2014

In Defense of Snooping Employers

Jessica Fink
California Western School of Law, jfink@cwsl.edu

IN DEFENSE OF SNOOPING EMPLOYERS

Jessica K. Fink*

In recent months, a plethora of states have turned their legislative attention to protecting employee privacy in the workplace, focusing specifically on passing state laws that protect the "social media privacy" of individuals in their states. Indeed, discussions of workplace privacy are everywhere nowadays: Media stories condemn employers' efforts to monitor their employees' email, Internet, and telephone usage. Employees rage about perceived invasions of their privacy. Politicians heatedly debate how to limit employers' prying conduct, passing laws designed to reign in certain types of monitoring by employers. At the same time, employers also find themselves perplexed as they grapple with how they can gather the information that they need to make important business decisions within an environment that views such efforts with disdain. In a world where technological advancements have made it easier than ever to collect massive amounts of information about those in the workforce and where employers feel an increasing need to collect such information, looming questions remain regarding the proper scope and limits of employees' privacy.

This Article represents one effort to answer these questions while taking the employers' perspective into account, explaining both the motivations behind and justifications for employers' efforts to "snoop" into their employees' private lives. The Article describes the means through which employers gather information about their employees, including through some recent, rather novel approaches to collecting such data. In addition, this Article discusses the financial, legal, and practical concerns that motivate employers to snoop in the first place, arguing that employers engage in this conduct for what frequently amount to very legitimate reasons. More significantly, this article places substantial responsibility for employer snooping with the courts themselves, highlighting particular decisions and doctrines that not only permit, but in fact encourage, employers to engage in these efforts to monitor employees.

At bottom, this paper attempts to put the "problem" of employer snooping into a broader context. While employers certainly should not have access to every aspect of their prospective and current employees' private lives, and while abuses of the boundaries undoubtedly exist, much of the snooping behavior for which employers have been condemned

represents more than just senseless meddling, but rather is part of a sound business plan designed to protect employers, employees, and the public at large.

INTRODUCTION

In February 2013, three members of Congress introduced legislation aimed at barring employers from requiring or requesting that any employee or prospective employee provide an employer with a username, password,

or other means of accessing a private email or social media account.[1] This federal law, coming on the heels of similar legislation passed in at least ten states[2] and pending in many others,[3] has been characterized as "vital to preventing employer requests for personal accounts becoming routine."[4] In the same vein, employees in recent years increasingly have complained about other types of alleged intrusions by employers – intrusions involving everything from the monitoring of telephone and email communications, to the use of global position systems (GPS) to track employees' whereabouts, to the application of sophisticated technology that can record virtually every keystroke made by an employee on his/her employer-owned computer.[5]

At first blush, the outrage expressed by both workers and the public regarding this type of employer conduct seems understandable, even predictable: What possible reason might an employer have for needing to delve into an employee's social media account? Why must an employer know the precise location of an employee at every moment of the workday? Should there not be some areas of an employee's life that can remain "private," safe from employer intrusion, even if such areas touch upon workplace activities? Given that employers' efforts to monitor employees show no signs of abating, and given that the technological means for engaging in such monitoring are only becoming more

---

* Associate Professor, California Western School of Law. J.D., Harvard Law School, 2001; B.A., University of Michigan, 1997. I am grateful to Professor Orly Lobel and the students in her Work, Welfare and Justice Seminar at the University of San Diego School of Law for their helpful suggestions with respect to this paper. Finally, many thanks to Camille Gustufson for her excellent research assistance.

1. *Social Networking Online Protection Act ("SNOPA")*, H.R. 537, 113th Cong. (2013). *See also* Michael O. Loatman, *Congress May Limit Employer Access To Personal Social Media Accounts,* DAILY LAB. REP., Feb. 11, 2013 (describing the implications of the new legislation). This actually was the second time that members of Congress had attempted to pass legislation of this nature. Previous bills, similarly aimed at limiting employers' access to prospective and current employees' email and social media account credentials, were introduced in both the House and the Senate in spring 2012 but failed to garner sufficient support to become law. *See id.*; *see also* Lance Whitney, *Democrats to employers: Stop asking for Facebook passwords*, CNET, (May 10, 2012), http://news.cnet.com/8301-1009_3-57431724-83/democrats-to-employers-stop-asking-for-facebook-passwords/ (describing a bill that seeks to stop employers from asking employees for their personal passwords to online accounts).

2. *See infra* note 93.

3. *See* Jean Eaglesham & Michael Rothfeld, *Wall Street vs. Its Employees' Privacy*, WALL ST. J. (Apr. 22, 2013), http://online.wsj.com/article/SB10001424127887323551004578436713224083592.html (highlighting states' efforts to adopt social-media privacy laws).

4. *See* Loatman, *supra* note 1.

5. *See* Robert Sprague, *Orwell was an Optimist: The Evolution of Privacy in the United States and its De-Evolution for American Employees*, 42 J. MARSHALL L. REV. 83, 84 (2008) (critiquing the lack of employee privacy).

sophisticated every day, the answers to questions like these will grow to be increasingly more pressing in the months and years to come.

This Article attempts to provide one response to this important set of questions, explaining both the motivations and justifications for this type of "snooping" behavior by employers. The Article not only describes the mechanisms typically adopted by employers to gather information about prospective and current employees, but also argues that such intrusions by employers in many cases are reasonable – and indeed, even prudent. This Article will begin in Part I by providing some history and context to the issue of employee workplace privacy, reviewing some of the relevant rights and responsibilities of employers with respect to employee privacy. Among other things, the Article will describe the very limited privacy rights that are available to employees, particularly for those who work in the private sector. In Part II, this Article will discuss the methods used by employers to gather information about employees, and will describe how various restrictions on conventional methods of information gathering have led to the evolution of more unusual – and arguably more intrusive – means of monitoring employees. While this section will generally describe a host of tools currently used by employers to gather information about prospective and current employees, it will pay particular attention to the recent flurry of attention surrounding employer requests for individuals' social media passwords. In Part III, this Article will explain why employers are more motivated than ever to engage in snooping behavior, laying out the financial, legal, and practical concerns that render it logical – and even advisable – for employers to snoop. In Part IV, this argument extends one step further, with a discussion of the role that the courts (including the U.S. Supreme Court) have played in permitting, and even *encouraging*, employers' efforts to monitor employees. Finally, in Part V, the Article will propose some limits on employers' right to snoop, articulating some responsibilities that employers should have when engaging in any monitoring of prospective or current employees.

At bottom, this Article sets out to put the alleged "problem" of employer snooping in a more informed context and to show that it is not the dilemma that many represent it to be – at least, not one that requires the heightened level of legislative attention and media hype that has emerged in recent months and years. While abuses of employee privacy unquestionably exist, employers by and large are not encroaching unreasonably into their employees' private lives. Employers gather information about prospective and current employees not out of some prurient desire to delve into the personal and private aspects of their lives, but rather out of an informed, careful, and logical consideration of the risks associated with *not* acquiring such information. While advances in technology have expanded employers' ability to snoop, employers' actions

in large part have been tailored to their legitimate needs.

I. THE LIMITED RIGHT TO PRIVACY IN A PRIVATE SECTOR WORKPLACE[6]

Any discussion of workplace privacy should begin with an understanding of one key idea: Employees in the modern American workplace possess extremely limited privacy rights.[7] Regardless of the specific workplace setting, employers generally possess broad latitude to scrutinize the background of potential employees and to monitor details of current employees' behavior.[8] Employers may launch thorough investigations into the qualifications of a job applicant, using a host of psychological and other tests; they may conduct extensive background checks on a potential employee; they may run Internet searches to learn as much as possible about a potential new hire.[9] With respect to current

6. While this article focuses on employer snooping within the private sector, many of the ideas discussed herein would apply with equal force to public sector employees. Public sector employees possess somewhat greater privacy rights than their private sector counterparts due to application of constitutional protections to their employers' conduct. *See* Pauline T. Kim, *Electronic Privacy and Employee Speech*, 87 CHI.-KENT L. REV. 901, 906 (2012) (noting that private sector employees generally cannot rely upon constitutional rights to being a privacy claim, but rather must turn to a common law privacy tort). However, the privacy rights of even public sector employees still are fairly limited in scope. *See generally* Paul M. Secunda, *Privatizing Workplace Privacy*, 88 NOTRE DAME L. REV. 277 (2012) (discussing how a heightened sense of privacy for public sector employees has become less certain in light of recent case law, including *City of Ontario v. Quon*); *cf.* Sheila A. Bentzen, *Safe for Work? Analyzing the Supreme Court's Standard of Privacy for Government Employees in Light of City of Ontario v. Quon*, 97 IOWA L. REV. 1283, 1286 n.5 (2012) (internal quotation marks omitted) (noting that "[p]ublic employees' privacy interests are not necessarily different from those of private employees, but the public employment relationship is governed by certain bodies of law, most notably the Constitution, that do not apply to the private sector").

