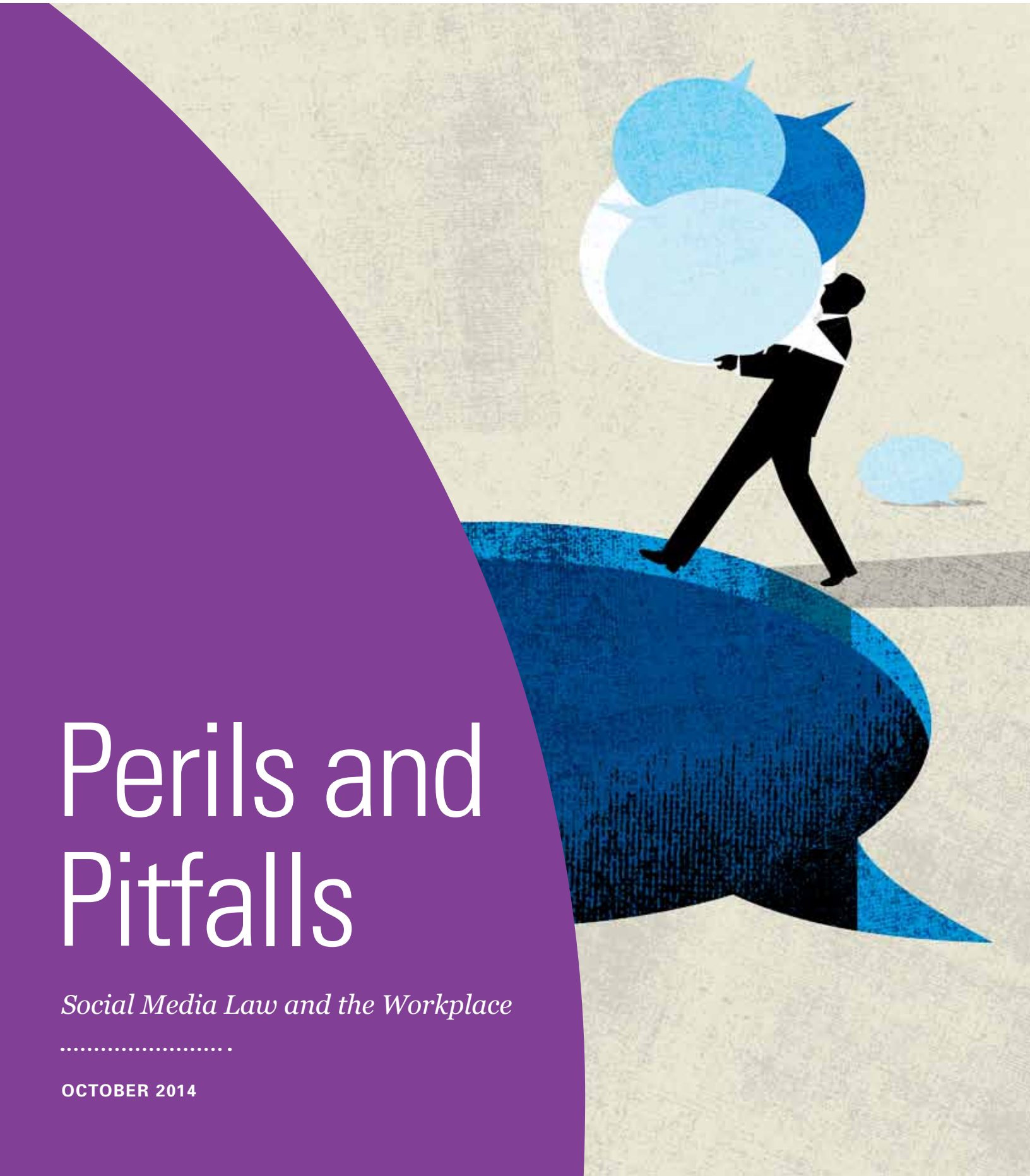
U.S. CHAMBER
Institute for Legal Reform



Perils and Pitfalls

Social Media Law and the Workplace

OCTOBER 2014

U.S. CHAMBER
Institute for Legal Reform

An Affiliate of the U.S. Chamber of Commerce

Table of Contents

Prepared for the U.S. Chamber Institute for Legal Reform by

Sara A. Begley, Joel S. Barras, Divonne Smoyer, and Amanda D. Haverstick
Reed Smith LLP

Introduction

The meteoric rise in workplace social media use has far outpaced the ability of federal legislators to produce laws to govern it. The result is a precarious absence of consistent legal standards to guide U.S. businesses.

Social media has radically transformed the way companies do business—so much so that what was once referred to as "using social media for business purposes" is now, simply, "social business." Among the redesigned business processes encompassed by this newly-coined concept are those involving company brand promotion, marketing of products and services, and communicating with customers, consumers, suppliers, and shareholders, among others. Branded social media pages on third-party services such as Facebook and Twitter help companies establish a social media presence and gain followers, fans, consumers, and subscribers. Companies can then leverage their social media presence as a platform for promotions, contests, and other events that encourage consumers to submit substantive descriptions and favorable reviews of a company's products and services. Social media sites also allow for word-of-mouth marketing via blogs, tweets, and chat room comments, all of which can be far more powerful than company-sponsored direct marketing programs.

These efforts appear to make good business sense for companies. Recent studies indicate that 75% of business customers rely on social media to make purchasing decisions, and 81% of individual consumers are influenced by friends' posts on social media when choosing which products to buy—with 47% of U.S. consumers reporting that Facebook is their number one buying influence.[1] Given these statistics, it is not surprising that recent surveys further indicate that 70% or more of marketing professionals have used Facebook to gain new customers.[2] Social media marketing budgets are also predicted to double over the next five years.[3]

Accompanying the increase in social media-focused business processes has been a growing trend among companies to allow employees to use social media at work. Many have even hired "bloggers," "endorsers," or employees with similarly unconventional job titles to focus exclusively on social business, including addressing public relations issues and providing near instantaneous online customer service. This practice should reward businesses, as 71% of surveyed customers relay they are likely to recommend a brand to others if they

> *Gaping holes exist in the standards governing employers' rights and responsibilities with respect to employee social media use.*

receive a quick brand response through social media.[4]

With all of the advantageous offerings from social media—with only more expected to develop—it will be increasingly critical that U.S. companies capitalize on these offerings to remain competitive in the global business environment. Doing so, however, means that companies must be successful at navigating the many landmines social media plants for them in the workplace. As ubiquitous as social media now is in the world of businesses, it is equally—if not more so—in the private worlds of the individuals that these businesses employ. As the two worlds attempt to co-exist and move forward in the workplace setting, collision of competing employer-employee interests is inevitable. This makes social media a high legal risk area for employers.

Unfortunately, the current legal landscape in the U.S. does nothing to help mitigate this risk. Gaping holes exist in the standards governing employers' rights and responsibilities with respect to employee social media use. There is no federal statute, for example, that defines the scope of companies' entitlement to online access to employees' social media activity, even when that activity involves the company or otherwise impacts the workplace or lives of other company employees. Federal legislation in this area would generally restrict employers' access to employee social media activity and include well-defined exceptions, bringing greater certainty for employers. Currently, however, the void in federal statutory law is filled by a hodgepodge of social media statutes in many (but not all) states that set inconsistent standards for multi-state and national employers. Worse still, there has been a rapidly developing National Labor Relations Board (NLRB or Board) "law" composed of a series of individual case rulings that limit companies' rights vis-à-vis their employees with respect to social media in the workplace.

