unless for business purposes.
- An instruction that employees not post or blog during business hours, unless for business purposes.
- An instruction that employees bring work-related complaints to human resources before blogging or posting about such complaints.
- A prohibition on using company email addresses to register for social media sites.
- A prohibition on posting false information about the company or its employees, customers or affiliates.
- A general instruction that employees use good judgment and take personal and professional responsibility for what they publish online.
- A demand that all employees with personal blogs that identify their employer include a disclaimer that the views expressed on the blog are those of the individual and not the employer.
- Policy regarding “friending” of bosses, managers, subordinates and clients, whether of the same or opposite sex.
- Specify uses of social media that violate company policy because they may create business problems or legal liability for the company.
- Eliminate employee expectation of privacy when using company-owned technology.
- Provide notice that monitoring will occur.
- Consider informing employees and potential employees that you intend to monitor the internet
- Obtain releases for such searches.
- Make employees aware that information posted to blogs should not harass or attack an employee, contractor, customer, or vendor based upon protected status.

- All company policies apply to on-line use: handbook, confidentiality of sensitive company data, privacy of personal information, discrimination and harassment, copyright
- Provide procedures for reporting violations of policy and designate specific individuals in the company who can be contacted regarding questions. It is best to have at least two people listed as contacts in case an employee is not comfortable speaking with the only individual designated.

All supervisors and human resources professionals must be trained in the appropriate use of social media and how to consistently enforce the employer's social media policies. Any policy addressing social media during employment must use broad language and be updated frequently, because social media will change quickly over time. Employers should also consider incorporating language specifically referencing social media into the confidentiality provisions of separation agreements.

V. MAKING HIRING DECISIONS BASED ON INFORMATION FROM SOCIAL MEDIA OUTLETS

Many employers and job recruiters check out potential employees on the internet, using sites such as Google, Yahoo, or Peoplefinder.com. There are hiring issues associated with using the Web, such as whether this kind of background check is lawful or whether a potential applicant is being discounted for participating in activity that is lawful but disapproved by the employer. In addition, an employer could be making a decision based on inaccurate information. A potential employer could also learn information about a candidate's protected status, workers' compensation claim, or bankruptcy.

Employers should consider whether the benefits of using social media to screen applicants outweigh the risks. If an employer wants to supplement traditional hiring practices with a social media search, the employer should consider the following approaches.

- Employers should screen applicants in a uniform manner by creating a list of the social media they will search for each applicant and the lawful information desired from the social media search about each applicant. If all applicants cannot be screened using the lawful criteria because an employer does not have the time, resources or inclination to do so, employers must be consistent, objective, and nondiscriminatory in selecting subsets of applicants to screen.
- Employers should have a neutral party, such as an employee in a nondecision-making role, conduct the social media search, filtering out any protected class information about the applicant and reporting only information that may lawfully be considered in making the hiring decision.

- Employers' representatives should not "friend" applicants in order to gain access to their nonpublic social-networking profiles.
- Employers must be able to point to a legitimate, nondiscriminatory reason for the hiring decision, with documentation to support the decision.
- Employers who are considering making an employment decision based on information found in social media should consult with counsel prior to doing so.

Even post-employment, social media issues creep into the relationship between the employer and the former employee. Supervisors and co-workers are increasingly asked to "recommend" former employees on LinkedIn after separation from employment. This "recommend" feature allows people in a professional network to write positive professional reviews about other people in their network, which will be visible on the former employee's LinkedIn page.

A positive recommendation on a person's LinkedIn page is the same as an employment reference and should uniformly be treated as such under the employer's post-employment reference policy. Employers could also consider adding to their post-employment reference policy a prohibition on managers from "recommending" or commenting on the job performance of former employees via social media without prior specific authorization from the human resources department.

The takeaway message regarding social media in the workplace is that employers can no longer ignore the risks. Employers must be cautious in addressing these emerging workplace issues, even though employment-related litigation involving social media is in its infancy. First, employers must understand the myriad of issues surrounding social media in the workplace in order to strike the appropriate balance in the eyes of their employees and the law. Then, employers must craft appropriate policies and procedures regarding social media that are consistent with their industry and firm culture, and apply such policies in a consistent, objective, and nondiscriminatory way.