7. *See* Sprague, *supra* note 5, at 84 (stating that "[e]mployees have virtually no privacy"); *see also id.* at 89 (citing the "near extinction" of privacy rights for employees); *see e.g.* Lindsay Noyce, *Private Ordering of Employee Privacy: Protecting Employees' Expectations of Privacy with Implied-in-Fact Contract Rights*, 1 AM. U. LAB. & EMP. L. F. 27, 27 (2011) (noting that "[e]mployees, perhaps irrationally, often overestimate the amount of privacy they should expect in technological communication").

8. *See* Sprague, *supra* note 5, at 84 ("The employer has the potential to be Big Brother, always watching, listening, and recording."); *see also* Boris Segalis, *Employee Privacy Gains in the United States*, INFO. LAW GRP. (Jan. 13, 2011), http://www.infolawgroup.com/2011/01/articles/enforcement/employee-privacy-gains-in-the-united-states/ (noting that "[t]raditionally, in the U.S., employees have enjoyed little privacy in the workplace. With respect to workplace communications, for example, employees generally are deemed not to have 'a reasonable expectation of privacy.' With some limitations, this allows employers to freely monitor and review employee communications").

9. *See* Sprague, *supra* note 5, at 84 (enumerating the monitoring and screening tools

employees, employers examine everything from employees' Internet, telephone, and email usage, to the keystrokes that they enter into their computers, to the coworkers with whom they socialize, to the number and length of the bathroom breaks that they take throughout the day.[10] As one commentator in this area has observed: "What is allowed to be monitored and what can be done with the monitoring . . . ? The answer seems to be that an employer can monitor virtually anything, and almost anything can be done with it."[11]

While employers do enjoy relative freedom to snoop into the private lives of potential and current employees, there is a hodgepodge of federal and state laws (and, in some limited cases, constitutional provisions[12]) that establish some boundaries for employers in this context.[13] The primary federal law that impacts employee privacy in the workplace is the Electronic Communications Privacy Act of 1986 (ECPA),[14] which consists of two parts: the Wiretap Act (Title I)[15] and the Stored Communications Act (Title II).[16] The Wiretap Act has a rather limited application to

---

that are available and used by employers for both applicants and current employees, ranging from video and electronic surveillance to internet tracking and keylogging).

10. *Id.*

11. Karin Mika, *The Benefit of Adopting Comprehensive Standards of Monitoring Employee technology Use in the Workplace*, CORNELL HR REV. (Sept. 22, 2012), http://www.cornellhrreview.org/the-benefit-of-adopting-comprehensive-standards-of-monitoring-employee-technology-use-in-the-workplace/.

12. *See generally* Kim, *supra* note 6 (citing the Fourth Amendment protection against unreasonable search and seizure); Secunda, *supra* note 6 (noting the Fourth Amendment guarantee for public employees); Bentzen, *supra* note 6 (discussing constitutional provisions impacting employees' right to privacy).

13. For a more thorough summary of the current state of the law in this area, including the privacy protections proposed in the RESTATEMENT (THIRD) OF EMP'T LAW (Tentative Draft No. 6, 2013), see Secunda, *supra* note 6 (discussing developments in employment privacy law, including under the context of a newly drafted Chapter 7 of the RESTATEMENT); *see also* Corey A. Ciocchetti, *The Eavesdropping Employer: A Twenty-First Century Framework for Employee Monitoring*, 48 AM. BUS. L. J. 285, 290-301 (2011) (discussing the indirect ways in which the legal system provides for employee privacy); *Sprague*, *supra* note 5, at 93-111 (noting that the "legal right to privacy in the United States" is provided in the "common law, constitutional law, and federal statutes."); Jill L. Rosenberg, Conference Presentation, *Is Big Brother Watching: Monitoring Employee Communications and Employee Privacy*, AM. BAR ASS'N LABOR AND EMPLOYMENT LAW CONFERENCE, 409 (2011), http://www.americanbar.org/content/dam/aba/administrative/labor_law/meetings/2010/annualconference/171.authcheckdam.pdf (discussing theories used in privacy rights litigation, while providing and suggesting procedures that can be used by employers to minimize belief among employees that their privacy rights are being violated according to the laws of both federal and selected state jurisdictions);

14. Electronic Communications Privacy Act of 1986 (ECPA), Pub. L. No. 99-508, 100 Stat. 1851, 1859 (codified as amended at 18 U.S.C. §§ 2510-2511 (2006)).

15. *Id.* at § 2511(1).

16. *Id.*at § 2701.

concerns regarding employee workplace privacy, since it prohibits only the interception of electronic communications *while in transmission*.[17] Most modern communications only are "in transmission" for a matter of seconds, minimizing the opportunities for interception.[18] The Stored Communications Act, however, has a more significant application to workplace monitoring, since it prohibits unauthorized access to communications while in electronic storage.[19] Indeed, in enacting the Stored Communications Act, Congress' intent was to provide protection to individuals' emails and text messages[20] – both of which represent fertile areas of employer monitoring.[21]

Despite these protections, however, the ECPA contains several significant exceptions that allow for employer monitoring under certain circumstances: Under the "consent exception," an employer can engage in monitoring if one of the parties to a communication consents to monitoring.[22] Under the "course of business exception," an employer can engage in monitoring that occurs in its normal course of business, such as by intercepting phone calls on telephone equipment used in the employer's ordinary course of business.[23] Under a third exception, the "provider exception," an employer that provides wire or electronic communications services can retrieve information stored on its system, if such access is necessary to protect its rights as the provider of this electronic service.[24] Thus, an employer that provides an email or voicemail system to its employees can, under this exception, freely access information from that voicemail or email system.

---

17. *See* Ciocchetti, *supra* note 13, at 291-93 (discussing the applicability of the Wiretap Act and noting that the vast majority of modern electronic communications are only considered to be "in transmission" for mere seconds prior to arrival at their final destinations).

18. *Id.*

19. *See* 18 U.S.C. § 2701(a) (2006) (stating that an individual who intentionally accesses a "wire or electronic communication while it is still in electronic storage in such a system" will be subject to punishment).

20. *See* Rosenberg, *supra* note 13, at 438 (observing that "Congress enacted the ECPA to make the already existing Federal Wiretap Act . . . applicable to newly emerging communication devices"); *see also* Ciocchetti, *supra* note 13,, at 291-92 (stating that "[t]he ECPA was intended to extend privacy protection from wire communications such as telephone calls, to electronic communications such as e-mails and text messages").

21. *See infra* note 56.

22. *See* Ciocchetti, *supra* note 13, at 293 (listing exceptions to the ECPA).

23. *See id.* (listing exceptions to the ECPA); *see also* Sprague, *supra* note 5, at 116-17 (stating that a business use exception to the Act exists, where employers are allowed to monitor calls for "telephone equipment used in the ordinary course of business").

24. *See* Ciocchetti, *supra* note 13, at 293 (noting that exceptions exist under multiple conditions, including consent, course of business, and "exception for employers that access stored information, if such access is necessary to protect its rights or property as the provider of the electronic service").

