New York Law Journal
SERVING THE BENCH AND BAR SINCE 1888
WWW.NYLJ.COM
An ALM Publication
VOLUME 254—NO. 03
TUESDAY, JULY 7, 2015

EMPLOYEES IN THE WORKPLACE

Expert Analysis

'1984' in 2015: Protecting Employees' Social Media From Misuse

• 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.

By **Wendi S. Lazar**

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.[1] 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.[2] Studies reveal this can lead to discrimination against employees,[3] 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[4] or enlist companies like Social Intelligence Corp. to prepare "social media dossiers" on current and potential employees.[5] But some companies have taken even more intrusive and Orwellian-steps by monitoring employee emails, Microsoft Lync activity,[6] Internet-usage, GPS movements, key-strokes, and text messages.[7] Some employers have gone so far as to implant RFID chips under their employees' skin to monitor them.[8]

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.[9] 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.[10]

Employers have historically balanced their desires to know as much as possible about their current and future employees with this risk of dis-

WENDI S. LAZAR *is partner and co-chair of the executives and professionals practice group at Outten & Golden.* ROBERT PHANSALKAR, *an associate at the firm, assisted in the research and writing of this column.*

crimination.[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,[12] as well as the Fair Credit Reporting Act (FCRA) and other state and local laws.[13]

Employers have long had regulatory and legal incentives to investigate employees, whether to avoid liability for a negligent hire[14] or to comply with government-contractor laws requiring a drug-free workplace.[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.[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.[17]

On the federal level, the Stored Communications Act and other similar laws[18] limit an employer's unauthorized 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.[19] Recent NLRB rulings provide additional protection that limit broad social media policies that stifle the association and communication of employees.[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,[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[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.[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.[24] It does, however, have an Off Duty Conduct Statute,[25] (as many other states do),[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.[27]

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.[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.[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

history and its apparent contradiction with employment at will.[30] As a result, courts seem disinclined to extend the law's reach into areas where employees might expect protection, including conventional areas such as dating,[31] political activity,[32] 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 adverse employment 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.[34] 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 fodder for adverse employment actions. Because this information is accessible, without clear penalties to an employer who overreaches into an employee's personal life, there is disincentive to curtail the practice.

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."