The need for social media legal reform could not be clearer. In this paper, we discuss why and how the increase in workplace social media use presents U.S. employers with considerable risks, both legal and commercial. We next address the current uncertain legal environment created by the inconsistency among state privacy statutes and the recent rash of *ad hoc* social media rulings by the NLRB. We conclude that the foregoing factors combine to make social media a high risk area for U.S. businesses that warrants the attention of federal lawmakers.

Social Media Exposes Employers To Significant Liability Risks

Among the many potential pitfalls associated with workplace social media use are claims brought under federal and state employment discrimination statutes.

This topic was the focal point of the March 12, 2014 Equal Employment Opportunity Commission (EEOC or Commission) meeting, where a "panel of experts" convened to provide the Commission with "information about the growing use of social media and how it impacts the laws the EEOC enforces."[5] The panel "explained … [that] [t]he use of social media has become pervasive in today's workplace and, as a result, is having an impact on the enforcement of federal laws."[6]

Two key issues addressed by panelists were: (1) hiring practices that may give rise to claims that employers based job candidate selections on protected characteristics learned through social media research; and (2) employee conduct on social media sites that may give rise to claims of discriminatory and hostile work environment.[7] Both issues expose U.S. businesses to considerable legal risks.

Hiring Discrimination Claims

Nowhere more than in the area of applicant screening are the pros and cons of social media so closely intertwined. One recent study reports that three-fourths of surveyed human resources and hiring executives use social media to vet job candidates, with an even greater share using it for recruiting.[8] But social media is a double-edged sword for employers in this area. On one hand, social media sources are a potential treasure trove of applicant information that can help employers win the war for talent while steering clear of applicants who commit resumé fraud or otherwise exaggerate their educational and work experiences. On the other hand, by researching applicants online, employers may unwittingly learn of applicants' protected characteristics, such as religion, national origin, or citizenship, and/or about their lawful off-duty conduct, such as firearm possession, tobacco use, or political activity (which are protected by various state employment laws). In many instances, employers would not know such information but for their social media research, and by doing so, they open themselves to claims that they relied on protected information when making their

hiring choices. As one legal publisher so aptly asked recently, "is the potential risk worth the potential reward?"[9]

This same dilemma was explained in a Press Release by the EEOC regarding its March 2014 meeting on workplace social media issues:

> The use of sites such as LinkedIn and Facebook can provide a valuable tool for identifying good candidates by searching for specific qualifications…[b]ut the improper use of information obtained from such sites may be discriminatory since most individuals' race, gender, general age and possibly ethnicity can be discerned from information on these sites.[10]

An EEOC representative at the meeting reported on two recent Commission "informal, procedural" rulings involving social media-related employment claims in the federal sector.[11] One involved a claim by a 61-year-old who alleged age discrimination based on the hiring employer's use of Facebook to recruit candidates to fill the position for which she had applied and been denied.[12] In addition to arguably advancing a disparate treatment theory of liability (a "fuzzy" proposition, in the words of the reporting EEOC representative[13]), the claimant also presented a novel theory of disparate impact liability:

> [T]hat by recruiting for the position in issue through social media, the employer discriminated on the basis of age because its social media recruiting focus "put older workers at a disadvantage," as "older people use computers less often and less fluently than younger people."[14]

An Administrative Law Judge (ALJ) had dismissed the claim for lack of evidence that the employer's use of social media to recruit for the position at issue actually had any age-based disparate impact.[15] On appeal, the EEOC approved the ALJ's decision based on its same reasons, adding that the claimant also had produced no evidence that the employer had recruited *exclusively* through social media.[16] (Although the EEOC does not elaborate on or explain the intent behind its use of the word "exclusively," it would appear to suggest that the EEOC's ultimate outcome in the matter might have been different if the employer *had* recruited exclusively through social media.)

As for court cases involving social media-based hiring discrimination claims, there are limited reported decisions.

- One federal district court in Kentucky that addressed such a claim, in *Gaskell v. Univ. of Kentucky*,[17] held that a hiring employer-defendant's knowledge of the candidate-plaintiff's protected trait (there, her strong conservative religious beliefs)—about which the employer had learned through online applicant screening—sufficed, when coupled with plaintiff's other supporting evidence, to preclude summary judgment dismissal of her discriminatory failure-to-hire claim.
- A federal district court in Illinois faced a similar claim, in *Nieman v. Grange Mutual Ins. Co.*,[18] where a 42-year-old unsuccessful job applicant claimed he had been disqualified for a position due to his age and in retaliation for suing his former employer—information about which, he alleged, the employer's hiring manager learned from his LinkedIn

> *"[T]he number of cases involving hiring discrimination will likely grow, as employers in present and future years that do conduct applicant social media research invariably will learn of more applicants' protected characteristics than employers in the past that did not have access to, or use, social media in hiring."*

profile while researching job candidates. The court did not reject the plaintiff's theory of liability as invalid, but ruled that he lacked factual evidence to support it, where the record showed that the hiring manager did *not* use social media to research job candidates, among other things.[19]

Overall, the available legal guidance suggests that a hiring employer's knowledge of an applicant's protected characteristic will be treated under the same legal standards—whether that knowledge is derived from social media sources or from other, more traditional ones. That stated, the number of cases involving hiring discrimination will likely grow, as employers in present and future years that *do* conduct applicant social media research invariably will learn of more applicants' protected characteristics than employers in the past that did not have access to, or use, social media in hiring.

Discriminatory Harassment Claims

In the context of discriminatory harassment arising from workplace social media use, courts similarly appear to view social media no differently than email and other existing technological platforms: all may be an extension of the workplace for which employers bear responsibility and may bear liability for hostile work environments, depending on the facts and evidence in a particular case.

The EEOC Press Release suggests social media-based harassment claims are at the forefront of plaintiffs' attorneys' radars. As one such attorney reportedly commented (while serving as a panelist at the EEOC meeting):

> Even if employees post harassing or derogatory information about coworkers *away from the workplace,* for example, an employer may be liable for a hostile work environment if it was aware of the postings, or *if the harassing employee was using employer-owned devices or accounts*. (Emphasis added.)[20]

Also discussed during the meeting was a recent EEOC "informal, procedural" decision to reverse an ALJ's dismissal of an employee's Title VII racial harassment complaint that arose from a co-worker's facially racist Facebook post.[21] The Commission determined that there was sufficient evidence of an ongoing pattern

of co-worker harassment, including the Facebook post, such that the complaint should not have been dismissed; the Commission remanded the case for investigation and further processing.[22]

Recent court decisions also demonstrate liability risks for employers in the area of social media harassment.