VI. DRUG AND ALCOHOL TESTING

A. The Americans with Disabilities Act

The Americans with Disabilities Act ("ADA") places some specific restrictions on an employer's pre-employment inquiries. The ADA breaks the hiring process into two phases: the pre-offer stage and the post-conditional-offer stage. At the pre-offer stage, disability-related questions and medical examinations are prohibited. In fact, an employer is precluded from asking any questions that are likely to elicit information about a disability. The purpose of these prohibitions is to prevent discrimination against individuals with hidden disabilities. However, such questions and medical examinations

are permitted after extending a job offer but before the individual begins work (i.e., the post-offer period).

Under the ADA, an employer may not ask about the existence, nature, or severity of a disability and may not conduct medical examinations until after a conditional job offer is made to the applicant. Drug testing is not a "medical examination" under the law, and therefore pre-employment screening tests for illegal drug use are permitted under the ADA. The prohibition against medical history questions and physical examinations ensures that an applicant's hidden disability is not considered prior to the assessment of an applicant's non-medical qualifications. At the pre-offer stage, an employer may only ask about an applicant's ability to perform specific job-related functions and other non-disability-related questions. In addition, all applicants can be required to demonstrate that they have the physical agility to perform the job. Individuals with obvious disabilities can be asked to demonstrate or describe how they would perform job functions.

The following are some examples of questions an employer may **not** ask during the pre-offer period, either on an application or during an interview:

- Do you have a heart condition? Do you have asthma or other difficulties breathing?
- Do you have a disability which would interfere with your ability to perform the job?
- How many days were you sick last year?
- Have you ever filed for workers' compensation? Have you ever been injured on the job?
- Have you ever been treated for mental health problems?
- What prescription drugs are you currently taking?

An employer may ask these questions, and others that are likely to reveal the existence of a disability, after it extends a job offer to an applicant as long as the employer asks the same questions of other applicants offered the same type of job. In other words, an employer cannot ask such questions only of those who have obvious disabilities. Similarly, an employer may require a medical examination after making a job offer as long as it requires the same medical examination of other applicants offered the same type of job.

Employers should be aware that a job offer cannot be rescinded simply because an employee or a medical examination reveals the existence of a disability during the post-offer period. An employer can withdraw the job offer only if it can be shown that the employee is unable to perform the essential functions of the job (with or without

reasonable accommodation), or that the employee poses a significant risk of causing substantial harm to himself/herself or others.

Employers should develop thorough job descriptions that identify the essential elements of the jobs in their organizations and use these job descriptions during interviews to keep the discussion focused on job-related functions and the applicant's qualifications. By relying on the job description, both the interviewer and the applicant will be aware of what will be required of the applicant in the event he or she is offered the position. Employers should also review their application forms to ensure that medical histories or questions that may elicit information about a disability (i.e., "Have you ever suffered a worker's compensation injury?") are not requested.

Drug abuse in the workplace has become an increasingly difficult issue facing employers. Although neighboring states such as Connecticut, Maine, Vermont, and Rhode Island have enacted drug-testing laws, New Hampshire does not have a statute that specifically addresses the topic of drug testing. In the absence of a drug-testing statute, New Hampshire employers can test an employee for drug use and refuse to hire or can fire an employee who tests positive or refuses to be tested. However, employers must approach drug testing with great care because of the risks of legal challenge under other laws, including invasion of privacy claims.

As there is no drug-testing statute in New Hampshire, there is no statutory prohibition against drug testing of employees. However, there is also no statute to provide guidance to employers who wish to test employees. The primary reason for an employer to utilize drug testing is to prevent employees from endangering the safety of themselves or others or posing a threat to property.