A second federal statute that might impact employer monitoring at work is the Computer Fraud and Abuse Act ("CFAA"),[25] which prohibits "knowingly access[ing] a computer without authorization or exceeding authorized access."[26] The CFAA, however, is not likely to apply to employee monitoring in any significant way. Most courts interpreting this statute have held that the scope of an individual's authorization to access a computer network should be analyzed according to "expected norms of intended use."[27] Because most employers are authorized to access computer networks that are their own property, this statute more typically applies "when employees or competitors hack into an employer's system to discover confidential information."[28]

In addition to these federal statutory protections (as well as legislative efforts by some states),[29] common law "invasion of privacy" principles also might provide some protection against employer intrusions. Employees may bring a tort claim alleging an unlawful "intrusion upon seclusion" by showing that an employer intruded into "a place or property where [the employee possessed] a reasonable expectation of privacy," and by establishing that this intrusion "would be highly offensive to a reasonable person."[30] Many employees, however, may have difficulty showing a *reasonable* expectation of privacy in areas monitored by their employer, particularly where monitoring takes place on or within the employer's property.[31] Indeed, courts will find liability for an intrusion upon seclusion

25. 18 U.S.C. § 1030 (2006) (outlining the circumstances that constitute an unauthorized use of a computer and detailing the consequences for an individual who is in violation of the CFAA).

26. *See id.* (defining what constitutes a violation of the CFFA).

27. Ciocchetti, *supra* note 13, at 294 (internal quotation marks omitted) (noting the difficult balance that employers must maintain between protecting the interests of their company and ensuring the privacy of employees and noting the response of the American legal system to this issue, explaining the context and implications for acts such as the CFFA).

28. *Id.* One additional source of statutory protection for employees can be found in Section 7 of the National Labor Relations Act (NLRA). *See* 29 U.S.C. § 157 (2006) (stipulating that employers may not interfere with employees' right to engage in concerted activities). Some have argued that certain types of surveillance by an employer constitute this type of unlawful interference because such conduct might "chill" employees' exercise of their right to engage in concerted activities. *See supra* notes 15-16 (prohibiting the interception of and access to certain communications).

29. *See, e.g.*, Ciocchetti, *supra* note 13, at 294-98 (describing analogous state legislation).

30. *See id.* at 299 (describing how employees can use common law and "invasion of privacy" torts as some protection against employer monitoring); *see also* Secunda, *supra* note 6, at 294-95 (internal quotation marks omitted) (explaining the elements of intrusion upon seclusion).

31. *See* Ciocchetti, *supra* note 13, at 300 (describing how the court may have applied the RESTATEMENT to the *Trotti* case.).

tort only where an employer invades very private locations, such as employee locker rooms or restrooms.[32] Accordingly, the common law – like its statutory counterparts – remains of minimal use to employees seeking protection from employer prying.[33]

II. PRACTICAL AND LEGAL HURDLES AFFECTING EMPLOYERS' ABILITY TO SNOOP

As noted above, the "right to privacy" at work exists as a rather illusory right, particularly for private sector workers. Employers possess significant latitude when it comes to gathering information about both prospective and current workers. This freedom to snoop, however, is not without any limits: While employers, in theory, possess an unfettered right to poke around in their employees' private lives, various practical and legal obstacles may hinder employers' ability to use certain methods of gathering information.

A. Limits Associated with Traditional Tools for Information Gathering

Employers face several restrictions with respect to their ability to research the backgrounds of both prospective and current employees, including limitations with respect to methods that traditionally have been used in the workplace. For example, while popular media frequently depicts the polygraph (i.e., lie detector) test as a common method of testing an individual's veracity, the federal Employee Polygraph Protection Act of 1988 effectively bars employers from using a polygraph test to screen either job applicants or current employees, except in very limited situations.[34] Similarly, while employers may want information regarding a

32. *Id.* at 301.

33. RESTATEMENT (THIRD) OF EMP'T LAW (Tentative Draft No. 6, 2013) also proposes some privacy protections for private sector workers, including a newly named tort of "wrongful employer intrusion upon [a] protected employee privacy interest." *See* Secunda, *supra* note 6, at 295-96 (noting and detailing the changes in RESTATEMENT (THIRD) OF EMP'T LAW (Tentative Draft No. 6, 2013) recognizing wrongful employer intrusion and defining it).

34. *See* Ian Byrnside, *Six Clicks of Separation: The Legal Ramifications of Employers Using Social Networking Sites to Research Applicants*, 10 VAND. J. ENT. & TECH. L. 445, 451 (2008) (noting that employers are increasingly monitoring job applicants' social media pages and observing that this leads to a gray area of the law, as employers have previously had legal ramifications for using certain methods to investigate an applicant's criminal history or financial status, using the EPPA as an example.); *see also* Stephen F. Befort, *Pre-Employment Screening and Investigation: Navigating Between a Rock and a Hard Place,* 14 HOFSTRA LAB. & EMP. L.J. 365, 401-02 (1997) (noting that more than half of all states have enacted statutes similar to the Employee Polygraph Protection Act, many with restrictions

potential or current employee's drug usage or medical status, both federal and state laws may limit employers' ability to conduct medical and/or drug testing as part of the hiring process,[35] as well as with current employees.[36] Employers wanting to explore a potential employee's credit history will have to comply with specific requirements under the Fair Credit Reporting Act,[37] and those wishing to check applicants' criminal records may run afoul of federal and/or state antidiscrimination statutes.[38]

In addition to the above-described tools, employers for many years relied on a battery of honesty tests, personality tests, and other psychological examinations in screening potential (and sometimes current) employees.[39] These examinations attempt to gauge an individual's integrity and/or assess the individual's psychological state by measuring traits such as the applicant's potential for violence, propensity for addiction, and reaction to figures of authority.[40] Yet, these tests also create both legal and practical challenges for employers. Certain types of questions on these exams may violate federal and/or state antidiscrimination principles, particularly where questions inquire into a candidate's religious beliefs or sexual practices.[41] These tests also have proven to be of questionable

---

even more stringent than those established by federal law).

35. *See* Byrnside, *supra* note 34, at 451-452 (noting the EPPA restriction on polygraph tests and the ADA restrictions on medical examinations and drug testing); *see also* Befort, *supra* note 34, at 392-99 (describing limitations on testing in both the private and public sectors).

36. *See* Rochelle B. Ecker, *To Catch a Thief: The Private Employer's Guide to Getting and Keeping an Honest Employee*, 63 UMKC L. REV. 251, 272 (1994) (discussing state legislation that limits employers' use of employee drug testing); *see also* Lisa Guerin, *Workplace Testing: What Your Employer May Require*, NOLO, *available at* http://www.nolo.com/legal-encyclopedia/workplace-testing-employer-requirements-29496.html (delineating the legality of various workplace testing methods).

37. *See* Byrnside, *supra* note 34, at 450-51 (comparing the difficulties an employer may legally have monitoring an employee's social media page to the potential legal challenges an employer faces when looking into an employee's financial history.).

38. *See id.* at 450 (noting that employment decisions based on criminal records must be "consistent with 'business necessity' and [must] not have a disparate impact on a certain class of applicants").

39. *See* Susan J. Stabile, *The Use of Personality Tests as a Hiring Tool: Is the Benefit Worth the Cost?,* 4 U. PA. J. LAB. & EMP. L. 279, 279-80 (2002) (exploring the effectiveness and privacy issues surrounding use of personality tests as a hiring technique).

40. *See* Befort, *supra* note 34, at 402-03 (describing the use of personality tests by employers to discover certain characteristics about a potential employee and noting the regulations against using a polygraph test on a potential employee); *see also* Stabile, *supra* note 39, at 283-85 (discussing the factors giving rise to the widespread use of personality tests).

41. *See* Befort, *supra* note 34, at 402-04 (describing the EPPA restriction on polygraph tests for hiring purposes as well as additional state legislation restricting polygraph use); *see also* Stabile, *supra* note 39, at 286-88 (describing the extent to which the Americans with Disabilities Act may limit employers' ability to administer certain types of personality tests); *see also* Stabile, *supra* note 39, at 289-98 (describing a variety of flaws in the

utility and reliability, largely because they "measure intangible qualities such as intelligence and ability to be truthful," thus injecting subjectivity into the scoring of the examinations and producing inconsistent and untrustworthy results.[42] Thus, even to the extent that an employer ventures to utilize these tools, the information gathered as a result may be of little utility.

