Bloomberg Law Reports® Labor & Employment

Technological Advances Change the Game for Employers

Christine Watts Johnston, Mark D. Pomfret and Henry T. Goldman
K&L Gates LLP

There is no question that advances in technology have made life easier for most businesses. The ease of access to data and availability of new technologies to open previously untapped sources of information, however, are creating new questions for employers. For example: Should employers use newly available internet and social networking resources to evaluate applicants and employees? What are the legal implications of using internet sites to gather employment-related information? Must employers use internet and social networking sites as part of their applicant review? What can employers do to protect their electronic information and systems without running afoul of employee privacy rights? Finally, what can employers do to protect or recover electronic information from departing employees? As new issues and concerns continue to arise and the law evolves in this area, employers are well advised to evaluate and assess their practices and policies with respect to the internet and online resources in all aspects of the employment relationship.

What Are Legal Concerns For Employers Who Use Internet and Social Networking Resources to Evaluate Applicants and Employees?

While there is no clear answer to the question of whether employers "should" evaluate their employees or potential employees with the plethora of potential information from online resources, employers who do so should proceed with care, particularly if they choose to access such information without an employee's or applicant's specific authorization. Internet and social networking sites provide employers with an entirely new level of insight into applicants and employees. However, with such access employees may face unknown or unintended consequences.

Do Not Violate Terms of Use

Employers need to be cognizant of a website's "terms of use" before using information garnered from such sites for the purpose of making employment decisions. As an initial matter, the "terms of use" of some websites explicitly prohibit the use of information found on the site for the purpose of making employment-related decisions. Accordingly, employers may be liable for breach of contract or other claims if they accept the terms of use of a particular website without carefully reviewing the restrictions created by those terms and unwittingly violate the terms. Moreover, by simply accepting the "terms of use" of a website an employer may inadvertently agree to be sued in a particular jurisdiction, which may not be as favorable for the employer.

Do Not Access Private Information

Employers also must be sure not to violate an individual's reasonable expectation of privacy. In some circumstances, the "terms of use" of a particular website might make clear that any information posted is not confidential, eliminating any question of whether a legitimate expectation of privacy could exist. Although there is significant case law holding that information that is publicly posted on the internet is not private, employers must not intrude into private or password protected sites. An employee's use of access restrictions or passwords could create a reasonable expectation that the information posted is private.

Confirm the Accuracy of Online Information and Share on a Need-to-Know Basis

If an employer does obtain information about an applicant or an employee through social networking sites, blogs or other online resources, it should be careful about reliance on and transfer of that information. Often employers may learn something about an applicant, or rely on information, without confirming the truth or accuracy of the information. An employer who shares information beyond those with a legitimate business need to know it may lose any conditional privilege it enjoys as an employer and face a defamation claim related to the spreading of false information. Given the prevalence of online identity theft and the possibility of mistaken identity, employers face a significant risk of relying on information that could either be the product of intentionally malicious false posting or simple mistaken identity.

Do Not Use Information that Would Violate Discrimination / Retaliation Laws

While some of the available online information may relate to an applicant or employee's qualifications or job skills, much of the information in cyberspace relates to those individuals' lives outside of work. For instance, employers who perform online inquiries into their employees or applicants may inadvertently access information concerning an individual's membership in a protected category or protected activity. In light of this possibility, employers must consider the potential of creating viable discrimination and/or retaliation claims. A number of different employment laws including the National Labor Relations Act (NLRA), the ADA and state Workers' Compensation Act, the Fair Labor Standards Act (FLSA), Title VII of the Civil Rights Act and the Age Discrimination in Employment Act (ADEA) all preclude employers from basing decisions on the exercise of statutory rights or the filing of claims under those statutes. Moreover, employers should consider the risk of uncovering information related to an applicant's military service or genetic characteristics. Obtaining knowledge of these data points, if an employer opts not to hire an otherwise qualified candidate, could likewise lead to a claim under the Uniform Services Employment and Reemployment Rights Act (USERRA) or under the Genetic Information Non-Discrimination Act (GINA).

Employers also must remain mindful of state laws prohibiting discrimination on the basis of lawful activities conducted outside of the workplace. Employers have faced claims of discrimination and retaliation based upon decisions made related to an applicant or employee's conduct such as smoking, drinking, supporting a particular

political candidate, or even working as a dancer in a topless bar. For example, an employer in New York could even face a claim if it takes adverse employment action against an employee as a result of the employee's blogging activity. New York law prohibits adverse action against employees for off-duty political activities, union activities, legal use of consumable products, and recreational activities." New York Labor § 201-d. Since "recreational activities" is defined to include "hobbies," an employee terminated as a result of his or her outside of work blogging or social-networking activity might have a claim under New York law. Similarly, an employer who learns through a Facebook profile or other electronic search that an employee is "in a relationship" with or dating someone and takes adverse action on that basis might also face a claim under New York law, since recreational activities also has been interpreted, at least by some courts, to include dating.

