A bank finds out its best trader is an extreme skier and makes a decision to fire that employee based on an assessment that he is an excessive risk-taker.

A young surgeon who is being considered for a promotion to chief of surgery posted pictures of his bachelor party that showed him to be a “party animal,” and he was not promoted.

Firing, not hiring or not promoting an employee because an employer does not like someone’s personality, hobbies or communications may be illegal, but the social media world, exponential growth of the Internet and the accessibility of inexpensive devices and technologies are making it easier for employers to do so regularly, while employees do not even realize their rights may have been violated. Employers can monitor and exploit employee communications anywhere at any time with few laws to stop them. Now, with third-party social media firms supplying this information to employers, the amount of personal data about employees is virtually unlimited, and biases go unchecked.

In addition to inappropriate monitoring, employers are investigating any information they can find on an employee outside the workplace. This includes psychological profiling of employees’ hobbies and behavioral traits in order to make decisions about their employment at every stage of the employment process: hiring, firing and promotion. Studies reveal this can lead to discrimination against employees, and the effect can be devastating to their careers. How employers get access to this information, and what access should be permissible, is currently being debated in legislatures and courts across the country.

Information Access and Risks

At no point in history have employers had more access to information about job applicants and employees than they do now. Some of this is benign, such as discovering a potential hire’s favorite musician through Spotify. Other information can be useful, such as evaluating someone’s experience as stated on their LinkedIn profile. But inherent in our hyper-public, transparent world is the risk for abuse and discrimination, raising legitimate questions about whether employer investigation and surveillance comply with the existing law or if those laws simply do not go far enough.

Employers can use big data populated with Facebook “Likes” to measure a potential hire’s behavioral tendencies or enlist companies like Social Intelligence Corp. to prepare “social media dossiers” on current and potential employees. But some companies have taken even more intrusive and Orwellian-steps by monitoring employee emails, Microsoft Lync activity, Internet-usage, GPS movements, key-strokes, and text messages. Some employers have gone so far as to implant RFID chips under their employees’ skin to monitor them.

While undoubtedly some of this information may be helpful, research has shown little correlation between more information and better employment decisions. In fact, the evidence suggests otherwise. A Carnegie Mellon University experiment using fake resumes and social media profiles sent to prospective employers revealed that employers that searched these profiles were less likely to interview candidates who publicly identified as Muslim than Christian. Similar studies have revealed that employers were more likely to interview applicants with Caucasian-sounding names than African-American-sounding names using resumes that were otherwise the same.

Employers have historically balanced their desires to know as much as possible about their current and future employees with this risk of dis-
cramination.\textsuperscript{11} The more information an employer gathers about their employees or potential hires, the greater the risk that an employer acts on or elicits information that runs afoul of various anti-discrimination statutes,\textsuperscript{12} as well as the Fair Credit Reporting Act (FCRA) and other state and local laws.\textsuperscript{13} Employers have long had regulatory and legal incentives to investigate employees, whether to avoid liability for a negligent hire\textsuperscript{14} or to comply with employees or potential hires, the greater the employer gathers about their employees.\textsuperscript{15} But recent regulatory expansion and the availability of personal information on the web have employers more willing than ever to take chances. 

Like the initial example of the high-risk trader, nowhere is this more pronounced than in finance, where regulations have incentivized employers to take significant risks in employment decisions. In the wake of the Dodd–Frank Wall Street Reform and Consumer Protection Act, financial services firms have experienced a massive increase in compliance-related inquiries and investigations. In an attempt to escape liability, many employers have distanced themselves from alleged wrongdoers by scapegoating employees. These not-so-transparent attempts to escape respondeat superior liability have contributed to the heightened focus on the employer’s role in hiring and supervising their employees.\textsuperscript{16}

While some state and federal laws prohibit using certain types of information as noted above, there are no federal laws that protect an employee from an employer’s use and abuse of information that is not related to employment and was intended as a recreational activity, such as social media communications. Some states, including Maryland and California, have prohibited employers from requiring or requesting their employees or job applicants to provide social media or password-protected websites.\textsuperscript{17} On the federal level, the Stored Communications Act and other similar laws\textsuperscript{18} limit an employer’s unauthor-

ized access to an employee’s personal email—but again, this is extremely narrow and limited because as long as an employee is accessing his or her information openly on an employer’s computer or employer-owned device, the employee may not have an expectation of privacy.\textsuperscript{19} Recent NLRB rulings provide additional protection that limit broad social media policies that stifle the association and communication of employees.\textsuperscript{20} 

Inherent in our hyper-public, transparent world is the risk for abuse and discrimination, raising legitimate questions about whether employer investigation and surveillance comply with the existing law.