- In one case litigated through verdict and appeal in California state court, *Espinoza v. Cnty. of Orange*,[23] a jury found an employer liable to an employee for disability harassment where his co-workers had posted offensive social media blogs about his "claw" hand (a birth defect by which he had only two fingers). On appeal, the employer argued that it did not maintain the blog site at issue and that it could not determine that the postings (which were made anonymously) actually came from its employees during the investigation into plaintiff's internal complaint.[24] The court denied the appeal and upheld the jury's verdict for plaintiff, reasoning that there was sufficient evidence for the jury to impute responsibility to the employer for the offensive blog posts because the harassing employees had accessed the blog site using the employer's computers and their blogs discussed workplace issues.[25]
- In another case decided in federal court, *Yancy v. U.S. Airways*,[26] a female employee sued her employer for harassment based in part on her male co-worker's posting a photograph on Facebook that depicted plaintiff leaning over a desk, exposing part of her underwear. Based on the totality of evidence, including that the company had investigated and taken appropriate remedial measures when plaintiff complained, and that she herself had made social media postings of a more graphic nature, the Circuit Court upheld the dismissal of the claim on summary judgment.[27]

The foregoing cases are representative of other cases that similarly involve claims of workplace harassment carried out in whole or in part through social media activity.[28]

Social Media Exposes Employers To Significant Business Risks

There are also considerable commercial interests jeopardized by employees' misuse of social media at work. Although employees can be valuable ambassadors for a company through their promotion of the company's brand and reputation via social media, when employees misuse this medium, the results can be caustic for a company's business.

The potential consequences of employee social media misuse are extensive and wide-ranging, such as: productivity loss when employees use social media for personal reasons during work hours; depression of employee morale; inappropriate communications between employees, including those that give rise to the discriminatory harassment claims discussed above, as well as online stalking, and other potentially criminal behavior; disparagement of company interests, which can harm brand reputation and result in customer losses; and dissemination of information that can waive the company's attorney-client privilege, forfeit its intellectual property rights, or violate securities laws.

Employee misuse of social media can also involve an employee's violation of his or her own confidentiality, non-disclosure, and/or

"Although employees can be valuable ambassadors for a company through their promotion of the company's brand and reputation via social media, when employees misuse this medium, the results can be caustic for a company's business."

non-solicitation agreement. Such violations can be driven by an array of different employee mindsets, ranging from inadvertence or carelessness, to malice against the company, to personal profit-seeking—such as where an employee plans to depart the company and knowingly steals confidential, propriety information, either to start a competing business or to assist a competitor entity to which the employee plans to transfer.

While these all can be destructive for a company and cause serious business losses, the aftermath of stolen proprietary information can be particularly catastrophic.[29] Instigating litigation against such a nefarious, departing employee may be a company's only option to try to safeguard and retrieve its proprietary information and prevent unfair competition that could mean the difference between survival and extinction, particularly for small businesses.

Trade secret theft involving social media has been a focus of several recent, high-stakes lawsuits. Illustrative is *Christou v. Beatport, LLC,*[30] where a nightclub brought suit against a former employee on claims that he had stolen trade secrets to facilitate post-employment competition by accessing the club's MySpace account and profiles of MySpace "friends," using login/password information he had access to as part of his job duties at the club. The court held, as a matter of first impression, that the MySpace data—namely, information regarding the club's customers/online "friends," including their personal cell phone numbers and email addresses—qualified for "trade secret" protection as a matter of law. The court's reasoning was: (1) this social media content was akin to a traditional database of customer contacts; (2) such a database could not be obtained through publicly available directories, nor readily be ascertained from outside sources; and (3) although, given adequate time and effort, a competitor might duplicate the MySpace information, such an endeavor would require thousands of individual "friend" requests (with no guarantee of a "friendly" response), and with the associated time required, any such duplication would not be current enough to be useful to a competitor. The court concluded that the employee's motion to dismiss must be denied, and the employer's trade secret theft claim allowed to move forward.

The number of lawsuits like *Christou* is considerable,[31] and it is expected to increase in coming years as "social business" becomes even more prevalent.

The Current Uncertain, and Largely Anti-Business, Legal Landscape

Compounding the significance of companies' vulnerabilities to the EEOC and the plaintiffs' bar arising from the increase in workplace social media use is a dearth of any clear national standard to guide employers.

What does exist is a smattering of state law statutes, each with its own unique phraseology and nuances, enforcement mechanisms (or lack thereof), and differing sets of social media circumstances exempted from their otherwise broad restrictions on employer rights. These state laws pose particular problems for employers that need access to their employees' social media content to conduct internal investigations into complaints of misconduct, which may avoid employment litigation altogether, and then to defend themselves in the event employment litigation does ensue. Added to the state law mishmash are an increasing number of NLRB rulings in individual cases that further limit employers' rights in this area.

Inconsistent State Social Media Statutes

Driven by privacy advocacy groups concerned about employers intruding into the personal lives of applicants and employees—and, somewhat ironically, triggered primarily by privacy invasions perpetrated by *public* employers[32]—more than a dozen states since 2012 have enacted laws protecting employees' social media account information from their employers[33]—Arkansas, California, Colorado, Illinois, Louisiana, Maryland, Michigan, Nevada, New Hampshire, New Jersey, New Mexico, Oklahoma, Oregon, Rhode Island, Tennessee, Utah, Washington, and Wisconsin.[34] These laws all generally bar employers from requiring or requesting that applicants and employees disclose their personal social media account usernames or passwords. Beyond that one common feature, however, state laws represent the antithesis of uniformity, creating a confusing landscape for multi-state employers to navigate and with which to comply.

The most troubling inconsistency relates to employers' ability to access their employees' social media accounts in the context of conducting internal investigations into workplace misconduct.

Far from being driven by any desire to pry into their employees' personal lives, employers' interest in accessing employee social media accounts stems from their legitimate business interests in maintaining safe and productive workplaces for employees, in which complaints of harassment and other untoward behavior are investigated fully and redressed promptly, as well as in ensuring against misappropriation of confidential, proprietary employer information and trade secrets. Employers often will be unable to further either of these important business interests without investigative access to social media information from their employees' accounts.

Some states recognize these valid employer interests by expressly exempting from their statutes' otherwise broad proscriptions on an employer's right to require access to employee personal social media accounts to investigate workplace misconduct. Other state laws, however, are either restrictive in the scope of investigative exemptions provided, or contain no such exemptions at all. The following overview illustrates the wide range of different state law provisions in this area, set forth from "best" to "worst" for employers in terms of their liberty to investigate:

- **Arkansas:** The statute grants employers nearly unconditional exemption from the statute's prohibitions, providing that employers may request an employee to disclose a personal social media account's username and password if his or her account activity is "reasonably believed to be relevant to the employer's formal investigation or related proceeding into that employee's alleged violation of a employer written policy, or a federal, state, or local law or regulation."[35]
- **Wisconsin:** Although the statute contains a broad investigative exemption for employers, it only allows employers to require that an employee show access to his or her Internet account; in other words, *the employer cannot require the employee to disclose a username, password or security information for the employee's personal Internet account* for purposes of securing investigative access. The laws in Oregon and Washington are similar.[37]
- **Louisiana, Michigan and New Jersey:** The statutes are vague and thus ambiguous in terms of the scope of employers' investigative rights. The laws appear to provide for a broad investigative exemption, but they add the qualifier that the exemption applies only if employers have "specific information" to justify it—without providing guidance on what type of information qualifies as "specific."[38]
- **Colorado and Maryland:** The statutes are much more restrictive for employers, permitting exemption only when employers are investigating specific types of misconduct (such as trade secret theft or securities fraud).[39]
- **Illinois and Nevada:** The statutes provide for no investigation exception at all for employers.[40]

Overall, the above depicts a confounding hodgepodge of different state statutory provisions regarding companies' ability to require access to employees' social media accounts to investigation workplace misconduct.[41] Businesses with employees in multiple states simply have not a shred of certainty in this area.