Faced with these obstacles in gathering information on their own, yet hungry for data about prospective employees in particular, many employers have turned to another seemingly reliable source for learning about potential new hires: soliciting reference information from a candidate's former employers. Yet, here too, employers frequently encounter barriers. In theory, employers possess significant latitude to provide reference information regarding a former employee, even where the reference will include negative information.[43] In order to encourage employers to share an accurate assessment of a former worker's abilities, the law grants employers a "qualified privilege" to communicate information to a prospective employer as part of a reference request.[44] Under this qualified privilege, an employer may not be held legally liable for the contents of a response to a reference request (i.e., through a defamation suit) so long as he or she does not communicate false information about an employee "with malice" – a term that different courts will define in different ways.[45]

Despite this potential protection, however, many employers remain wary of providing reference information. Employers fear the cost of having to litigate an expensive defamation suit to prove the existence of the qualified privilege if they do provide negative information about a former employee.[46] Moreover, employers worry that providing even *positive*

---

accuracy of personality tests to screen applicants).

42. *See* Ecker, *supra* note 36, at 260 (noting the issues with using personality tests and honesty tests and observing a recent California court ruling that the use of the former was difficult to justify); *see also* Stabile, *supra* note 39, at 297 (noting that many who have studied these tests have expressed "real concern about both the reliability and validity of personality tests"); *see also* Stabile, *supra* note 39 at 289-98 (describing the faults of personality tests).

43. *See* Stabile, *supra* note 39, at 283-84 (discussing employers' capacity to provide reference information).

44. *See* Befort, *supra* note 34, at 407 (describing the restrictions on a former employer when providing information about an employee to a prospective employer).

45. *Id.* at 408. While some courts apply a common law standard for malice, requiring "a showing of actual ill will or intent to [harm] the plaintiff," other courts use an "actual malice" standard, which "requires a plaintiff to prove that [a] statement was made with knowledge of its falsity or in reckless disregard of [its truth or falsity]." *See id.* at 408 (internal quotation marks omitted) (describing the standards used to determine if a former employer has exceeded its legal boundaries when providing information about an employee to a prospective employer).

46. *See* John Ashby, *Employment References: Should Employers Have an Affirmative Duty to Report Employee Misconduct to Inquiring Prospective Employers?*, 46 ARIZ. L.

information about a former worker may lead to trouble down the road, since employers may face exposure for negligent misrepresentation if an employee who received a positive reference subsequently exhibits violence or otherwise harms a member of the public.[47] Accordingly, confronted with this difficult decision regarding what information about a former employee should be provided to a prospective employer, many employers simply refuse to provide any substantive information at all, limiting reference information to the employee's dates of employment, positions held, final pay, and certain other objectively-verifiable information.[48] Others entirely refuse to respond to reference requests.[49]

B. The Rise in More Creative Tools for Information Gathering

Thus, when it comes to using traditional tools for gathering information about both prospective and current employees, many employers find themselves stymied in their efforts. At the same time, however, employers are under increasing pressure to gather information about their workers – both about prospective employees and about those who currently are employed.[50] Accordingly, faced with an increasing concern for gathering information and a decreasing ability to use traditional methods to do so, many employers have adopted more novel approaches for obtaining the data that they need.

Almost as a matter of course nowadays, employers use the Internet to gather information about prospective and current employees, taking advantage of the massive amounts of newly available information to assist

---

REV. 117, 118 (2004) (using a hypothetical about a potentially violent former employee to illustrate the precarious situation the employer is faced with when the violent employee's prospective employer calls for a reference); *see also* Stabile, *supra* note 39, at 283-84 (noting the impact of cost on employers' perceived threat of suit).

47. *See* Ashby, *supra* note 46, at 118 (describing the difficult decisions an employer must make and factors they must consider when providing a reference to a prospective employer).

48. *Id.* at 119; *see also Fact Sheet 16: Employment Background Checks: A Jobseeker's Guide*, PRIVACY RIGHTS CLEARINGHOUSE (November 2013), *available at* https://www.privacyrights.org/content/employment-background-checks-jobseekers-guide (observing that while "[a] former boss can say anything truthful about your performance [but] most employers have a policy to only confirm dates of employment, final salary, and other limited information").

49. Ashby, *supra* note 46,, at 119 ; *see also* Susan J. Wells, *No, Not That John Gotti*, N.Y. TIMES (Oct. 22, 1998), http://theater.nytimes.com/library/tech/98/10/circuits/articles/22chec.html (observing that "[m]any employers have adopted a policy of giving only basic information when asked for references on former employees because they fear lawsuits").

50. *See infra* Section III (discussing why employers seek to gather information on their employees).

them in their hiring decisions.[51] A 2009 survey by CareerBuilder.com reported that 45% of the 2600 hiring personnel surveyed stated that they viewed candidates' social networking sites as part of the hiring process.[52] Additional studies have reported that at least 75% of recruiters and/or employers use some type of Internet searching as part of the applicant screening process.[53] Even behemoth employers like Microsoft – a company that presumably has a wealth of resources that it could devote to the hiring process – cites social media research as a now-typical part of its hiring process.[54] As more and more data about potential workers becomes available on the Internet, and as these types of online tools become increasingly more sophisticated, employers likely will utilize these tools at an ever-growing pace.

Technology also has made it substantially easier for employers to monitor their current employees' activities.[55] For example, employers may monitor current employees' Internet usage or email communications, particularly when the employee is using an employer-provided computer or using the employers' server for this activity.[56] If employees are using a cellular phone provided by the employer, the employer may examine their text messages, voicemails, and/or listen in on their telephone conversations.[57] Employers may record the keystrokes made by the

51. Byrnside, *supra* note 34, at 446-47; *see also id.* at 456 (citing a "growing trend among employers to conduct online background checks of job applicants by searching their MySpace and/or Facebook profiles"); *see also* Margaret Keane et al., *Social Networking: New Risks of Familiar Liabilities*, *in* PRIVACY & DATA SEC. LAW 2011, 87, 93 (PLI Intellectual Prop., Course Handbook Ser. No. G-1049, 2011) (observing that "[e]mployers are increasingly and routinely using the Internet to conduct background research on applicants and employees to use in making employment decisions"); *see also* Wendy S. Lazar & Lauren E. Schwartzreich, *Employee Privacy Rights: Limitations to Monitoring, Surveillance and Other Technological Searches in the Private Workplace*, *in* EMP'T DISCRIMINATION L. & LITIG., 373, 378 (PLI Litig. & Admin., Prac. Course Handbook Ser. No. H-860, 2011) (stating that "[h]uman resource professionals turn increasingly to social media for background information on candidates").

52. *See* Lazar & Schwartzreich, *supra* note 51, at 378 (citing the aforementioned survey, in which over 600 human resource and recruiting professionals participated).

53. *See* Byrnside, *supra* note 34, at 456 (discussing several studies that have shown over 75% of employers using the internet to research job applicants); *see also* Ciocchetti, *supra* note 13, at 285 n.2 (noting that "the majority of employers monitor the electronic activities of their employees in some form or another").

54. *See* Byrnside, *supra* note 34, at 456 (discussing Microsoft's use of social media in screening job applicants).

55. *See* Kim, *supra* note 6, at 913 (noting that "[w]hile employers have always had an interest in monitoring their employees' activities, technological change has increased both the incentives and means to do so").

56. *See* Ciocchetti, *supra* note 13, at 307-09, 312-14 (discussing corporate practices in monitoring employee email, text messages, and computer usage as well as the practice of "Internet Clickstream Monitoring").