Must Employers Use Internet and Social Network Searches as Part of Applicant Review Processes and How Should They Do It?

Consider Potential Negligent Hiring Claims

Even before employees and potential new hires engaged in prolific use of internet and social networking sites, employers often faced the risks of negligent hiring claims. Such claims arise where an employer has an obligation to make an appropriate investigation, such an investigation would have revealed the unsuitability of a candidate for a particular duty to be performed, and it was unreasonable for the employer to hire the candidate in light of information known or that should have been known. While there have not yet been published cases assigning liability as a result of a failure to do an internet or social networking search in particular, performing such searches, particularly for certain types of jobs, may provide employers with a low cost insurance against such claims.

Develop Consistent Policies and Procedures and Provide Training

Employers who do opt to search online should develop formal procedures to ensure that such searches are being performed consistently and uniformly. These procedures should include, among other things, reporting only job-related information, complying with relevant terms of use, and taking steps to check the accuracy of online information. Likewise, employers should consider providing training to those within their organizations who may be using online searching resources and making employment decisions to ensure that such employees are aware of the risks and properly documenting their activities and bases for employment decisions.

Update Background Check Forms and Applications

Employers should consider whether their online checking activities violate federal and/or state background checking laws. The Fair Credit Reporting Act (FCRA) requires that an applicant or employee provide written consent prior to an employer conducting a "consumer report" or background check on an employee through a third party "consumer reporting agency." Because "consumer reporting agency" has been

broadly interpreted, some websites that fall within an employer's on-line search could implicate the FCRA. Moreover, employers have specific disclosure requirements depending upon how they use information obtained through such reports. Employers may need to update their background check authorization and disclosure forms and their employment applications to reflect new electronic search practices.

What Information Can Employers Monitor and Review On Their Systems Without Violating Employee Privacy?

What is an Employee's "Reasonable" Expectation of Privacy in an Employer's Computer Systems?

Many employers have policies that define how employees are permitted to use their electronic resources and systems. The key to such policies and the determining factor in many cases concerning the employer and employee's respective rights to information contained on an employer's computer systems depend upon whether an employee has an objectively reasonable expectation of privacy. In order to assess the "reasonableness" of any asserted expectation of privacy, courts typically will consider whether (a) the employer has a policy banning personal or other objectionable use; (b) the employer monitors employee use of its systems; (c) third parties have a right of access to the computer or email; and (d) the employer notified the employee, or the employee knew of, the employer's use and monitoring policy. *In re: Asia Global Crossing, Ltd.*, 322 B.R. 247 (Bankr. S.D.N.Y. 2005).

Despite the existence of a well-drafted policy that clearly dispels any expectation of privacy, an employer's practices may, nonetheless, create an expectation of privacy for employees. In *City of Ontario v. Quon*, the United States Supreme Court is expected to answer the question of whether a police department with a "no-privacy" policy could create a reasonable expectation of privacy with respect to employees' use of the department's hand-held devices. At issue is the fact that, despite the department's official no-privacy policy, a police lieutenant gave permission to police officers to use their devices for personal text messages. When the department discovered that officers were using the devices to send sexually explicit text messages, or for so-called "sexting," the officers were terminated. Relying on the apparent expectation of privacy created by the lieutenant, the officers sued. The Supreme Court's impending decision could provide important insight that may be applicable to private sector privacy claims.

Are Employee Blogs or Attorney Communications "Private"?

Similar questions of privacy arise when employees use their work computers to conduct their personal business or express themselves through blogs. Employer policies should address blogging activity, both in terms of defining permitted activity as well as addressing concerns ranging from the disclosure of confidential or proprietary information belonging to the employer, compliance with anti-harassment and other workplace policies, to explicitly or implicitly suggesting that their personal views are attributable to the employer.

Likewise, questions of privacy with respect to email arise frequently when a current or former employee has contacted his or her attorney through the employer's electronic communication systems and such communications become integral to a claim by one party against the other. In such cases, where the sanctity of attorney-client communications is balanced against the expectation of privacy, courts' determinations vary depending upon the circumstances and application of factors like those set forth in the *In re: Asia Global* case. An example of the importance of these factors is found in *Nat'l Econ. Research Assoc. v. Evans*, No. 04-2618-BLS2, 2006 BL 104766 (Mass. Super. Ct. Aug. 3, 2006). In that case, a Massachusetts court evaluated whether emails sent by an employee to his lawyer through his personal password-protected "Yahoo" account but on his employer-owned laptop computer could remain privileged. In its decision, the court upheld the attorney-client privilege, but noted that the language of the employer's policy did not explicitly state that the employer could review personal emails sent through internet accounts on company computers. Accordingly, the language and specificity of an employer's policy is imperative to establishing a clear understanding of an employer's rights.