Lack of Predictability in Litigation Discovery

Compounding the difficulties for employers posed by statutes in states that restrict employer access to employee social media content for purposes of conducting workplace investigations in the normal course of business—*before* litigation and potentially avoiding litigation—is the uncertainty for employers that have a need for that content once *in* litigation. The utility of social media content for employers in litigation is both myriad and diverse, and its importance cannot be understated. But litigation discovery procedures provide no guarantee that employers will be able to obtain such content. Although existing federal discovery rules do not require reform in this area (judges are appropriately considering social media evidence just like any other type of evidence that may be sought in discovery[42]), the inherent uncertainty of courts' outcomes when ruling on discovery motions makes employers' need for certainty that they can obtain social media content *pre*-litigation that much more critical. Indeed, such content can often be outcome-determinative in employment litigation.

Demonstrative in this regard is a recent sexual harassment case, *Debord v. Mercy Health Sys. of Kansas, Inc.*[43] The case arose when an employer discharged a female employee for making Facebook posts via her cell phone during work hours. The employee then sued, seeking to hold the employer liable for sexual harassment. She argued that her male supervisor had sexually harassed her and the employer should have been aware of the harassment by virtue of her posting statements about it on Facebook. The court ruled for the employer on summary judgment. The court reasoned the employee's Facebook posts did not constitute proper notice sufficient to trigger the employer's duty to take corrective action because there was no evidence that the employer was monitoring its employees' social media activity, and when coworkers brought the posts to the attention of Human Resources, the employer conducted an investigation and otherwise acted promptly and properly in response.

The case is significant for two reasons. First, it shows that disposition of a harassment suit can depend on whether an employer consistently monitors its employees' social media activity; here, the employer consistently did not, which ultimately meant it could not be held liable for having notice of an employee's complaints of harassment via social media. Had the employer been monitoring employees' social media activity, but not been consistent in doing so, the outcome in the case likely would have been different. The current inconsistency among state statutes, however, will make it difficult, if not impossible, for multi-state employers to treat all employees consistently with respect to social media monitoring. Second, the case illustrates the importance of an employer being able to conduct an investigation into alleged misconduct by reviewing an employee's social media posts; here, the employer was able to do so and did so appropriately—ultimately leading to its exoneration for harassment liability in the suit. In states that prohibit such investigations, an employer would not be able to do so and could face a different litigation fate.

Social media content can also be critical for employers in wage and hour litigation. An employee's social media activity can be

> *These court cases instruct that although social media activity by employee-plaintiffs may indeed be highly relevant to an employer's ability to present a substantive defense to employment claims, courts may bar employers from obtaining that information in discovery.*

evidence of hours spent working—which may confirm or refute a plaintiff's claim for unpaid overtime hours—and can be evidence of an employee's actual daily job duties—which may confirm or refute a claim for misclassification for overtime eligibility. In *Palma v. Metro PCS Wireless, Inc.,*[44] for example, current and former employees sought unpaid overtime wages under the Fair Labor Standards Act (FLSA). The defendant-employer sought discovery (through interrogatories and document production requests) of "all posts to Plaintiffs' social media accounts from 2010 to the present that relate to 'any job descriptions or similar statements about this case or job duties and responsibilities or hours worked which Plaintiffs posted on LinkedIn, Facebook or other social media sites'…including "all private messages Plaintiffs sent from these sites." The employer argued that this sought-after information was relevant to its affirmative defense that plaintiffs were not entitled to overtime pay because they were properly classified as exempt and/or that they did not actually work more than 40 hours per week (as plaintiffs may have made posts regarding their actual job duties and/or posts containing comments that contradicted their testimony regarding breaks taken during work hours). The court denied the motion to compel, reasoning that the requests were overbroad and speculative.

Similarly illustrative is *Mancuso v. Florida Metropolitan Univ., Inc.,*[45] an FLSA action where a non-exempt employee sought back overtime wages from his employer. Following the employee-plaintiff's deposition, during which he was questioned about his use of Facebook and MySpace, the employer issued a subpoena *duces tecum* to online social media providers to try to obtain the content of the plaintiff's social media activity. Although admitting that time spent using Facebook and MySpace during work hours could bear on the amount of back overtime wages he was due, the plaintiff moved to quash the subpoenas and/or for entry of a protective order to narrow the subpoenas' scope. The court held that the plaintiff did have standing to seek to quash the subpoenas, relying on other courts' decisions, including one that held that "an individual has a personal right in information in his or her profile and inbox on a social networking site and his or her webmail inbox in the same way that an individual has a personal right in employment and banking records."[46] (Ultimately, the court denied plaintiff's motion due to procedural defects in his papers.)

These court cases instruct that although social media activity by employee-plaintiffs

may indeed be highly relevant to an employer's ability to present a substantive defense to employment claims, courts may bar employers from obtaining that information in discovery.[47] The potential preclusion of employers obtaining social media content during litigation underscores the importance that employers be lawfully entitled to monitor and amass such social media information *before* litigation. Indeed, had the employer in *Palma* done so, it might have learned that its employees had been wrongly classified and were working hours for which they should have been paid overtime, leading to corrective measures to remediate the situation—avoiding litigation altogether.

Social media information may be critical to enabling an employer to adequately defend its interests in litigation, but waiting to obtain that information in litigation discovery will often be too late. Predictability for employers regarding entitlement to obtain that information in the regular course of business, *before* litigation, is thus that much more critical.

Social Media "Legislation" by the NLRB

EXPANSION OF JURISDICTION INTO NON-UNION WORKFORCES

The NLRB administers and enforces the National Labor Relations Act (NLRA),[48] which Congress enacted to encourage employees to engage in collective action "for the purpose of negotiating the terms and conditions of their employment or other mutual aid or protection."[49] With the persistent decline in unionized workforces,[50] there are strong arguments that the NLRA's relevance has similarly declined. For example, the proliferation of federal, state, and local wage and hour and other employment law statutes tends to monopolize employment professionals' time rather than concerns related to employee collective action (outside of the wage and hour collective action sphere).

President Obama's appointees to the NLRB and its independent General Counsel[51] have engaged in a systematic campaign to counter this marginalization by seeking to increase the number of unionized employees across the country and asserting the Board's jurisdiction over employers with non-union workforces. Through aggressive prosecution of unfair labor practice charges based on novel legal arguments,[52] unprecedented rule-making[53] and pro-union decisions,[54] the NLRB and its General Counsel have successfully reengaged the attention of U.S. businesses.