57. *Id.* at 307-09, 320-21; *see also* Lazar & Schwartzreich, *supra* note 51, at 377

employee at his/her computer and track the searches conducted by the employee via Internet search engines.[58] Indeed, this type of monitoring has become commonplace in the workplace. A recent study by the American Management Association found that 66% of employers monitor their employees' website activities.[59] 43% of employers review their employees' email and 40% analyze the contents of outbound email communications.[60] 45% of employers track the content, keystrokes, and time that employees spend at their keyboards.[61] 45% of employers monitor the time spent by employees on telephone calls and/or the numbers called by employees and another 16% of employers record employees' telephone conversations.[62] An additional 10% of employers monitor employees' voicemail messages.[63]

Employer monitoring also extends beyond examining computer and telephone usage, involving even more novel methods of tracking employees' activities. Many employers also may use "access panels" in the workplace—electronic devices that control entry into a doorway, stairwell, elevator, or other restricted area.[64] Individuals wishing to enter these restricted areas must provide a password, swipe an identification card, or utilize fingerprint or iris identification.[65] These access panels not only provide employers with workplace security by preventing unauthorized individuals from entering certain areas, but also can allow employers to track employee behavior.[66] By placing access panels on restroom or break room doors, for example, employers can monitor whether and to what extent employees utilize such facilities.[67] Employers

---

(discussing companies' recent tendencies to request access to employees' private communications through wireless cell phone services); Kim, *supra* note 6, at 902.

58. *See* Ciocchetti, *supra* note 13, at 315-16, 320 (discussing the practice of keystroke monitoring and search engine monitoring).

59. *See 2007 Electronic Monitoring and Surveillance Survey*, AMA/ePolicy Institute Research, Feb. 8, 2008, *cited in* Carlin, *infra* note 102, n.9 (noting the percentages of employers that stated in an AMA survey that they review their employees' email contents, keystrokes, and time spent on keyboards, and that have fired employees for internet misuse).

60. *Id.*

61. *Id.*

62. *Id.*

63. *Id.*

64. *See* Ciocchetti, *supra* note 13, at 302 (discussing the use of security access panels that require an input from employees in order to enter certain areas of an employer's facility).

65. *See id.* (discussing the various inputs used for access panels).

66. *See id.* at 303 (discussing the dual use of access panels for both security and employee monitoring).

67. *See id*. (discussing potential patterns employers would monitor for employee movement using access panels). On a related (but somewhat more extreme) note, some employers may use technology to monitor whether employees actually wash their hands when using the restroom at work; *see also id.* at 303-04 n.63 (discussing how at least one

similarly have used global position systems (GPS) and Radio Frequency Identification (RFID) to monitor the location of their employees and property.[68] These systems can track employees' specific location within a workplace at any given time, and also provide accurate reports on employees' productivity by compiling data regarding the speed at which employees are working.[69] While these technological advances are relatively new with respect to their use in the workplace (thus rendering their legal status somewhat in flux),[70] they too represent an area where technological advancements have allowed employers to delve even further into areas once viewed as private.[71]

As employers have stepped up their use of creative methods for gathering information about employees, one tactic in particular has captured the attention of the public, the media, and governmental actors. In recent years, some employers have requested (or in some cases, insisted) that prospective and/or current employees provide the employers with access to their social media sites.[72] For example, in 2010, the Maryland Department of Corrections asked an employee who was returning to his

company has invested in a device that will detect when an individual enters a restroom, identify whether that individual is an employee, and confirm whether that employee activates the soap dispenser while in the room. If the employee fails to activate the soap dispenser during the visit to the restroom, then a notification is provided within the room to remind that individual that hand washing is required).

68. *See id.* at 310 (discussing the use of RFID to physically track employees); *see also* Jennifer L. Parent, *Advising Clients on Today's Top Employment Law Issues*, *in* ASPATORE THOUGHT LEADERSHIP, EMPLOYMENT LAW 2013: TOP LAWYERS ON TRENDS AND KEY STRATEGIES FOR THE UPCOMING YEAR *2 (2013) (discussing the use of GPS to physically track employees).

69. *See* Ciocchetti, *supra* note 13, at 310 (noting that RFID tracking can generate real-time monitoring of employee location within the workplace).

70. *See* Parent, *supra* note 68, at *2 (discussing a Supreme Court case that reversed a criminal conviction for a failure of law enforcement to get a warrant before using GPS to track a suspect, noting a best practice of informing employees of tracking policies, and discussing federal cases dealing with the ownership of social media pages); *see also* Ciocchetti, *supra* note 13, at 311-12 (noting that requiring employees to swallow RFID chips is illegal in several states).

71. Ironically, this use of technology to "push the envelope" regarding the bounds of employee privacy in some cases may work to the detriment of the *employer*. Employees also increasingly are becoming savvy about the extent to which technology can assist them in various workplace situations. *See, e.g.*, David Koeppel, *The Secret Spy Living in Your iPhone*, THE FISCAL TIMES, July 28, 2011 (describing employee's use of blackberry device to record conversation with a superior during a negative performance review); *see also id.* (discussing one plaintiff attorney's observation that more than 50% of her potential clients possess some type of digital evidence with respect to their claims).

72. *See* Debra Donston-Miller, *Facebook Password Debate Stirs Deep Social Fears*, INFO. WEEK (Mar. 27, 2012), http://www.informationweek.com/thebrainyard/news/social_networking_consumer/232700304/facebook-password-debate-stirs-deep-social-fears (discussing Facebook's reaction to employers requesting access to employees' Facebook pages).

position as a security guard following a leave of absence to provide the Department of Corrections with his social media login and password.[73] According to the Department of Corrections, this request was made in order to check for any gang affiliations by the employee.[74] In another instance, a New York statistician interviewing for a new position was asked to provide his prospective employer access to his Facebook page.[75] Various municipal employers also have put these types of policies in place, requiring certain employees – most frequently those working in a security or law enforcement capacity – to provide their employers with access to their personal social media sites as a condition of employment.[76]

Even if an employer does not ask a prospective or current employee for their social media login credentials, employers can gain access to these websites through a variety of other methods. In some cases, employers may ask applicants or employees to log on to a social media site in the presence of an employer representative. This allows the employer to review the contents of the site at that time (a practice known as "shoulder surfing").[77] In other cases, the employer may ask the employee to "friend" a staff member of the employer, thereby allowing that individual access to the information on the social media site.[78] Finally, some employers utilize third party applications that can scour and collect some of the information

---

73. Manuel Valdes & Shannon McFarland, *Employers asking job applicants for Facebook passwords*, THE ASSOCIATED PRESS, Mar. 20, 2012, *available at* http://news.yahoo.com/employers-ask-job-seekers-facebook-passwords-170500338.html; *see also* Emil Protalinski, *Employer demands Facebook login credentials during interview*, ZDNET (Feb. 20, 2011), http://www.zdnet.com/blog/facebook/employer-demands-facebook-login-credentials-during-interview/327 (discussing ACLU's representation of the aforementioned job applicant); Leslie Horn, *Employers Asking Applicants for Facebook Passwords*, PC MAG. (Mar. 17, 2012), http://www.pcmag.com/article2/0,2817,2401254,00.asp.

74. *See* Protalinski, *supra* note 73 (discussing the Maryland Department of Corrections' reasons for asking for the aforementioned job applicant's Facebook password).

75. *See* Valdes & McFarland, *supra* note 73 (discussing a job applicant's refusal to provide a potential employer with his Facebook password).

76. *See* Horn, *supra* note 73 (discussing various situations wherein employers have asked for applicants' Facebook passwords); *see also* Walter M. Stella, *The Importance of Compliance with Employment Law in an Ever-Changing, High-Tech Era*, *in* ASPATORE THOUGHT LEADERSHIP, EMPLOYMENT LAW 2011: TOP LAWYERS ON TRENDS AND KEY STRATEGIES FOR THE UPCOMING YEAR *5 (2011) (discussing the potential legal implications of using social media to monitor employees).

77. *See* Horn, *supra* note 73 (describing "shoulder surfing" and noting that it is a violation of Facebook's own terms of use); *see also* Valdes & McFarland, *supra* note 73 (defining "shoulder surfing").

