SPECIAL REPORT

California® Employer Resources

Social Media and HR: How to Manage Your Risks

Introduction

Do you use social media? Maybe not—but your employees almost certainly do, both off-duty and at work. By the end of 2011, Facebook boasted 845 million monthly active users and 483 million daily active users. One study found that Twitter usage at work jumped 700 percent in 2011 from the previous year, while employees were three times more active on Facebook in 2011 than they were in 2010.

Whether at work or not, your employees could be using these and other widely accessed social media sites to post racy photos and videos, pen harsh or profanity-laced blogs, or criticize your company and management. Even if they only post seemingly innocuous "status updates" about their day, or take a more passive-observer approach to social media, your employees' activities open you up to a wide range of potentially costly legal and reputational risks.

This Special Report will bring you up to speed on the risks out there and provide practical advice on how to reduce your exposure.

Why You Should Worry

You might think you don't really need to concern yourself with the rise of social media because it's not particularly relevant to your line of business. Think again.

CONTENTS

Many kinds of legal problems can arise from employee or management misuse of social media, including:

- Employees divulging confidential information, whether intentionally or not. An employee posts on his personal Twitter feed about a new strategic initiative that he puts long hours into, or posts a workplace photo showing a product under development.
- Employees disparaging the employer, supervisors and managers, co-workers, clients, or vendors. A disgruntled employee takes to Facebook to decry what she views as a workplace injustice.
- Employees damaging the employer's reputation. An employee posts an offensive video of himself on YouTube while wearing a T-shirt emblazoned with the employer's name.
- Employees harassing co-workers. An employee leaves intimidating comments on a co-worker's Facebook wall.
- Employees endorsing the employer's products or services without making necessary disclosures. An employee raves about one of her employer's products on the employer's Facebook page without disclosing her relationship to the company.
- Discrimination or perceived discrimination. A manager decides not to hire an applicant after viewing his Facebook profile, which makes clear that he has a disability.
- Unfair labor practices. A supervisor terminates an employee for commenting on a co-worker's online post about the unfairness of their wages or hours.

As you can see, employees' and managers' misuse of social media creates a minefield for their employers. The good news is that, in many cases, the misuse stems more from a lack of knowledge than actual malice. By learning more about the risks, you can take steps to address them with your employees and preempt problems.

The Hiring Traps

At first glance, social media can seem like a dream come true when it comes to hiring new employees—it can enable you to learn more about a candidate than was possible in the past. While this ability it definitely has its benefits, it's also fraught with potential pitfalls.

Discrimination

It can almost seem like a cardinal sin these days not to check out an applicant online, but simply Googling someone's name and following the links to social media websites could lead you down a dangerous path. You can easily discover information on social media sites that you would never think of asking about in an interview or that would be illegal for you to ask.

You might, for example, discover a protected characteristic—like race, religion, age, sexual orientation, marital status, pregnancy, or disability—or genetic information ("Today I did the breast cancer 5K in Mom's honor") by looking at someone's profile. You could also learn about arrests and convictions, workers' compensation claims, or bankruptcy filings.

Possessing any of that information might open you up to claims of unlawful discrimination if you eventually choose not to hire the person—even if your decision has nothing to do with the protected information you uncover.

Employers should also be aware that using social media to recruit employees could lead to a pool of applicants lacking in diversity. Studies have shown, for example, that the professional social networking site LinkedIn has significantly fewer African American than white users. Social media sites also tend to skew younger, raising the possibility of age discrimination claims.

Similarly, when employees or others make job postings available to their online friends and acquaintances, they're likely to reach a group with similar demographics.

Consumer reporting laws

To limit their risks, some employers turn to third-party agencies to conduct social media searches on applicants. These agencies can make sure you don't

FCRA and ICRRA Notification Requirements

If you plan on using a third party to conduct social media searches on applicants, you must satisfy several requirements. In addition to obtaining consent from the applicant, you must provide a clear and conspicuous disclosure in writing (before the report is procured or ordered) in a document consisting solely of the disclosure. It should:

- Disclose that an investigative consumer report may be obtained.
- Identify the legally permissible purpose of the report.
- Disclose that the report may include information on the applicant's character, general reputation, personal characteristics, and mode of living.
- Identify the name, address, and telephone number of the investigative consumer reporting agency conducting the investigation.
- Disclose the nature and scope of the investigation requested.
- Notify the applicant of the website address of the investigative consumer reporting agency or, if the agency has no website address, the telephone number of the agency, where the applicant may find information about the agency's privacy practices, including whether the applicant's personal information will be sent outside the United States or its territories.