Employers should conduct the drug testing during or close to an employee's work time. Employers should test only for drug use that might have an impact on work performance. Employers should provide notice to employees of the drug-testing program or policy to give employees the opportunity to decide whether to contest the program, quit, or refuse to accept the job or undertake measures to pass the tests.

Although prospective employees have a right to privacy, the United States Supreme Court has held that both blood and urine collection are minimally intrusive and not harmful to job applicants when conducted in the right environment (workplace or collection facility) without direct observation by the tester. In other words, it would be considered an invasion of the candidate's privacy if the employer required a urine sample while other people in the room were watching. However, if there is a worry about tampering with the sample, the employer may be allowed to have one person of the same sex as the candidate present when the sample is given. Caution is advised in these circumstances.

Employers should be careful to administer drug testing in a non-discriminatory manner. Discrimination can be implied if an employer tests only certain applicants for a position.

An employer cannot pick and choose which applicants for the same position will be tested.

If an employer tries to administer a drug test to an applicant in an underhand manner without the applicant's knowledge or consent, legal issues can be raised. For example, an employer is not allowed to pick up strands of hair that a potential employee has left on a chair during the interview and use them as a sample for a drug test.

VII. REFERENCE AND BACKGROUND CHECKS

1. Reference Checks

During the application and interview process, an employer should obtain information from several references who are willing to discuss the applicant's prior work history. The purpose of conducting a reference check is to gather additional information. However, questions that are unlawful to ask during an interview are likewise unlawful to ask during a reference check. Employers should ask specific questions which focus on the applicant's prior work experience. Employers should be cautioned that legal sanctions in the form of negligent hiring or negligent retention suits may be successful if no effort is made to check past references.

Where former employers are reluctant to discuss an applicant's work history for fear of defamation lawsuits or the like, one solution is to obtain a "reference authorization, waiver, and hold harmless agreement" from the applicant. This waiver authorizes the disclosure of past employment information and releases both prospective and past employers from all claims and liabilities arising from the release of such information. Without this waiver form, some employers will divulge only limited information, generally covering the date of hire, job title, and date of separation.

2. Fair Credit Reporting Act, 15 U.S.C. §1681, et seq.

The Fair Credit Reporting Act ("FCRA") governs credit and certain other background investigations on applicants and employees when the information is obtained through a third party without direct firsthand knowledge of the information. Examples include requesting a criminal background check through a background check company rather than directly from the state police, obtaining a driver's license record check through an auto insurance company rather than directly through the DMV, etc. Before requesting a consumer report, or an investigative consumer report, an employer must: (1) provide the applicant or employee with a clear and conspicuous written disclosure that informs the individual that a report may be requested; and (2) obtain written consent from the applicant or employee authorizing the employer to procure such a report. If an investigative consumer report is requested, the employer must also disclose: (1) that such a report, including information relative to the individual's character, general reputation and personal characteristics and mode of living, may be made and such disclosure is made in a writing mailed, or otherwise delivered to the individual not later than three days after the date on which the report was first requested; (2) inform the applicant that

he or she has the right to request a complete and accurate disclosure of the nature and scope of the investigation; and (3) the disclosure must state that the applicant, upon written request, may obtain a summary of rights under FCRA as prescribed by the Federal Trade Commission.

The employer must provide certification to the consumer reporting agency before requesting a report on an applicant. If the employer decides to take adverse action based in whole or part on the report, then the employer must provide the applicant with a copy of the report and a summary of rights under the FCRA as prescribed by the Federal Trade Commission. The employer may not take adverse action until these documents have been provided to the applicant. After taking adverse action, the employer must: (1) provide notice of the adverse action to the individual; (2) provide the name, address and telephone number of the consumer reporting agency and a statement that the agency did not decide to take adverse action and is unable to provide specific reasons why the adverse action was taken; and (3) provide notice of the applicant's right to obtain a free copy of the credit report and to dispute the accuracy or completeness of any information in a consumer report furnished by the agency.