78. *See* Valdes & McFarland, *supra* note 73 (noting that employers are using various measures to monitor their employees' Facebook pages); *see also* Marie-Andree Weiss, *The Use of Social Media Sites Data by Business Organizations in their Relationship with Employees*, J. INTERNET L., Aug. 2011, at 16, 23 (stating that while becoming a friend just to "spy" on one's employee may be legal, it may also raise ethics issues).

from an individual's Facebook profile.[79]

Predictably, many have denounced this practice as a dramatic overreach by employers. According to one commentator – a law professor and former federal prosecutor – "[i]t's akin to requiring someone's house keys . . ., an egregious privacy violation."[80] In the words of another observer, "Would we let a potential employer walk around our houses, opening drawers, looking at our letters, checking our diaries, little blackbooks, and contents of our liquor cabinets? I think not."[81] The sponsor of an unsuccessful 2012 Senate bill aimed at outlawing this practice referred to these employer requests for social media credentials as "an unreasonable and intolerable invasion of privacy."[82] Even the American Civil Liberties Union (ACLU) has involved itself in fighting this practice.[83]

---

79. *See* Torie Bosch, *Can Legislation Preventing Employers From Requesting Facebook Passwords Really Protect Privacy*, SLATE (Mar. 28, 2012, 4:20 PM), http://www.slate.com/blogs/future_tense/2012/03/28/employers_don_t_have_to_request_facebook_passwords_to_invade_applicants_privacy_.html (discussing legislation to protect employee privacy); Joshua Brustein, *Keeping a Closer Eye on Employees' Social Networking*, N.Y. TIMES (Mar. 26, 2010, 6:51 PM), http://bits.blogs.nytimes.com/2010/03/26/keeping-a-closer-eye-on-workers-social-networking/ (describing a new software that monitors an employee's social media accounts for their employer); Valdes & McFarland, *supra* note 73 (enumerating additional strategies employers use to monitor employees' social media pages).

80. *See* Valdez & McFarland, *supra* note 73 (discussing the measures employers take to monitor an employee's social media page).

81. *See* Donston-Miller, *supra* note 72 (describing a movement advocating for consequences for employers who violate their employees' privacy through social media sites).

82. *See* Whitney, *supra* note 1 (describing proposed legislation to restrict employers from requesting an employee's social media information).

83. *See* Horn, *supra* note 73 (noting the ACLU's opposition to "shoulder surfing"); *see also* Emil Protalinski, *ACLU: Employers Demanding Facebook Passwords Is Privacy Invasion* (Mar. 22, 2012, 10:24 PM), http://www.zdnet.com/blog/facebook/aclu-employers-demanding-facebook-passwords-is-privacy-invasion/10693 (quoting an ACLU attorney's statement that "[i]t's an invasion of privacy for private employers to insist on looking at people's private Facebook pages as a condition of employment or consideration in an application process. . . . People are entitled to their private lives"). Interestingly, while Facebook's Chief Privacy Officer previously claimed that requesting employees' and applicants' login information would violate the company's terms of use, indicating that Facebook might take legal action against employers engaged in this practice, the company has not yet taken any legal action against any employer and may have backtracked with respect to this position. *See* Bosch, *supra* note 79 (discussing attempts to introduce bills to protect employee privacy); Anne Fisher, *Must You Give a Job Interviewer Your Facebook Password?*, CNN MONEY (Mar. 28, 2012, 12:08 PM) http://management.fortune.cnn.com/2012/03/28/facebook-password-job-interview/ (instructing applicants on declining to give social media password information to a prospective employer during an interview); Shel Israel, *The Great Facebook Employee Password Non-issue*, FORBES (Mar. 25, 2012, 8:32 PM), http://www.forbes.com/sites/shelisrael/2012/03/25/the-great-facebook-employee-password-

Yet other observers have criticized the apparent hysteria that has surrounded this issue. According to these commentators, requests for social media credentials represent nothing more than "a few clumsy missteps by socially backward organizations, or even legitimate steps in the vetting of candidates for positions that would require high security clearance."[84] According to one reporter who has studied this issue, "on closer examination it turns out there have been very few reported instances of privacy abuse and none of them seem to have happened very recently."[85] According to this reporter, virtually all reported cases of individuals being asked to turn over password information involve government positions (primarily public safety jobs), and all occurred more than one year ago.[86] This reporter could not find an example of a private sector employer demanding a prospective or current employee's social media password.[87] Thus, while valid objections to this practice may exist, there is scant evidence to indicate any threat of employers demanding social media passwords or similar information on a broad scale.

Moreover, employers have valid reasons for wanting access to this information. Some employers, particularly those in a public safety or similar field, may want to check for security risks associated with hiring or retaining a particular worker.[88] Employers likewise may want to review an employee's social media web site(s) to gather important information about an employee's judgment that might not otherwise be available to an employer.[89] Finally, some employers may use employees' social media credentials to more specifically measure an employee's potential for success in a position. Indeed, at least one recent study has concluded that checking a candidate's Facebook profile may be the best predictor of that candidate's success within a company – significantly more accurate than

nonissue/ (arguing that the media is exaggerating privacy invasions surrounding employees' social media activity).

84. *See* Donston-Miller, *supra* note 72 (observers have argued that "when you break down the events, this issue is nothing but a tempest in a teapot").

85. *See* Israel, *supra* note 83 (discussing the media's portrayal of social media abuse by employers).

86. *See id.* (noting that the threat of employers abusing social media has been exaggerated).

87. *See id.* (noting that the threat of misuse of social media by employers, especially private employers, is overstated).

88. *See supra* notes 74-76 and accompanying text (describing situations where employers may feel concerned about the implications of their employees' social media postings).

89. *See, e.g.*, David Mielach, *Hiring Managers Reveal Social Media Secrets*, BUSINESS NEWS DAILY (April 18, 2013), http://www.businessnewsdaily.com/2377-social-media-hiring.html (hiring managers have declined to hire candidates who post inappropriate or provocative pictures online, and/or whose social media pages include evidence of drinking or drug use, poor communication skills, bad-mouthing of a prior employer, or making discriminatory comments).

even standard personality tests.[90]

Despite the potential benefits associated with acquiring an applicant's or employee's social media credentials, and the relatively limited scope in which this tactic is used, politicians are responding to this practice with predictable fervor. On the federal level, three members of Congress recently introduced the Social Networking Online Protection Act ("SNOPA"), designed to limit employers' access to the login credentials of employees' and applicants' social media accounts.[91] The law would impose significant fines on employers that request or require any employee or applicant to provide the employer with a username, password or other means of accessing a private email or social media account, as well as on employers that retaliate against individuals who refuse to provide such information.[92] This legislation follows on the heels of successful efforts by several states to regulate this area.[93] Indeed, on the state level, this type of legislation has become something of a trend: A recent report by the National Conference of State Legislatures asserts that social media privacy legislation has been introduced or is in the process of being implemented in thirty-five states since the start of 2013.[94] As states inevitably jump on this bandwagon, and as federal lawmakers continue to contemplate their own pending legislation, employers are on the verge of losing a powerful tool in their information-gathering arsenal.

---

90. *See* Horn, *supra* note 73 (citation omitted) (describing "shoulder surfing" and identifying employers' motivation to "shoulder surf").

91. *See* Loatman, *supra* note 1 (describing various states' proposed legislation to prevent employers from violating employees' privacy rights by monitoring their social media).

92. *See id.* (discussing "SNOPA" and proposed social media privacy legislation in different states). Notably, this legislation represents Congress's second attempt to regulate in this area. Virtually identical legislation was introduced in Congress in 2012 but failed to become law. *Id. See also* Whitney *supra* note 1 (discussing possible legislative action to combat social media abuse by employers).