The disclosure should also inform the individual that he or she can view the file maintained by the agency, during normal business hours, and how he or she can obtain a copy.

In either the disclosure or the consent form, you must provide a check box for the applicant to indicate that he or she wishes to receive a copy of any report that is prepared. If checked, you must send a copy of the report (at no charge) within three business days of the date that the report is provided to you; you can contract with the agency to send the copy.

California Employer Resources™ products are designed to help California employers keep up to date on the latest developments in the constantly changing field of employment law and employee relations. Readers' comments and suggestions are always welcome.

Postmaster, send address changes to:
1819 Polk Street, #290
San Francisco, CA 94109

Customer Service: (800) 695-7178
Fax: (888) 321-5066
Email: custserv@employeradvice.com

President: Matthew T. Humphrey
Production: Alix Hammond

see information that might form the basis of a subsequent discrimination claim. Remember that these agencies may be considered "consumer reporting agencies" under the federal Fair Credit Reporting Act (FCRA) and California Investigative Consumer Reporting Agencies Act (ICRAA), so you must obtain consent before searches are conducted. FCRA and ICRAA also have stringent preliminary notification requirements.

If you ultimately decide not to hire an applicant based on information in a consumer report, you must give the applicant notice of this and include a copy of the report and the Federal Trade Commission's (FTC's) *A Summary of Your Rights Under the Fair Credit Reporting Act.*

Negligent hiring

Social media searches on applicants could result in negligent hiring claims, too. An employer can be held liable for hiring an individual it knew or should have known possessed a certain propensity at the time of hiring; some experts have speculated that the legal standards for employers that have checked an employee's social media activities could be stricter than for those that don't.

If you hire someone whose posts show misogynistic tendencies ("Women are the root of all evil") or a propensity for violence ("I came really close to slamming that guy's head into the wall"), and that person later harasses female employees or engages in workplace violence, those posts could well provide grounds for a lawsuit.

Smart Social Media Practices for Hiring

Despite the risks, many employers will find it worthwhile to conduct online searches of applicants, including their social media profiles and accounts. To protect yourself from discrimination charges, the wise approach is to develop a list of legitimate information you'd like to know. The list could include:

- expressions of hate
- drug use or other illegal conduct
- disparaging comments about work (including employers, co-workers, customers, and vendors)
- the frequency of online activity
- judgment

The checklist is then used by a searcher who will not be involved in the hiring decision, such as a member of the HR staff or a third-party agency. The searcher can filter the information he or she uncovers and provide the decision maker with only relevant material.

It's best to do the search after the interview but before the offer, or to make the offer contingent on passing the check. In most cases, and certainly if you will use a third party to perform the search, you should obtain the applicant's consent before the search.

Additional best practices include:

- Be consistent, using the same practices for every applicant.
- Give the applicant a chance to explain/respond to troubling information.
- Keep complete records of the factors used for hiring decisions, including negative information found online.

Punishing Social Media Conduct: Why You Need to Exercise Some Caution

You're probably safe disciplining an employee for engaging in unlawful online activity at work or spending too much time at work using social media for personal purposes. But outside of these clear-cut situations, you could run afoul of several laws when disciplining an employee based on his or her social media activity.

The National Labor Relations Act (NLRA)

Section 7 of the NLRA gives union and nonunion employees the right "to engage in concerted activities for the purpose of collective bargaining or other mutual aid or protection." (California law also prohibits employer restrictions or discipline based on discussions of wages and working conditions.)

Protected activities can include two or more employees discussing working conditions, and it's now clear that such discussions can occur online. In fact, the National Labor Relations Board's (NLRB's) Acting General Counsel Lafe Solomon has been quoted as equating comments on social media sites with talking "at the water cooler."

It's not surprising, then, that the past two years have seen a jump in NLRB complaints related to disciplinary actions based on employees' work-related postings on social media. For example:

- The NLRB issued a complaint alleging that a sports bar and restaurant unlawfully discharged and threatened to sue two employees who participated in a Facebook conversation initiated by a former co-worker about the employer's tax withholding practices.[1] According to the NLRB, the conversation on Facebook related to employees' shared concerns about a term and condition of employment: the employer's administration of income tax withholdings.