EMPLOYEE USE OF SOCIAL MEDIA CONSTITUTES PROTECTED ACTIVITY

As part of its pro-union agenda, the NLRB has focused much of its attention on the use of social media in the workplace. Initially, the NLRB and its General Counsel operated under the conclusion that employee social media communications are protected to the extent they (a) discuss terms and conditions of employment (b) among employees. This standard applies regardless of whether the conversation occurs solely through social media; for example, tweeting a comment that sparks a conversation among employees satisfies part (b) of the test. The number of potential "bystanders" with access to the webpage, tweet, etc., is irrelevant.[55] Conversely, an employee's comments on social media are generally not protected if they are mere gripes not made in relation to group activity

> *The NLRB also appears on the cusp of granting access to employer-provided email (and potentially employer-generated social media) to unions and employee-initiated organizing campaigns.*

among employees.[56] Of course, this distinction is not always obvious.

NLRB case law has followed its General Counsel's social media memos.[57] For example, in *Design Technology Group,*[58] a group of employees lodged complaints with their manager about a supervisor. Subsequently, on Facebook, the employees discussed their complaints and disparaged their supervisor. The Facebook post was seen by the manager and the employees were terminated from their employment. In concluding that the employer violated the NLRA, the NLRB found that the employees were engaged in protected concerted activity and that the complaints on Facebook "were complaints among employees about the conduct of their supervisor as it related to their terms and conditions of employment."

HEIGHTENED SCRUTINY OF EMPLOYER POLICIES

As with the "protected activity" analysis, the General Counsel's social media memos set the stage for subsequent Board action. The NLRB's leading decision on social media policies is *Costco Wholesale Corp.*[59] In *Costco,* the NLRB concluded that the Company violated the NLRA by maintaining a rule prohibiting employees from electronically posting statements that "damage the Company… or damage any person's reputation."[60] In reaching this conclusion, the NLRB stated that a violation is dependent on a showing that: "(1) employees would reasonably construe the language to prohibit Section 7[61] activity; (2) the rule was promulgated in response to union activity; or (3) the rule has been applied to restrict the exercise of Section 7 rights."[62] In applying this analysis to find a violation of the NLRA, the NLRB ignored the employer's good faith intent not to apply the policy to protected activity.

UNION ACCESS TO EMPLOYER-PROVIDED EMAIL

The NLRB also appears on the cusp of granting access to employer-provided email (and potentially employer-generated social media) to unions and employee-initiated organizing campaigns. Early in 2014, the NLRB announced that it would decide whether employers must permit employees to use workplace email in their collective action to improve wages, hours, and working conditions.[63]

In *Purple Communications,* the ALJ followed established precedent in holding that the employer properly denied access to its email systems for union purposes. In reaching this decision, the ALJ cited a Bush-era decision which held that "employees have no statutory right to use the[ir] Employer's e-mail system for Section 7 purposes."[64] In a request for briefs from interested parties,[65] the NLRB publicized its intent to reexamine this holding.[66]

The NLRB also indicated its decision in *Purple Communications* may touch upon two related questions:

(1) Do employee personal electronic devices (e.g., phones, tablets), social media accounts, and/or personal email accounts affect the proper balance to be struck between employers' rights and employees' Section 7 rights to communicate about work-related matters? If so, how?

(2) Identify any other technological issues concerning email or other electronic communication systems that the NLRB should consider in answering the foregoing questions, including any relevant changes that may have occurred in electronic communications technology since *Register-Guard* was decided. How should these affect the NLRB's decision?

Finally, the NLRB's proposed changes to its regulations governing union elections have been well-publicized.[67] Most of the attention on these proposed rules has focused on the shortened period in which employers can conduct pro-employer campaigns under these new rules. Often overlooked is the requirement that employers provide employee contact information to the unions earlier in the process, as well as requiring, for the first time, that employers provide employee email addresses to the union. Unions now have another method of contacting employees and can more easily find employee Facebook pages and other social media sites by inputting the email addresses into the sites' search functions.

Conclusion

The inconsistency among state laws governing employers' ability to access employees' social media accounts, the NLRB's ad-hoc, pro-employee rulemaking and decisions, and the importance of social media content to employers in litigation combine to make workplace social media use a high risk area for U.S. businesses and warrant the attention of federal lawmakers.

A critical problem area is employers' inconsistent rights from state to state with respect to investigations into workplace misconduct, forcing multi-state employers to either universally adhere to the most restrictive provisions from each state law or implement different enforcement standards for different employees depending solely on the state where the employees work.

The uncertainty is further exacerbated by states with legislation pending but not yet enacted into law. Even in the states without statutes partially or fully prohibiting employers from requiring employee access to social media account information for investigation purposes, the wording of the statutes is often so ambiguous (and untested within the courts) that employers lack needed guidance and are forced to act conservatively or risk becoming a legal test case. Unfortunately, taking the seemingly most "risk adverse" course of action—avoiding employee social media use altogether—may still expose employers to liability. A failure to fully investigate complaints of workplace

"Unfortunately, taking the seemingly most 'risk adverse' course of action—avoiding employee social media use altogether—may still expose employers to liability."

misconduct by one employee can result in liability on the employer's part to another employee—such as in the case of a discriminatory harassment complaint by one employee against another. It has become imperative that federal and state laws develop a better and more consistent balance between employees' interest in online privacy and employers' interest in enforcing important workplace policies and fully investigating reported violations. Unfortunately, many of these governing bodies and their regulatory agencies are pursuing pro-union agendas without regard to the business and economic realities involved in employer-employee relations.

Endnotes

1 *See* Shea Bennett, *Social Media Business Statistics, Facts, Figures & Trends 2014* (Apr. 25, 2014) (hereinafter, "Bennett"), *available at* http://www.mediabistro.com/alltwitter/social-business-trends-2014_b56645; Jeff Bullas, *22 Social Media Facts and Statistics You Should Know in 2014* (Jan. 16, 2014) (hereinafter, "Bullas"), *available at* http://www.jeffbullas.com/2014/01/17/20-social-media-facts-and-statistics-you-should-know-in-2014/.

2 *See* Bennett, *supra*; Bullas, *supra.*

3 *See* Kimberlee Morrison, *20 Marketing Trends and Predictions to Consider for 2014* (Oct. 31, 2013), *available at* http://socialtimes.com/infographic-20-marketing-trends-and-predictions-to-consider-for-2014_b137315.

4 *See* Bennett, *supra.*

5 *See* Press Release, U.S. Equal Employment Opportunity Commission, *Social Media Is Part of Today's Workplace but its Use May Raise Employment Discrimination Concerns* (Mar. 12, 2014) (hereinafter, "EEOC Mar. 12, 2014 Press Release"), *available at* http://www1.eeoc.gov/eeoc/newsroom/release/3-12-14.cfm?.

6 *Id.*

7 *Id.*

8 *See, e.g.*, Hannah Morgan, *Want to Get a Job Fast? Become a Social Media Savant—A survey finds more than three-quarters of employers hire using social networks* (Sept. 11, 2013), *available at* http://money.usnews.com/money/blogs/outside-voices-careers/2013/09/11/want-to-get-a-job-fast-become-a-social-media-savant; *see also* Jobvite, *Recruiters Increasingly Adopt Marketing Tactics in Fierce Competition to Hire, 2013 Jobvite Social Recruiting Survey Shows* (Sept. 5, 2013), *available at* http://recruiting.jobvite.com/company/press-releases/2013/recruiters-increasingly-adopt-marketing-tactics-2013-jobvite-social-recruiting-survey-shows/.