93. Maryland, Illinois, California, Michigan, New Mexico, Utah, Arkansas, Washington, Colorado and New Jersey have already enacted legislation that limits employer access to social media accounts. *See* Loatman *supra* note 1 (noting progress that has been made in legislation that restricts employer access to employees' social media sites); *see also* Joseph J. Lazzarotti, *More states limit employer access to employee social media accounts*, LEXOLOGY (May 23, 2013), http://www.lexology.com/library/detail.aspx?g=7f39acc0-6ca1-48be-a4f9-a3348c8d9cf3 (detailing new legislation in states to protect employees privacy); *Arkansas Enacts Employer, School Social Media Privacy Protection Laws*, DAILY LABOR REPORT NO. 82, Apr. 29, 2013, at A-8 (describing Arkansas's new law to restrict both employers' and higher education institutions' access to prospective students' and employees' social media password information); Lorraine McCarthy, *New Jersey Governor Signs Bill Limiting Employer Access to Social Media Accounts*, DAILY LABOR REPORT NO. 168, Aug. 29, 2013, at A-10 (noting a recent law passed in New Jersey prohibiting employers from requiring prospective or current employees to give employers their social media passwords).

94. Eaglesham & Rothfeld, *supra* note 3.

III. EMPLOYER MOTIVATIONS FOR SNOOPING: WHY EMPLOYERS SNOOP

Employers have adopted a broad range of methods to gather information about prospective and/or current employees. But why are employers so fixated on gathering this information in the first place? Why do employers care about who employees might associate with outside of work, or about what an individual might post on his/her social media page, or about the specific internet sites visited by a (presumably otherwise-productive) employee? Some have adhered to the relatively simplistic argument that employers choose to peek into their employees' private lives without any legitimate cause. There are, however, a variety of considerations that not only justify employers taking these intrusive steps to investigate their workers, but also render such steps prudent and necessary.

A. Financial Motivations for Snooping

A host of financial considerations motivate employers to monitor their employees' behavior. These financial concerns play a large role during the hiring process. Given today's competitive business environment, employers must take every possible step to maximize gains and minimize losses. Employers often unnecessarily waste substantial resources as part of the hiring process. Not only is recruiting and interviewing candidates a costly endeavor, but employers can also waste significant resources due to poor hiring decisions – decisions which ultimately force an employer to retrain (or replace) an employee.[95] Accordingly, employers increasingly have directed their resources toward finding an employee who represents the best possible "fit" for a position.[96]

In this respect, the use of technology to snoop into a job applicant's background has become an indispensible part of the hiring process. As

95. *See* Stabile, *supra* note 39, at 282-83 & nn.13-14 (observing that "replacing employees is costly" and citing statistics placing the cost of replacing one bad hire at "1.5 times the worker's salary and benefits") (citations omitted); *see also* Jay Goltz, *The Hidden Costs of Bad Hiring*, N.Y. TIMES, Mar. 1, 2011, http://boss.blogs.nytimes.com/2011/03/01/the-hidden-costs-of-bad-hiring/ (estimating that two "bad hires" could cost an employer as much as $40,000 in increased unemployment insurance expenses alone, and could run up to $200,000 if the employees' actions resulted in lost customers).

96. *See* Byrnside, *supra* note 34, at 448 (noting that "[e]mployers often seek as much information as possible about job applicants to ensure the best fit between an applicant and the employer's organization") (citation omitted); *see generally* Stabile, *supra* note 39, at 279-80 (discussing employers' use of personality and other tests to eliminate applicants possessing negative traits and determine the "fit" between an applicant and any open position).

noted above, employers have utilized the Internet to research candidates with increasing frequency in recent years.[97] What once may have seemed like a significant intrusion on a job applicant's privacy has now become an accepted – and even *expected* – part of the interview process.[98] In fact, some observers have argued that "it would be irresponsible for an employer not to conduct such easy and cost-effective due diligence before hiring or promoting employees."[99] As this technology becomes even more cost-efficient in years to come, and as individuals post more and more information online, one should expect employers to use this simple and cost-effective screening tool with even greater frequency.[100]

With respect to current employees, employers possess similar concerns regarding maximizing profitability and efficiency, and these concerns likewise may lead employers to monitor their workers. In today's workplace, "incessant distractions litter workplaces and entice workers to stray from their duties."[101] In a depressed business climate where profit margins consistently tighten, employers have become increasingly focused on eliminating behaviors that might detract from the bottom line.[102] For example, employers want to ensure that employees are not spending excessive time surfing the Internet in lieu of performing their duties. According to one report, "[e]ven minor personal Internet use in the workplace can lead to millions in lost profits."[103] This same study predicted that "[t]his potential loss may only get worse as the average gen-y'er spends upwards of thirty four percent of their time online doing personal tasks, as opposed to the twenty five percent found in the rest of the

97. *See supra* notes 51-54 and accompanying text (discussing employers' surveillance of employees' social media activities).

98. *See* Weiss, *supra* note 78, at 16 (describing results of 2009 survey which showed that 79% of hiring managers and recruiters in the United States review online information about prospective employees, and showing that 75% of U.S. companies surveyed have policies *requiring* employees in charge of hiring to utilize online research).

99. *See id.* (noting the ease of accessing prospective and current employees' social media pages); Keane, *supra* note 51, at 93 (citation omitted).

100. *See* Byrnside, *supra* note 34, at 453 (observing that "[t]he more economical it becomes to obtain information about a potential employee's private life, the greater the likelihood employers will use it") (citations omitted) (internal quotation marks omitted).

101. Ciocchetti, *supra* note 13, at 285 (citation omitted).

102. *See* Sprague, *supra* note 5, at 111 (arguing that "[o]ne significant motivation for monitoring is performance-based, ensuring that employees are performing their work effectively and efficiently, or at all.") (citation omitted); *see also* Michael Carlin, *Employers are Watching Your Facebook: Worker Privacy Significantly Diminished in the Digital Era*, NAT'L L. F. (June 8, 2011), http://nationallawforum.com/2011/06/08/employers-are-watching-your-facebook-worker-privacy-significantly-diminished-in-the-digital-era/ (noting that "[p]roductivity concerns also cause many employers to monitor employees").

103. Carlin, *supra* note 102 (citation omitted); *see also* Larry Swisher, *Nine of 10 Workers Accept, Like Monitoring of Computer Use by Employers, Survey Finds*, DAILY LAB. REP., May 24, 2013, at A-13 (estimating business loss due to personal computer use).

working population."[104] Another study recently found that, for a business with 100 employees, the time lost due to non-work-related computer activities "is the equivalent of paying nearly seven . . .workers to do nothing at a total cost of $385,000 per year in wages . . ."[105]

Employers likewise may monitor employees to avoid more direct types of financial harm. Excessive personal use of a company's broadband capacity or email accounts may result in decreased productivity, costly storage shortages, and/or slower network operations.[106] Visiting social media sites or other unsecure web sites from a company computer can introduce data security risks like malware, phishing, or other viruses into the employer's computer system.[107] In some cases, employers may monitor employees to prevent seemingly mundane yet ultimately costly financial injuries – for example, using video surveillance to prevent the theft of office supplies or other company property.[108]

One final financial consideration that motivates employers to snoop may arise out of a company's desire to protect its trade secrets. As one commentator observed, "[n]ew technology leads to new ways that competitors or employees can steal confidential company information."[109] A 2010 study by a software security company found that an astonishing

---

104. Carlin, *supra* note 102, n.32 (citation omitted).

105. Swisher, *supra* note 103.

106. *See* Ciocchetti, *supra* note 13, at 286 (explaining companies' rationale for monitoring employee computer use) (citation omitted).

107. *See* Weiss, *supra* note 78, at 19 (detailing the ease of contracting viruses and malware through social media links); *see also* Paul M. Secunda, *King and Spalding's Surprising New Email Policy*, WORKPLACE PROF BLOG (Apr. 22, 2013), *http://lawprofessors.typepad.com/laborprof_blog/2013/04/king-and-spaldings-surprising-new-email-policy.html* (implementing an email policy under which firm employees are barred from accessing *any* personal email accounts (i.e., anything other than the individual's kslaw.com email account) from any firm computer, or from any computer connected to the firm's computer network). In implementing its policy, King & Spalding cited advice from both internal and outside security experts indicating that accessing personal email accounts from firm computers could create a significant security risk to the firm and its clients. *Id.* The firm further noted that "individual users who innocently click on malicious e-mails are often the cause of security breaches." *Id.*

108. *See* Ciocchetti, *supra* note 13, at 322 (detailing the reasons companies employ video surveillance in the workplace) (citation omitted); *see also* Alexis C. Madrigal, *Dunkin Donuts' Employee Surveillance Cut Thefts Up to 13%*, THE ATLANTIC (Apr. 20, 2012), http://www.theatlantic.com/technology/archive/2012/04/dunkin-donuts-employee-surveillance-cut-thefts-up-to-13/256152/ (asserting the broad use of video surveillance by fast-food restaurants, which lose approximately seven percent of sales due to employee theft); *cf.* Stabile, *supra* note 39, at 281 n.7 (citing a 1991 study that estimates the direct cost to employers of employee theft as close to $50 billion, as well as other studies placing the cost at $40 billion) (citations omitted).