  The board observed that before the Facebook conversation, this shared concern had been brought to the employer's attention by at least one employee who noted on Facebook that she

had requested it be discussed at an upcoming management meeting with employees. The conversation that transpired on Facebook was therefore deemed not only to embody "truly group complaints" but also to contemplate future group activity.

An administrative law judge (ALJ) ruled against the employer, finding that the terminated employees engaged in concerted activity within the meaning of the NLRA when they participated in the Facebook discussion.

Notably, the ALJ also found that an employee's selection of the "Like" option on the former employee's Facebook posting constituted participation in the discussion that was sufficiently meaningful as to rise to the level of concerted activity. In the context of Facebook communications, it constituted an assent to the comments being made and a meaningful contribution to the discussion.

- The NLRB filed a complaint against a Chicago-area auto dealership, alleging unlawful termination of a salesman for posting photos and comments on Facebook that were critical of the dealership.[2] The employee and his co-workers had been unhappy with the low quality of food and beverages at a dealership event promoting a new BMW model because they believed their sales, and thus commissions, would suffer.

  After the event, the salesman posted photos and complained on his Facebook page that only hot dogs and bottled water were offered to cutomers. Other employees had access to the Facebook page and commented. The next week, the dealership's management asked the salesman to remove the posts, and he immediately complied. Nevertheless, he was fired shortly thereafter.

  An ALJ upheld the termination, holding that it was based on other activity, but found the postings involving the sales event and the subsequent exchange of comments with other employees was protected activity.

- The NLRB issued a complaint alleging that Hispanics United of Buffalo (HUB)—a nonprofit that provides social services to low-income clients—discharged five employees in violation of the NLRA.[3] In this case, an employee posted on her Facebook page a co-worker's allegation that employees didn't do enough to help the organization's clients.

  The post generated responses from other employees who defended their job performance and criticized working conditions. After learning of the posts, HUB discharged the five participating employees, claiming that their comments constituted harassment of the employee originally mentioned in the post.

  In the first written decision in one of these cases following a full hearing, the ALJ found that the HUB employees' actions were protected under the NLRA. According to the ALJ, the employees were taking the first step toward taking a group action to defend themselves against accusations about their job performance.

- The NLRB filed a complaint alleging that an employer illegally terminated an employee who posted negative remarks about her supervisor on her Facebook page from her home computer.[4] The posting drew supportive comments from co-workers, prompting the employee to post additional negative comments about the supervisor. That case settled before reaching a hearing, and the employer agreed not to discipline or discharge employees for engaging in discussions about their wages, hours, and working conditions with co-workers and others while not at work.

Bullying and Harassment Move Online

Much has been made of the bullying of teens and pre-teens on social media sites, but online bullying and harassment aren't limited to the young. Employees are taking to the sites and blogs to post gossip, rumors, biased comments, racial slurs, and sexual comments about co-workers, customers, and vendors. What starts with a "friend" request can quickly turn to threats and harassment.

And guess what? You can be just as liable for off-hours online harassment as you are for harassment in the workplace. In an unpublished case earlier this year, the California Court of Appeals affirmed a jury verdict awarding an employee over $820,000 for disability harassment after the employee's co-workers started two blogs that posted critical and offensive comments about the employee. The blogs weren't created on the employer's computers or approved of by the employer, but the employer knew about them and failed to take adequate steps to prevent harassment. (For more on this case, see the May 2012 issue of CEA.)

If it doesn't already, make sure your antiharassment policy clearly applies to the use of social media, and treat complaints of online harassment as you would complaints of workplace harassment.

At press time, appeals were pending in the three cases above that didn't settle.

So what type of social media activity will trigger the NLRA? The ALJ in the HUB case explained that an individual employee's action qualifies as "concerted" as long as the employee engages in it with the goal of initiating or inducing group action. The employee needn't explicitly state that this is his or her goal.

Moreover, while a protected action must be intended to initiate group action, the ALJ noted that the group doesn't have to be trying to change its working conditions. Rather, Section 7 of the NLRA may protect concerted activity for employees' "mutual aid and protection" that is motivated by a desire just to maintain the status quo.