New York has been slower to act. New York, like many other states,\textsuperscript{21} has proposed legislation, but has no existing law that protects employees from employers requesting passwords for employees’ personal social media or email accounts or limiting the access and use of employee information. New York’s proposed legislation would protect employees from employers asking for personal passwords on employees’ and prospective employees’ social media accounts\textsuperscript{22} and would prohibit employers or educational institutions from requesting user names or passwords for employee social media or personal accounts on certain electronic devices.\textsuperscript{23} The proposed regulations are a start in the right direction, but much more needs to be done to adequately protect employee privacy rights or to re-invigorate existing law and make it relevant to the new technological workplace.

New York has historically lacked any meaningful privacy protections for employees and has no general privacy law.\textsuperscript{24} It does, however, have an Off Duty Conduct Statute,\textsuperscript{25} (as many other states do),\textsuperscript{26} which could pave the way for legal changes and protections if it were to become more inclusive of social media as a “recreational activity” or recognized online communications published outside of work as “protected activity.” While the statute is flawed and the law has failed to protect plaintiff employees in more conventional cases it may be a starting place for change.\textsuperscript{27} 

\textbf{Off-Duty Conduct Law}

New York adopted the Off Duty Conduct Statute 20 years ago, which in many respects was inconsistent with its at-will employment history as it prohibited employers from taking an adverse employment action against employees or applicants for employment on the basis of their legal, off-duty conduct. Of course, when the law went into effect in 1993, social media did not even exist. Section 201-d of the Labor Law instead grew out of a national campaign by the tobacco lobby to prevent discrimination against employees who smoke.\textsuperscript{28} New York’s law, however, goes further and broadly protects employees from adverse employment actions, if the employee has engaged in legal off-duty activities without using company property or equipment.

Specifically, the law was meant to protect employees engaging in political activities, legal recreational activities (and non-compensated leisure time activities), using legal, consumable products, off company property and outside working time, and union membership or the exercise of rights related to union activity. It states that it is unlawful for an employer to “refuse to hire, employ or license, or to discharge from employment or otherwise discriminate against” an employee because of the employee’s protected activities.\textsuperscript{29}

Although social media sounds like it could fit neatly into this statute’s protected “recreational activity,” given how New York and federal courts have construed the statute, employees have modest protection. Judicial hostility toward the law appears rooted in its tobacco
New York has an Off Duty Conduct Statute, which could pave the way for legal changes and protections if it were to become more inclusive of social media as a “recreational activity” or recognized online communications published outside of work as “protected activity.”

Whether on social media sites or over dinner in a restaurant, off-duty communications and conduct should not be markets like California. Compare N.Y. EXEC. LAW 296(16), with CAL. LAB. CODE §201-d. See infra notes 9 and 10.

31. See infra notes 9 and 10.

32. As courts seem disinclined to extend the law’s reach into areas where employees might expect protection, including conventional areas such as dating, political activity, and even personal decisions regarding cohabitation.

33. Given its narrow construction, can this statute prohibit employers from gathering and using information that involves employee “recreational activities” thus protecting an an employer’s discharge action based on this activity? Could social media itself be a “recreational activity”? These questions remain largely unresolved. Aside from a recent case involving a blogger at a large financial institution, which settled before any judicial resolution, few cases have applied section 201-d to social media activity. But courts should be mindful that the law exists for a reason and that extending it to social media is not inconsistent with the law’s plain language, regardless of its origins.

Conclusion

As employees find new ways to stay connected, employers find new ways to literally track their every move. Whether or not New York’s Off-Duty Conduct Statute is rehabilitated, employees need protection in the workplace from employers prying into their social lives and stifling their communications and activities. If employees are worried about everything they do or put on Facebook, we will wind up with a society where our most basic freedoms are repressed and creativity stifled. Whether on social media sites or over dinner in a restaurant, off-duty communications and conduct should not be