9 Practical Law, A Thomson Reuters Legal Solution, *Aim Higher in Hiring: Social Media in Recruitment* (June 16, 2014) (explaining that "[e]mployers can often bolster their defenses to hiring discrimination complaints by claiming that individuals involved in hiring decisions were not aware of the candidate's protected class status," given that many protected characteristics "are not apparent from resumes or job applications, but may be a part of a candidate's social media identity," yet "[e]mployers that learn about protected characteristics through social media forfeit ignorance of protected characteristics as a defense"), *available at* http://us.practicallaw.com/3-571-2470?q=aim+higher+in+hiring.

10 *Id.*

11 *Id.*

12 *See* video transcript of EEOC March 12, 2014 Meeting, *available at* http://www.eeoc.gov/eeoc/meetings/3-12-14/video.cfm (hereinafter, "EEOC Video"); *see also* Jack Moore, *Think Before You Post: EEOC Cases Show Pitfalls of Social Media In The Workplace*, Federal News Radio 1500AM (Mar. 13, 2014) (hereinafter, "Moore"), available at http://www.federalnewsradio.com/434/3580540/Think-before-you-post-EEOC-cases-show-pitfalls-of-social-media-in-the-workplace; *see id.* (discussing EEOC administrative rulings presented at March 12, 2014 meeting, including *Reese v. Salazar, Sec'y, Dep't of Interior*, slip op., EEOC Agency No. NPS100602 (Nov. 15, 2012) (hereinafter "*Reese* slip op."), *available at* http://www.eeoc.gov/decisions/0120122339.txt.

13 EEOC Video.

14 *Id.; Reese*, slip op. at 2.

15 EEOC Video; *Reese*, slip op. at 2.

16 EEOC Video; *Reese*, slip op. at 3.

17 *Gaskell v. Univ. of Kentucky,* Civ. A. No. 09-244-KSF, 2010 WL 4867630 (E.D. Ky. Nov. 23, 2010).

18 *Nieman v. Grange Mutual Ins. Co.,* No. 11-3404, 2013 WL 1332198 (C.D. Ill. Apr. 2, 2013).

19 *Neiman*, 2013 WL 1332198, at *11-14. Indeed, the only record evidence was that: the hiring manager denied under oath ever having used any social media sites, including LinkedIn, to research candidates; plaintiff supported his contrary assertion not with any evidence about the hiring manager in question, but with studies showing that *most* employers used social media to research candidates, coupled with his own speculation that the hiring manager there likely had as well; LinkedIn's response to plaintiff's subpoena for information about viewers of his profile indicated affirmatively that the hiring manager in question had never opened a LinkedIn account by which

she could have viewed plaintiff's profile; there was no evidence that the hiring manager knew plaintiff's exact age, much less that she relied on it as a decision-making factor; and there was strong evidence supporting her legitimate reasons for deciding that plaintiff's attitude and demeanor during his interview made his personality unsuited for the job in question (which plaintiff, appearing *pro se*, had effectively corroborated to the court by his litigation misconduct (found by the court separately to be so "contumacious and in bad faith" as to subject him to sanctions)). *Id. at* *2, 3, 6-7, 11-14, 15. In addition, there was uncontested evidence that the hiring manager had actually offered the job to two other candidates who were older than the plaintiff but who had declined (one age 57, the other 48). *Id.* at *2, 3, 6-7, 11-14, 15.

20 EEOC Mar. 12, 2014 Press Release, *supra*.

21 *See* EEOC Video (discussing *Knowlton v. LaHood, Sec'y, Dep't of Transportation*, EEOC Agency No. 2012-24254-FAA-05 (June 15, 2012), *available at* http://www.eeoc.gov/decisions/0120121642.r.txt).

22 *See id.*

23 *Espinoza v. Cnty. of Orange,* No. G043067, 2012 WL 420149 (Ct. of App., Fourth Dist., Div. 3, Cal., Feb. 9, 2012).

24 *Id.*

25 *Id.* at *7.

26 *Yancy v. U.S. Airways,* No. 11-30799, 469 F. App'x 339, 2012 WL 1109341 (5th Cir. Apr. 4, 2012).

27 *Id.*

28 *See, e.g.*, *Suvika Enter. dba Himalyas Rest. v. Roy*, No. 2014-10244 (Butler Cnty., PA Ct. Comm. Pleas, filed March 7, 2014) (harassment action seeking damages, inter alia, for harassment of employees and defamation on social media networks); *Smith v. Blitzlocal LLC, et al.*, No. 1110-13151 (Multnomah Cnty., [Ore.] Cir. Ct., filed Oct. 10, 2011) (alleging sexual harassment involving older, male bosses who hired a group of 18-year-olds for social media marketing work and then treated office as "their personal hunting grounds for potential sexual conquests," but when plaintiff complained, the employer allegedly forced her to retract her complaint by threatening to fire her). *See also cf. Fennell v. Marion Indep. Sch. Dist.*, 963 F. Supp. 2d 623, 628 (W.D. Tex. 2013) (ruling in favor of students who asserted racial harassment claims based on "comments, taunts and electronic images sent via cell phone texts and on social media websites, such as Facebook").

29 The risk of such occurrences is exacerbated when the employee in question is adhering to an employer's bring-your-own-device-to-work (BYOD) policy—a growing trend among companies, under which employees are encouraged or required to use *personal* computing devices (laptops, tablets, smartphones, and the like (collectively, Devices))—to perform work functions. Disputes over ownership and access rights to work-related data stored on BYOD Devices are particularly thorny for companies. Whereas the individual employee technically owns the Device and has a privacy interest with respect thereto, the company technically "owns" the information on that Device, with the employee only having access to it on his or her Device by virtue of the company's granting permission in the context of the employment relationship. These competing interests may present confounding concerns for companies seeking to secure access to, or to establish ownership rights in, proprietary information stored on BYOD Devices upon the employee's departure, or in the event of a conflict between the company and employee.

30 *Christou v. Beatport, LLC,* 849 F. Supp. 2d 1055 (D. Col. 2012).

31 *See, e.g.*, *Eagle v. Morgan*, 2013 WL 943350 (E.D. Pa. Mar. 12, 2013); *Pre-Paid Legal Servs., Inc.. v. Cahill*, 924 F. Supp. 2d 1281 (E.D. Okla. 2013); *Ardis Health, LLC v. Nankivell*, 2011 WL 4965172 (S.D.N.Y. Oct. 19, 2011); *PhoneDog v. Kravitz*, 2011 WL 5415612 (N.D. Cal. Nov. 8, 2011); *Amway Global v. Woodward*, 744 F. Supp. 2d 657 (E.D. Mich. 2010).