Further, the ALJ explained, NLRA protection doesn't depend on whether:

- the organizing activity was ongoing
- the employees communicated their concerns to their employer before the discipline
- the employees intended to take additional action

On the other hand, the NLRB's acting general counsel has stated that "an employee's comments on social media are generally not protected if they are mere gripes not made in relation to group activity among employees." For example:

- An employee at a retail store posted a Facebook comment complaining about "tyranny" at the store and suggesting that the employer would get a wakeup call because lots of employees were about to quit.[5] Several co-workers responded to his comment, expressing emotional support and asking why he was so wound up.

  In response, the employee asserted that the assistant manager was being a "super mega puta" and complained about being chewed out for mispriced or misplaced merchandise. The employee claimed that two other co-workers also made supportive comments (he subsequently deleted the postings).

  At least one co-worker who viewed the employee's Facebook postings provided a printout to the store manager, who told the employee that his Facebook comments were slander and that he could be fired. The manager imposed a one-day paid suspension that precluded promotion opportunities for 12 months. She also prepared a discipline report stating that the employee had put bad things on Facebook about the employer and assistant manager and that the employee's behavior was not within company guidelines.

  The NLRB concluded that the employee's Facebook postings expressed an individual gripe and were not concerted. It found that they contained no language suggesting that the employee sought to initiate or induce co-workers to engage in group action—the postings expressed only his frustration regarding his individual dispute with the assistant manager over mispriced or misplaced items.

  Importantly, none of the co-workers' Facebook responses indicated that they had interpreted the employee's postings otherwise. The responses merely indicated that the co-workers had found the employee's first posting humorous, asked why the employee was so "wound up," or offered emotional support. The NLRB also found no evidence that established that the employee's postings were the logical outgrowth of prior group activity.

- An employee of a chain of home improvement stores used her cell phone during her break to update her Facebook status with a comment that consisted of an expletive and the name of the store. Four individuals, including one of her co-workers, "Liked" that status, and two other individuals commented on the status.

  About 30 minutes later, the employee posted again, this time commenting that the employer did not appreciate its employees. Although several of her friends and relatives commented on this second post, the four co-workers who were her Facebook friends did not respond. The employee was subsequently fired for her Facebook comments.

  The NLRB concluded that the postings were merely an expression of an individual gripe. The first status update was posted because the employee was frustrated about an interaction with her supervisor. She had no particular audience in mind when she made that post, the post contained no language suggesting that she sought to initiate or induce co-workers to engage in group action, and the post did not grow out of a prior discussion about terms and conditions of employment with her co-workers.

  The NLRB also pointed out the lack of evidence that she was seeking to induce or prepare for group action or to solicit group support for her individual complaint. Although one of her co-workers offered her sympathy and indicated some general dissatisfaction with her own job,

Beware the Employee Testimonial

Employees can hurt you with their social media activity despite having the best of intentions—like when an employee uses Twitter to heartily endorse your products.

Such testimonials will likely run head-on into the FTC's *Guides Concerning the Use of Endorsements and Testimonials in Advertising*. The guides address endorsements by consumers, experts, organizations, and celebrities as well as the disclosure of important connections between advertisers and endorsers.

Under the guidelines, if a connection exists between an endorser and the seller of an advertised product that might materially affect the weight or credibility of the endorsement (because the connection is not reasonably expected by the audience), the connection must be fully disclosed.

For example, say your company manufactures MP3 players, and one of your employees posts enthusiastic messages promoting your products on a Facebook page or Twitter account designated for discussions of new music download technology. Knowledge of the employee's job would probably affect the weight or credibility of her endorsement. The employee, therefore, must clearly and conspicuously disclose her relationship to the company to readers of the page or account.

that co-worker did not engage in an extended discussion with the employee over working conditions or indicate interest in taking action with her.

Whistleblower protections

Federal and state whistleblower laws might protect employees who complain online about company conditions affecting public safety and health or report potential violations of securities laws. The federal Sarbanes-Oxley Act, for example, prohibits employers from firing employees for providing information—or causing information to be provided—that assists an investigation of any conduct the employees reasonably believe violates certain securities laws.

In California, Labor Code Section 1102.5 prohibits employers from retaliating against an employee for disclosing information to a government or law enforcement agency if the employee has reasonable cause to believe the information discloses a violation of state or federal law. It's conceivable that the law could be triggered by discipline in response to a posting on social media.