What Can An Employer Do to Protect or Recover Electronic Information From a Departing Employee?

Employers Are Proactively Protecting Against Theft of Confidential Information

Employers continue to encounter rogue employees who use their systems without authorization or who exceed authorized access, including by attempting to steal confidential or proprietary information at the time of their departure. In the information age, employers are taking more aggressive steps, in terms of both prevention and reaction, to address the heightened risks associated with information transfer. For example, some employers are implementing tighter security protocols, limiting access to confidential information on their systems, and actively monitoring system usage. Employers also have increased their efforts to protect against theft by disabling mechanisms that allow for unauthorized downloading, investigating potential violations (including with the assistance of computer forensic experts), and pursuing claims against employees for equitable relief and damages.

Data Privacy Laws Raise the Stakes

These information transfer problems have new implications in light of increasingly stringent laws regulating data privacy. Most states now have laws in place that require businesses, including employers, who maintain "personal information" (which typically includes the first and last name of a resident in combination with a social security number, drivers license or financial account information) belonging to residents of the state, to take certain measures to ensure data privacy and protect against identity theft. For example, as of March 1, 2010, employers in Massachusetts will be required to comply with regulations that require that businesses establish a written security program, encrypt data on devices if feasible, and monitor to identify instances of unauthorized access or use of personal information.

Employers Should Consider Computer Fraud and Abuse Act Claims

Employees who steal information from their employers, including "personal information," now may face claims based on additional theories beyond traditional common law and statutory claims based on contract, trade secret laws, and unfair competition laws. Employers are asserting claims against employees under such statutes as the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030 et. seq. The CFAA has evolved from an exclusively criminal statute designed to address computer hacking activity into a device for employers to recover damages and equitable relief through a private right of action.

The rapidly developing case law interpreting the statutory terms within the CFAA will continue to impact the availability and breadth of these claims to employers, albeit in different ways. Currently, there is a split among the Federal Courts of Appeals regarding the question of what it means for an employee or former employee to access an employer's protected computer "without authorization." In *Int'l Airport Centers, LLC v. Citrin*, 440 F.3d 418 (7th Cir. 2006), the Court held that a former employee who had wiped his laptop clean and erased data from the protected computer prior to his departure to form a competing business was acting "without authorization." The Court reasoned that, when the employee violated his duty of loyalty to his employer his authority to access the laptop terminated. On the other hand, another Court recently interpreted the term "without authorization" much more narrowly in *LVRC Holdings, LLC v. Brekka*, 581 F.3d 1127 (9th Cir. 2009). In that case, the Court held that a person uses a computer "without authorization" only when the person either has not received permission to use the computer (such as a hacker) or when the employee uses the computer after the employer has explicitly rescinded access permission. Regardless of these opposing viewpoints, employers should be sure that their policies and practices appropriately restrict access and that they possess the legal and forensic tools that may assist with their recovery of misappropriated information or data.

Conclusion

Employers cannot avoid reevaluating their practices and policies to address new issues in the workplace that arise as a result of the prevalence of the internet and online resources in and out of the workplace. In each stage of the employment relationship—from hiring to firing—employees' online activities are impacting an employer's rights and responsibilities.

Mark D. Pomfret is a partner at K&L Gates in the firm's Boston office. He represents local, regional and national employers in all areas of employment and labor law. He has significant experience before federal and state courts in employment related litigation defending against discrimination, sexual harassment, wrongful termination, privacy, civil rights, whistleblower, contract, and tort-based claims, as well as enforcing noncompetition and other restrictive covenant obligations. Mr. Pomfret also has successfully handled numerous administrative proceedings and investigations on behalf of clients before various federal and state agencies, including the U.S. Equal Employment Opportunity Commission, the U.S. Department of Labor, and the National Labor Relations Board.

Henry T. Goldman is of Counsel to K&L Gates LLP in the firm's Boston office. He represents employers in employment and labor law matters, including planning, counseling and litigation. His employment work encompasses negotiating and drafting employment and severance agreements; negotiating and advising on change in control agreements; design of non-competition, confidentiality, and non-disclosure agreements; adherence to legal requirements in the use of temporary employees and independent contractors; reductions in force; plant closings; employee relations, discipline, and discharge issues; Sarbanes-Oxley compliance and investigations; sexual harassment; wage and hour issues; compliance with myriad employment-related laws; and handling employment issues in mergers and acquisitions.

Christine Watts Johnston is an associate in the Boston office of K&L Gates LLP. She concentrates her practice in the employment and labor area where she represents employers in all aspects of labor and employment law. Ms. Johnston frequently represents management in employment disputes in state and federal courts, at the Equal Employment Opportunity Commission, the Massachusetts Commission Against Discrimination and before other federal and state agencies. Ms. Johnston has significant experience representing employers in contract disputes, noncompetition and misappropriation of trade secret cases, discrimination, harassment and retaliation cases and tort-based claims.