The definition of "consumer report" excludes communications made by a third party to an employer in connection with an investigation of suspected misconduct relating to employment or compliance with applicable laws, regulations or written employment policies. Employers, after taking an adverse action against an employee based on a report by a third-party investigator, are required to disclose to the employee a summary of the report. Employers do not have to disclose the sources of information for the report.

FCRA contains prohibitions on the reporting of medical information by consumer reporting agencies to an employer unless the employee or prospective employee provides prior consent. Medical information contained in a consumer report furnished to an employer must be relevant to the employment, and the employee or prospective employee must sign a written consent form that describes in clear and conspicuous language the use for which the information will be furnished.

New Hampshire has enacted a Right to Privacy Act, codified in RSA 359-C. The purpose of the Act is to protect the confidential relationship between financial institutions and creditors and their respective customers. RSA 359-C:2. The Act provides that no state or local government official, agency or department may obtain financial or credit records or information from financial institutions or creditors regarding specific customers except under limited circumstances and by limited methods. N.H. RSA 359-C:4.

New Hampshire's Fair Credit Reporting Act, RSA 359-B, is an almost verbatim enactment of the federal Fair Credit Reporting Act (FCRA). 15 U.S.C. § 1681 et. seq. The purpose is to limit dissemination of information in consumers' credit files to those with a direct and immediate need for that information, and to insure its currency as well as its accuracy. State v. Credit Bureau of Nashua, Inc., 115 N.H. 455, 342 A.2d 640 (1975).

3. *Criminal Background Investigations*

New Hampshire employers may inquire into convictions that have not been annulled by a court, such as, "Have you ever been arrested for or convicted of a crime that has not been annulled by a court?" See RSA 651:5, X(c).

New Hampshire law mandates that employers conduct criminal records checks for certain positions. These positions include positions that require direct contact with children, positions with residential care facilities, positions with home health care providers, and positions with entities authorized by the New Hampshire Department of Health and Human Services to offer personal care services.

4. *Motor Vehicle Background Investigations*

An employer may obtain the motor vehicle records of an employee or prospective employee if such person grants permission to the employer.

VIII. ADDITIONAL PRIVACY ISSUES

1. New Hampshire recognizes an individual's right to privacy. RSA 644:9 states:

I. A person is guilty of a misdemeanor if such person unlawfully and without the consent of the persons entitled to privacy therein, installs or uses:

(a) In any private place, any device for observing, photographing, recording, amplifying or broadcasting sounds or events in such place; or

(b) Outside a private place, any device for hearing, recording, amplifying or broadcasting sounds originating in such place which would not ordinarily be audible or comprehensible outside.

II. As used in this section, "private place" means a place where one may reasonably expect to be safe from surveillance but does not include a place to which the public or a substantial group thereof has access.

A violation triggers a misdemeanor penalty.

2. The New Hampshire Supreme Court in Hamberger v. Eastman, 106 N.H. 107, 112 (1964) identified four interests protected under the right to privacy:

- (1) Protection from intrusion upon one's physical and mental solitude or seclusion;
- (2) Protection from public disclosure of private facts;
- (3) Protection from publicity which places one in a false light in the public eye;
- (4) Protection from appropriation of one's name or likeness for the benefit or advantage of another.

a. Surveillance

New Hampshire RSA 644:9 protects individuals from certain invasions of privacy. Under the statute, a person is guilty of a misdemeanor if he or she installs certain devices for observing, photographing, recording, amplifying, or broadcasting sounds or events.

New Hampshire RSA 644:11 is a criminal defamation statute which imposes a misdemeanor penalty for the oral or written communication of false information.

New Hampshire RSA 570-A codifies New Hampshire's wiretapping and eavesdropping law which prohibits, except in very limited circumstances, interception of any wire or oral communication without the consent of all parties to the communication.

(i) Video Monitoring

The First Circuit in Vega-Rodriguez v. Puerto Rico Tel. Co., 110 F.3d 174 (1st Cir. 1997) has held that a public employer did not invade an employee's privacy, and the monitoring was a legitimate goal of an employer when the monitoring was knowingly performed, revealed and disclosed to the employees.