Lawful off-duty activity

California law restricts employers' right to demote, suspend, or discharge an employee for certain lawful conduct that occurs during nonworking hours and away from the employer's premises. You might get away with firing an employee for conduct portrayed in his profile if the conduct was illegal (say, underage drinking), but even illegal conduct could be protected in some situations.

For example, state law prohibits employers from excluding individuals from employment based solely on most marijuana convictions that are more than two years old, or arrests that did not end in conviction or referral to or participation in a criminal diversion program, such as a work program as part of probation.

Political activities/affiliations

The Labor Code prohibits employers from making, adopting, or enforcing a rule, regulation, or policy that: 1) forbids or prevents employees from engaging or participating in politics, or 2) controls or directs employees' political activities or affiliations. You also can't attempt to influence employees to adopt or refrain from adopting a particular course of political action by threatening discharge. Taking disciplinary action against an employee for online political activity or speech could violate these laws.

Social Media Policy Dos and Don'ts

A policy regulating employee use of social media is essential to minimizing liability and potential damage to your company's reputation and operations. No single policy will work for every employer—the right policy depends on numerous factors, including the company's culture and how the company uses social media as part of its work. For example, some employees may be expected to use social media as part of their jobs.

Critical components

In general, most social media policies should address the following:

- the definition of "acceptable use" (Which sites or tools can be used at work? Who can use them? For what purpose? When?)
- the type of work-related information that can and cannot be discussed
- discriminatory or harassing statements and activity
- proprietary and confidential information
- the use of logos and similar brand identity
- disclaimers (that opinions are an employee's and not the employer's)
- disclosure of connections
- LinkedIn usage (A manager's LinkedIn recommendation of a terminated employee could support a wrongful termination claim.)

- the level of privacy employees can expect regarding their computers, email, and Internet use (If monitoring will occur, disclose that.)
- the consequences of violating the policy (discipline up to and including termination)

It's a good idea to encourage civility, common sense, good judgment, and an awareness of legal issues like copyright, defamation, and invasion of privacy. These reminders can protect both you and your employees.

Include the social media policy in your employee handbook and reinforce it with paycheck and email reminders. Require all employees to sign an acknowledgement form on first receipt as well as when they receive updates.

NLRA implications

Besides addressing specific disciplinary actions based on employee social media activity, the NLRB has found fault with several underlying social media policies. In fact, the NLRB has ruled against the policies in some cases despite finding that the particular activity at issue wasn't protected by the NLRA.

As of our print date, the NLRB has released two reports describing the social media cases it has reviewed. The most recent report, issued this past January, emphasized that "employer policies should not be so sweeping that they prohibit the kinds of activity protected by federal labor law, such as the discussion of wages or working conditions among employees."

For example, the NLRB has taken issue with policies that prohibited employees from:

- making disparaging remarks when discussing the company or the employee's superiors, co-workers, and/or competitors
- engaging in inappropriate discussions about the company, management, and/or co-workers
- depicting the employer in any way online without prior company permission
- posting pictures of themselves in any media, including the Internet, that depict the company in any way, including in a company uniform, corporate logo, or company vehicle
- using any social media that may violate, compromise, or disregard the rights and reasonable expectations as to privacy and confidentiality of any person or entity
- making a communication or post that constitutes embarrassment, harassment, or defamation of the employer or any employee, officer, board member, representative, or staff member

Before You Monitor Your Employees' Online Activity ...

Many employers have implemented computer usage and similar policies that incorporate monitoring of their employees' electronic communications on employer-provided equipment and technology. Monitoring might seem like a no-brainer, but you should keep in mind some caveats before engaging in the practice.

To begin with, the Federal Wiretap Act and the Electronic Communications Privacy Act of 1986 impose criminal and civil penalties against any person (including an employer) who intentionally intercepts an electronic communication, with certain exceptions. That means you must respect the privacy controls in your employees' social media accounts. If you try to circumvent them, you could violate the law as well as the website's terms of service.

Employers that intend to use electronic devices to monitor employees should obtain advance written authorization from each employee to avoid violating privacy rights and criminal laws. You may also want to obtain signed acknowledgements of the monitoring policy.

Finally, while courts have upheld employee monitoring, they typically expect employers to restrict the monitoring to legitimate work-related purposes.