32 *See* Courtney B. Lario, *What Are You Looking At?: Why the Private Sector's Use of Social Media Need Not Be Legislated*, 38 Seton Hall Legis. J. 133, 137-140 (2013) (chronicling development of state social media laws, commencing with Maryland in 2012 (following the state's Department of Public Safety and Correctional Services requiring in 2011 that a corrections officer provide his Facebook password as a condition of recertification, "supposedly to determine whether the officer had ties to gang members," which led to the state American Civil Liberties Union ("ACLU") taking a stance and publicizing the event and then a public outcry that eventually resulted in passage of the Maryland "User Name and Password Privacy Protection Act"), "the first of its kind and marked the beginning of a nationwide trend").

33 *See* National Conference of State Legislatures, *Employer Access to Social Media Usernames and Passwords*, *available at* http://www.ncsl.org/issues-research/telecom/employer-access-to-social-media-passwords.aspx ("NCSL") ("last, update Sept. 28, 2014").

34 Bills restricting employers from requiring applicants and/or employees to share their social media

account access information have been introduced in more than a dozen additional states, with bills either active in committee, approved by a state's senate and sent to its house/general assembly (or vice versa), "laid on table," or marked "carryover" from the last legislative session—and thus ostensibly still pending (as of the NCLS's last reported update on September 28, 2014)—in Georgia, Hawaii, Iowa, Kansas, Massachusetts, Minnesota, Missouri, Nebraska, New York, North Carolina, Ohio, and Pennsylvania. *See* NCSL, *supra*.

35 A.C.A. § 11-2-124 (2014).

36 2013 Wisconsin Act 208.

37 *See* Oregon: ORS § 659A.330 (2013) (employers are not prohibited from conducting investigations (*without requiring employees to provide personal social media account information prohibited by this law*) to: ensure compliance with applicable laws, regulatory requirements, or prohibitions against work-related employee misconduct based on the employer's receipt of specific information about an employee's activity on a personal online account or service; the exemption requires employees to share content that is reported to the employer, which the employer must view in order to make a factual determination); Washington: Rev. Code Wash. (ARCW) § 49.44.200 (2013) (employers may require an employee to share the contents of a personal social networking account (*but not require the disclosure of login information*) if conducting any of a broad range of investigations "to make a factual determination in the course of conducting an investigation," in responding to information about activity on an employee's account, to ensure compliance with: applicable laws; regulatory requirements; or prohibitions against work-related employee misconduct; or to investigate an allegation of the unauthorized transfer of proprietary, confidential, or financial employer information to an employee's personal account).

38 *See* Louisiana: 2014 La. ACT 165; Michigan: 2012 Mich. Pub. Acts 478; New Jersey: 2012 NJ A2878 (NS).

39 *See, e.g.,* Colorado: Colo. Rev. Stat. § 8-2-127 (2013) (exempting only investigations *to ensure compliance with applicable securities or financial law or regulatory requirements* based on receipt of information about an employee's use for business purposes of, or information about the unauthorized downloading of an employer's proprietary information or financial data to a personal web site to, a personal web site, Internet web site, web-based account, or similar account); Maryland: Md. Code Ann., Lab. & Empl. § 3-712 (2012) (permitting investigating employees upon employer's receipt of information about the use of a personal website, Internet website, web-based account or similar account by an employee for business purposes, *if* the investigation is for the purpose of *ensuring compliance with securities or financial law, or regulatory requirements*, or the unauthorized downloading of an employer's proprietary information or financial data to a personal website, internet website, web-based account or similar account) (emphasis added).

40 *See* Illinois: 820 ILCS 55/10 (2014); Nevada: Nev. Rev. Stat. Ann. § 613.135 (2014).

41 The state laws have varying terms on a number of other issues as well. Discussion of these details is beyond the scope of this article.

42 *See* March 27, 2014 letter from Chamber of Commerce, United States of America, Randel K. Johnson, Senior Vice President, Labor, Immigration and Employee Benefits, and James Plunkett, Director, Labor Law Policy, to EEOC Chairperson Berrien and Commissioners Barker, Feldblum, Lipnic and Yang.

43 *Palma v. Metro PCS Wireless, Inc.,* No. 11-cv-02560, 860 F. Supp. 2d 1263 (D. Kan. 2012).

44 *Mancuso v. Florida Metropolitan Univ., Inc.,* No. 8:13-cv-698-T-33MAP, 2014 WL 1877578, at *1-2 (M.D. Fl. Apr. 29, 2014).

45 *Mancuso v. Florida Metropolitan Univ., No. 09-61984,* 2011 WL 310726 (S.D. Fl. Jan. 28, 2011).

46 *Id.* at *2 (quoting *Crispin v. Christian Audiger, Inc.*, 717 F. Supp. 2d 965, 974 (C.D. Cal. 2010)). *See also, e.g., J.T. Sherman Lumber Co. v. Gilco Lumber, Inc.*, 2008 WL 3833216, at *1 (N.D. Miss. Aug. 14, 2005 (holding that party had standing to challenge subpoenas directed to internet service providers, such as Microsoft, Yahoo, and Google).

47 For a comprehensive discussion of the factors that federal district courts have considered when determining the scope of an employer's discovery rights as to an employee's private social media information, as well as an extensive review of the numerous federal district court rulings on this topic, *see Giacchetto v. Patchogue-Medford Union Free Sch. Dist.*, 293 F.R.D. 112 (E.D.N.Y. 2013).

Plaintiff there was a teacher who claimed she had "adult ADHD" that qualified her as "disabled" and that after she notified her school of the condition, she suffered mocking and disparate treatment, resulting in her filing a charge with the New York Division of Human Rights (state counterpart to EEOC), after which she allegedly was disciplined in retaliation. In litigation discovery, the employer-defendant sought signed authorizations for the release of records from all of the plaintiff's social media accounts, including Facebook, Twitter, and MySpace, insofar as they contained information falling within any of the following categories:

postings about her emotional and psychological well-being; postings about her physical damages; and/or any accounts of the events alleged in her complaint. Plaintiff refused the employer's discovery request, leading to an employer motion to compel. The employer argued in support of its motion that information from plaintiff's social media accounts was relevant to her substantive disability claim as well as to her claim for damages, because the information would reflect her "levels of social interaction and daily functioning" and her "emotional and psychological state," and that any accounts of the events on which she based her mocking and disparate treatment claims were also relevant and discoverable. Plaintiff argued in opposition that the employer's request was a speculative "fishing expedition 'designed to harass [her],'" and that it would unnecessarily impinge on her privacy rights. The court granted in part and denied in part the employer's motion. In its ruling, the court first established:

[T]hat Defendant is seeking social networking information as opposed to traditional discovery materials does not change the Court's analysis [as to relevance and discoverability under FRCP], [but the] fact that the information Defendant seeks is in an electronic file as opposed to a file cabinet does not give [it] the right to rummage through the entire file.