1. For a comprehensive discussion on employer surveillance tactics, see Corey A. Ciocchetti, "The Eavesdropping Employer: a Twenty-First Century Framework for Employee Monitoring," 48 AM. BUS. L.J. 285 (2011).
2. See infra note 4.
3. See infra notes 9 and 10.
4. See Anna North, "How Your Facebook Likes Could Cost You a Job," N.Y. TIMES (Jan. 20, 2015, 10:01 AM), http://optalk.blogs.nytimes.com/2015/01/20/how-your-facebook-likes-could-cost-you-a-job/.
5. See Jennifer Preston, "Social Media History Becomes a New Job Hurdle," N.Y. TIMES (July 20, 2011), http://www.nytimes.com/2011/07/21/technology/social-media-history-becomes-a-new-job-hurdle.html; see also Number of Employers Passing on Applicants Due to Social Media Posts Continues to Rise, According to New CareerBuilder Survey, CareerBuilder (June 26, 2014), http://www.careerbuilder.com/share/aboutus/pressreleasesdetail.aspx?sd=6%2F26%2F2014&id=pr829&ed=12%2F31%2F2014.
6. Tim Greene, "Microsoft Lync Gathers Data Just Like NSA Vacuums up Info in Its Domestic Surveillance Program," NETWORK WORLD (Feb. 20, 2014, 9:15 AM), http://www.networkworld.com/article/2175369/uc-voip/microsoft-lync-gathers-data-just-like-nsa-vacuums-up-info-in-its-domestic-surveillance-progr.html.
7. Ciocchetti, supra note 1.
8. Rory Cellan-Jones, "Office Puts Chips under Staff's Skin," BBC News (Jan. 29, 2015), http://www.bbc.com/news/technology-31042477.
9. Allesandro Acquisti and Christina M. Fong, "An Experiment in Hiring Discrimination Via Online Social Networks," (Oct. 26, 2014) (unpublished manuscript) (on file with the Social Science Research Network).
10. Marianne Bertrand and Sendhil Mullainathan, Are Emily and Brendan More Employable than Lakisha and Jamal? A Field Experiment on Labor Market Discrimination (Nat'l Bureau of Econ. Research, Working Paper No. w9873, 2003), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=428367.
11. See, e.g., Gregory M. Saylin and Tyson C. Horrocks, The Risks of Pre-employment Social Media Screening, SOC'Y FOR HUMAN RES. MGMT. (July 8, 2013), http://www.shrm.org/hrdisciplines/staffingmanagement/articles/pages/preemployment-social-media-screening.aspx.
12. See, e.g., Title VII of Civil Rights Act of 1964, as amended, 42 U.S.C. §2000e et seq.; the Genetic Information Nondiscrimination Act of 2008 (GINA), 42 U.S.C.A §2000ff-1 (2010); the Americans with Disabilities Act (ADA) Amendments Act of 2008, 42 U.S.C. §12101, et seq.; see also Equal Employment Opportunity Commission, EEOC Enforcement Guidance on Disability-Related Inquiries and Medical Examinations of Employees Under the Americans with Disabilities Act (July 27, 2000).
13. 15 U.S.C. 1681 et seq.; but see *Sweet v. LinkedIn Corp.*, No. 5:14–cv–04531–PSG, 2015 WL 1744254 (N.D. Cal. April 14, 2015) (holding that LinkedIn is not a consumer reporting agency under the FCRA). Several state laws also protect against these abuses, but New York generally lags behind comparable markets like California. Compare N.Y. EXEC. LAW 296(16), with CAL. CIV. CODE §1786 et seq.
14. See, e.g., *Kelly G. v. Bd. of Educ. of City of Yonkers*, 99 A.D.3d 756 (2d Dept. 2012).
15. 41 U.S.C. §8102, et seq.
16. Proposed regulations for the Financial Industry Regulatory Authority (FINRA) highlight the concern. Under proposed FINRA Rule 3110(e), which takes effect July 1, 2015, member firms will be required to investigate applicants registering with FINRA. Although Rule 3110(e) requires member firms to follow the law while conducting these investigations, FINRA has incentivized them to push the boundaries.
17. MD. CODE ANN., LAB. & EMPL. §3-712; CAL. LAB. CODE §980.
18. 18 U.S.C. 2701–11.; see also the Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. §2510, et seq.
19. Compare *Levanthal v. Knapek*, 266 F.3d 64, 74 (2d Cir. 2001) (holding that employer's unclear policy regarding monitoring of computers established a reasonable expectation of privacy) with *Muick v. Glenayre Elec.*, 280 F.3d 741, 743 (7th Cir. 2002) (no reasonable expectation of privacy in workplace computer files where employer had announced that he could inspect the computer).
20. See, e.g., *Triple Play Sports Bar and Grille*, Nos. 34-CA-012915, 34-CA-012926 (NLRB Aug. 22, 2014) (holding that Facebook "likes" can be a concerted activity)); *Hispanics Utd. of Buffalo & Carlos Ortiz*, No. 03-CA-027872 (NLRB Dec. 14, 2012) (holding that Facebook activity can be concerted activity if other employees participate and discuss work conditions); but see *Karl Knauz Motors and Robert Becker*, No. 13-CA-46452 (Sept. 28, 2011) (holding that employee activity must be concerted and discuss work conditions to be protected).
21. National Conference of State Legislatures, Access to Social Media Usernames And Passwords, http://www.ncsl.org/research/telecommunications-and-information-technology/employer-access-to-social-media-passwords-2013.aspx (last visited April 8, 2015).
22. Assemb. B. 2891, 2015-2016 Reg. Sess. (N.Y. 2015); S.B. 3927, 2015-2016. Reg. Sess. (N.Y. 2015).
23. Assemb. B. 4388, 2015-2016 Reg. Sess. (N.Y. 2015).
24. See *Mack v. U.S.*, 814 F.2d 120, 123 (2d Cir. 1987).
25. N.Y. LAB. LAW §201-d.
26. See also COLO. REV. STAT. §24-34-402.5; N.D. CENT. CODE §14-02.4-08; CAL. LAB. CODE § 98.6; CAL. LAB. CODE §96(K).
27. For further discussion regarding section 201-d and specifically its application to social media, see Karlee S. Bolaños and Kyle W. Sturgess, "Will Lifestyle Discrimination Statutes Protect Employee Social Media Use?" NYLJ (March 28, 2011).
28. See National Conference of State Legislatures, Discrimination Laws Regarding Off-Duty Conduct, http://www.ncsl.org/documents/employ/off-dutyconductdiscrimination.pdf (last updated Oct. 18, 2010).
29. Unfortunately, while the law gives employees a private right of action, the statute does not provide for recovery of attorney fees by a prevailing plaintiff and has some major exceptions to its scope. This includes its application to professional journalists and civil servants who are prohibited by law from engaging in political activity—activity that "creates a material conflict of interest related to the employer's trade secrets, actions that involve an employer's proprietary or business information, activity related to certain collective bargaining agreements or personal service contracts with a professional employee; and actions where there was a reasonable belief that the action is "required by statute, regulation, ordinance, or other governmental mandate." N.Y. LAB. LAW §201-d.
30. *McCavitt v. Swiss Reinsurance Am. Corp.*, 89 F.Supp.2d 495, 498 (S.D.N.Y. 2000) aff'd, 237 F.3d 166 (2d Cir. 2001) (discussing tobacco lobby's role in §201-d).
31. *New York v. Wal-Mart Stores*, 207 A.D.2d 150 (2d Dept. 1995) (holding that employer may fire employees where company policy prohibited employees from dating because dating is not a "recreational activity" under §201-d).
32. *Wehlage v. Quinlan*, 55 A.D.3d 1344 (4th Dept. 2008) (failing to extend §201-d to activities that did not fall under specifically enumerated categories in statute).
33. *Bilquin v. Roman Catholic Church, Diocese of Rockville Ctr.*, 286 A.D.2d 409 (2d Dept. 2001) (holding that an employer may fire an employee for cohabiting with a man who is married to another woman because such activity is not a "recreational activity" under §201-d).
34. *Tagocon v. J.P. Morgan Chase*, No. 10116415, complaint filed (N.Y. Sup. Ct. Dec. 20, 2010) (case was removed to federal court and settled after mediation).