- revealing—including through the use of photos—personal information regarding co-workers, company clients, partners, or customers without their consent
- using the company name, address, or other information on their personal profiles

What were the NLRB's objections to these prohibitions? In a nutshell, the policies violated the NLRA because they were overly broad:

- Policies that prohibit "disparaging" or "inappropriate" remarks when discussing the employer or related parties, without any limiting language, would prohibit protected criticism of the employer's labor policies, treatment of employees, and terms and conditions of employment. This is particularly the case if the policy doesn't define broad terms like "inappropriate," "personal," "private," "confidential," and "embarrassment" using specific examples or limiting the terms in any way that would exclude NLRA Section 7 activity.

- Policies that prohibit employees from posting photos that depict their employer, its logo, and the like could also prohibit an employee from engaging in protected activity. For example, an employee would be barred from posting a photo of employees carrying a picket sign with the employer's name.
- Policies that prohibit the use of the company name, address, or other information on employee's personal profiles—if intended for the legitimate purpose of preventing disclosure of certain protected company information to outside parties—must be narrowly drawn to address those interests. Because of the function that personal profiles serve in letting employees use a social network to find and communicate with their co-workers, such a prohibition could be especially harmful to NLRA rights if not narrowly drawn.

It's worth noting, though, that the NLRB took no offense with an employer's rule that precluded employees from pressuring their co-workers to connect or communicate with them via social media. The NLRB found that the rule was sufficiently specific in its prohibition and clearly applied only to harassing conduct. The rule couldn't be reasonably interpreted to apply more broadly to restrict employees from attempting to friend or otherwise contact colleagues for the purposes of engaging in protected activity.

Here's the takeaway from these NLRB decisions:

- Don't use broad language such as prohibiting employees from making "inappropriate" or "disparaging" comments. Be more specific—for example, by banning harassing comments or the disclosure of information related to products in development.
- Clearly state that nothing in the social media policy is intended to restrict employees' right to discuss wages and working conditions or otherwise engage in protected activity.
- Narrowly tailor any restrictions to accomplish legitimate business purposes, like preventing harassment and discrimination and protecting company-owned intellectual property and confidential information.

Social Media Training

Even if your employees sign acknowledgements that they received a social media policy, that's no guarantee that they actually understand the policy or what it means as far as what they can and can't do online. Training is therefore a must.

Your social media training for all employees should cover:

- a primer on social media, including the different websites
- why a policy is necessary
- an overview of the policy
- what is and isn't allowed
- who is authorized to speak on the employer's behalf
- the use of disclaimers
- monitoring of online activity (if monitoring will occur)
- consequences for violating the policy

Additionally, you should train HR staff on how to properly use social media in their tasks, how misuse can lead to problems, and how to document that decisions are based on legitimate business reasons.

Conduct training on a regular basis to keep up with changes in the policy *and* social media itself. Depending on the demographics of your workforce, you might want to offer different versions of the training. For example, your Baby Boomer employees may need more extensive training on what exactly social media is than your Millennial employees. Younger employees, who feel little reluctance to post personal information on their unprotected profiles, might need more training on some of the risks of freely posting business-related information online.

1 *Triple Play Sports Bar*, NLRB No. 34-CA-012915, 2012

2 *Karl Knauz Motors, Inc. d/b/a Knauz BMW*, NLRB No. 13-CA-46452, 2011

3 *Hispanics United of Buffalo, Inc.*, NLRB No. 3-CA-227872, 2011

4 *American Medical Response of Connecticut, Inc. and International Brotherhood of Teamsters, Local 443*, NLRB No. 34-CA-12576, 2010

5 *Walmart*, NLRB No. 17-CA-25030, 2011

The Password Issue

Earlier this year, an uproar resulted after a media report that some employers are requiring job applicants to turn over the passwords to their social media accounts. As this report went to print, the California legislature was considering proposed legislation that addresses this issue head-on.

Assembly Bill 1844 would prohibit an employer from requiring an employee or applicant to disclose a user name or account password to access social media used by the employee or applicant.

The bill, proposed by Nina Campos (D-San Jose), has received support from a broad coalition, including the California Chamber of Commerce, the American Civil Liberties Union, and the American Federation of State County and Municipal Employees.

A similar bill, Senate Bill 1349, has been introduced on the Senate side.