Giacchetto, 293 F.R.D. at 114 (quotation and citation omitted). The court noted there was significant disagreement among courts as to the discovery of private sections of employees' social media sites, with several holding such information discoverable only if there is a threshold evidentiary showing that a public profile page contained information undermining plaintiff's claims—an approach with which the *Giacchetto* court disagreed on the grounds that it could "lead to results that are both too broad and too narrow." *Id.*, at 114 n.1 (citation omitted). In specifically addressing the first category of social media information sought (postings about plaintiff's emotional and psychological well-being), the court commented initially that "[c]ourts have reached varying conclusions regarding the relevance of social networking postings in cases involving claims for emotional distress damages." *Id.* at 115 (citation omitted). The court explained: that an individual may express some degree of joy, happiness, or sociability on certain occasions sheds little light on the issue of whether he or she is actually suffering emotional distress. If the Court were to allow broad discovery of Plaintiff's social networking postings as part of the emotional distress inquiry, then there would be no principled reason to prevent discovery into every other personal communication the Plaintiff had or sent since alleged incident.

[There should be] an important distinction between the relevance of social networking information to claims for physical damages and claims for emotional damages, [for although] the relevance of a posting reflecting engagement in a physical activity that would not be feasible given the plaintiff's claimed physical injury is obvious, the relationship of routine expressions of mood to a claim for emotional distress damages is much more tenuous.

Id. The court concluded that plaintiff's routine status updates and/or other communications that were not generally relevant to her claim for emotional distress damages, but that certain limited social networking postings should be produced, namely, any specific references to the emotional distress she claims she suffered or treatment she received in connection with the incidents underlying her claims (e.g., references to a diagnosable condition or visits to medical professionals), and any postings that referred to alternate potential sources/causes of her claimed emotional distress. *Id.* As to postings about plaintiff's physical damages, and any accounts of events alleged in complaint, the court held the information was relevant and discoverable, ordering that plaintiff must produce any postings or photographs on social media sites that reflected physical capabilities inconsistent with her claimed injuries and any accounts of events alleged in her complaint, contradictory or otherwise. *Id.* at 116.

Surveyed by the *Giacchetto* court in reaching its decisions are the following lead court decisions in this area: *Potts v. Dollar Tree Stores*, 2013 WL 1176504 (M.D. Tenn. Mar. 20, 2013); *Kennedy v. Contract Pharmacal Corp.*, 2013 WL 1966219 (E.D.N.Y. May 13, 2013); *Keller v. Nat'l Farmers Union Property & Cas. Co.*, 2013 WL 27731 (D. Mont. Jan. 2, 2013); *Tompkins v. Detroit Metro Airport*, 278 F.R.D. 387, 388 (E.D. Mich. 2012); *Mailhoit v. Home Depot U.S.A., Inc.*, 285 F.R.D. 566, 570 (C.D. Cal. 2012); *Reid v. Ingerman Smith LLP*, 2012 WL 6720752 (E.D.N.Y. Dec. 27, 2012); *Robinson v. Jones Lang LaSalle Ams., Inc.*, 2012 WL 3763545 (D. Or. Aug. 29, 2012); *Howell v. Buckeye Ranch, Inc.*, 2012 WL 5265170 (S.D. Ohio Oct. 1, 2012); *Sourdiff v. Texas Roadhouse Holdings, LLC*, 2011 WL 7560647 (N.D.N.Y. Oct. 24, 2011); *Offenback v. L.M. Bowman, Inc.*, 2011 WL 2491371 (M.D. Pa. June 22, 2011); *EEOC v. Simply Storage Mgmt., LLC*, 270 F.R.D. 430 (S.D. Ind. 2010).

48 29 U.S.C. §§ 151-169.

49 29 U.S.C. § 151.

50 In 2013, the union membership rate—the percent

of wage and salary workers who were members of unions—was 11.3 percent and there were approximately 14.5 million union workers. In 1983, the first year for which comparable union data is available, the union membership rate was 20.1 percent and there were approximately 17.7 million union workers. U.S. Department of Labor, Bureau of Labor Statistics, *News Release USDL-14-0095* (Jan. 24, 2014).

51 The General Counsel, appointed by the President to a 4-year term, is independent from the Board and is responsible for, among other duties, the investigation and prosecution of unfair labor practice cases.

52 For example, in the well-publicized *Boeing* case, the NLRB's General Counsel asserted that Boeing's decision to build its factory in South Carolina constituted illegal retaliation against unionized employees in Washington for having exercised their right to strike.

53 For example, the NLRB passed a rule requiring employers to post a notice explaining employee rights under the NLRA, which was later enjoined by federal appellate courts.

54 *See, e.g., Piedmont Gardens,* 359 NLRB No. 46 (Dec. 15, 2012) (reversing 34-year precedent and holding that witness statements collected by an employer during an internal disciplinary investigation must be provided to the union if the union's need for the information outweighs the employer's confidentiality interests).

55 NLRB, Office of General Counsel, *Memorandum OM 11-74* (Aug. 18, 2011).

56 NLRB, Office of General Counsel, *Memorandum OM 12-31* (Jan. 25, 2012).

57 NLRB, Office of General Counsel, *Memorandum OM 11-74 supra;* NLRB, Office of General Counsel, *Memorandum OM 12-31, supra*; NLRB, Office of General Counsel, *Memorandum OM 12-59* (May 30., 2012).

58 59 NLRB No. 96 (2013).

59 358 NLRB No. 106 (2012). The *Costco* decision also invalidated the following four employer policies regarding the dissemination of confidential or sensitive information that implicates social media communications: (a) "unauthorized posting, distribution, removal or alteration of any material on Company property" is prohibited; (b) employees are prohibited from discussing "private matters of members and other employees…includ[ing] topics such as, but not limited to, sick calls, leaves of absence, FMLA call-outs, ADA accommodations, workers' compensation injuries, personal health information, etc."; (c) "[s]ensitive information such as membership, payroll, confidential financial, credit card numbers, social security number or employee personal health information may not be shared, transmitted, or stored for personal or public use without prior management approval"; and (d) employees are prohibited from sharing "confidential" information such as employees' names, addresses, telephone numbers, and email addresses. *Id.*

60 *Id.*

61 Section 7 of the NLRA establishes the fundamental right of employees to engage in concerted activity to advance their wages, hours and working conditions.

62 *Id.* at *2.

63 *Purple Communications, Inc.*, 361 NLRB No. 43, 200 LRRM 2041 (2014).

64 *Register-Guard*, 351 NLRB 1110 (2007), *enfd. in relevant part and remanded sub nom. Guard Publishing v. NLRB*, 571 F.3d 53 (D.C. Cir. 2009). While the NLRB's motivation is intended to encourage and aid union organizing activity, such a ruling will also give plaintiffs' lawyers perhaps the single best tool to target employees in their recruitment efforts for class action lawsuits or assembly-line, single-plaintiff actions.

65 *See, e.g., Brief of Amicus Curiae the Chamber of Commerce of the United States of America in Support of Respondent Purple Communications, Inc.*

66 On September 24, 2014, the Board issued its partial decision in *Purple Communications*, but decided to "sever and hold for further consideration the question whether Purple's communications policy was unlawful." *See Purple Communications,* 361 NLRB No. 43 (2014).

67 *See* NLRB Election Rules and Regulations Fact Sheet, *available at* http://www.nlrb.gov/news-outreach/fact-sheets/amendments-nlrb-election-rules-and-regulations-fact-sheet.

U.S. CHAMBER
Institute for Legal Reform

202.463.5724 main
202.463.5302 fax

1615 H Street, NW
Washington, DC 20062

instituteforlegalreform.com