109. Rosenberg, *supra* note 13, at 473-74; *see also* Weiss, *supra* note 78, at 19 (detailing the possibility of employees leaking confidential information or trade secrets through use of social media).

94% of users of one large social networking site readily accepted a "friend request" from a complete stranger (who happened to be presented to them as a pretty young woman).[110] Even more shocking, when this same study then selected twenty of the individuals who had accepted the friend request and engaged them in real-time conversation online, 73% of the sample had – within a mere two hours of conversation – revealed to this new "friend" confidential information belonging to their employer, including business strategies and information about unreleased products.[111] In 2004, even Apple – a company known for keeping its trade secrets under wraps – discovered confidential information about unreleased products posted on a publicly-accessible Internet bulletin board.[112] The disclosure of this type of proprietary information can cost a business hundreds of thousands of dollars in any given year: a 2001 survey in which 138 *Fortune 1000* companies reported data, the survey authors concluded that losses of proprietary information and intellectual property ranged between $53 billon and $59 billion in a single year.[113]

B. Concerns About Liability Prevention as a Motivation for Snooping ("Prophylactic Monitoring")

On top of the financial incentives that might motivate an employer to snoop, employers also may feel compelled to monitor employees as a means of preventing legal exposure in various areas. For example, as discussed in greater detail below,[114] employees who use workplace computers or other employer-provided equipment to browse pornographic web sites, display sexually explicit content, or disseminate racially insensitive material may expose their employers to liability in a harassment or discrimination case.[115] In some disturbing news for employers, some

110. Weiss, *supra* note 78, at 20 (citation omitted).

111. *Id.* (citation omitted); *see also* Ciocchetti, *supra* note 13, at 286 (stating that "[f]ailing to monitor [employees properly may] allow rogue employees to steal trade secrets or send out confidential information in violation of various federal and state laws") (citations omitted).

112. Rosenberg, *supra* note 13, at 474.

113. U.S. CHAMBER OF COMMERCE ET AL., TRENDS IN PROPRIETARY INFORMATION LOSS 1 (2002), *available at* www.uschamber.com/sites/default/files/issues/technology/files/informationloss2.pdf. Notably, an entire cottage industry has arisen to take advantage of these types of concerns. One online communication services company recently launched a new type of software, called Social Sentry, designed to help employers monitor their employees' Facebook and Twitter accounts, with one focus being to help employers watch for the release of confidential or embarrassing information. *See* Brustein, *supra* note 79 (describing Teneros' social media monitoring service).

114. *See infra* Section IV.B.1 (discussing the incentives of utilizing employee computer surveillance to avoid liability for hostile workplace claims).

115. *See* Kim, *supra* note 6, at 913 (observing that "employers now also fear that

studies have indicated that over 20% of all email users have received sexually explicit email in the workplace.[116] Similarly, employees may abuse their employer's email system through a practice called "spoofing"—intentionally sending messages that appear to be from someone else—in order to harass the recipient or otherwise disseminate an inappropriate message.[117] In either circumstance, these inappropriate emails or other Internet activities can form the basis of harassment or other lawsuits against an employer.[118] By monitoring employees' use of the employer's Internet and email systems, an employer may be able to learn of—and eliminate—such inappropriate usage before it can create a hostile environment or other negative ramifications for employees.[119]

Employees' disclosure of confidential or other proprietary information also can create potential liability for employers, thus motivating employers to monitor workers in order to prevent these disclosures. For example, an "[e]mployee['s] mishandling of electronic files could also result in improper disclosure of customers' private information or other security breaches[.]"[120] In one fairly unusual case, the personal information of Shell Oil Company employees in dangerous parts of the world was leaked to a blogger and subsequently published, posing a threat to the lives and well-being of these workers.[121] Had harm befallen any of the workers whose information was made public, Shell might have been concerned about its own liability for failing to prevent this leak from taking place. Similar arguments about the need to prevent harms caused by leaked information have been cited by Wall Street to justify its efforts at snooping: In opposing the rash of new legislation that limits employer access to employees' social media accounts, securities regulators have expressed concern that "the raft of new laws aimed at protecting employees' privacy puts investors at

---

employee misuse of electronic communications will . . . giv[e] rise to charges of racial or sexual harassment . . . .") (citation omitted); *see also* Rosenberg, *supra* note 13, at 443 (stating that inappropriate emails may serve as evidence in sexual harassment and/or discrimination suits) (citation omitted).

116. *See* JEFFREY ROSEN, THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA 79 (Vintage Books 2001) (2000) (discussing the privacy of employees' communications in the workplace).

117. Rosenberg, *supra* note 13,, at 443-44.

118. *See id.* at 443 (describing the exposure to litigation caused by e-mail misuse); *see also* Ciocchetti, *supra* note 13,, at 285 (emphasizing employers' disdain for exposure to liability caused by employees' misuse of workplace technology).

119. *See infra* at Section IV.B.1 (concluding that an employer's incentive for monitoring extends beyond just preventing the creation of a sexually hostile environment, and that such monitoring may be essential to forming an affirmative defense for any harassment claims that ultimately are brought against the employer).

120. Kim, *supra* note 6, at 913 (citations omitted).

121. *See* Carlin, *supra* note 102 (discussing the possibility of kidnapping and insider trading based on the leaked information).

risk."[122] These regulators worry that the rapid dissemination of financial advice on social networks like Facebook and Twitter "could create new channels for Ponzi schemes and other frauds,"[123] and argue that fighting these frauds will be complicated by state laws that bar employers from monitoring what their employees pitch to investors.[124]

Employers also might snoop into ostensibly private areas of their employees' (or, more typically, prospective employees') lives out of a concern over liability for negligent hiring. While the standards for determining liability in this area may vary somewhat from one jurisdiction to the next, most jurisdictions examine whether an employer knew, or *should have known*, of an employee's unfitness for a position or dangerous propensities.[125] In at least one jurisdiction, courts applying this standard will focus on "the adequacy of the employer's pre-employment investigation into the employee's background" in determining the employer's liability for negligent hiring.[126] This emphasis on employers conducting a "reasonable investigation" before hiring a new worker provides further motivation for an employer to snoop as part of the hiring process. What exactly constitutes a "reasonable investigation"? How deeply should a prospective employer dig? An employer nowadays likely would be expected at least to conduct a basic Internet search before hiring an individual.[127] Indeed, with so much information now available over the Internet—and with Internet searches rapidly becoming a standard part of the hiring process—an employer may appear negligent if it does *not* engage in such pre-hiring "snooping."[128] If a candidate's Facebook page is plastered with images of him holding assault weapons, abusing small animals, or snorting cocaine—and if the candidate then engages in similar threatening or illegal activity once hired by an employer—a jury likely would be hard-pressed to find that such readily-available clues would fall outside the scope of the employer's reasonable investigation.

Quite simply, employers need to know if a prospective or current employee is a drug addict, a criminal, or has violent tendencies. If the

122. Eaglesham & Rothfeld, *supra* note 3.

123. *Id.*

124. *See Id.* ("Wall Street's self-regulator, the Financial Industry Regulatory Authority, says financial firms need a way to follow up on 'red flags' suggesting misuse of a personal account").

125. *See* Weiss, *supra* note 78, at 18 (citing Ponticas v. K.M.S. Invs., 331 N.W.2d 907, 911 (Minn. 1983)).

126. Weiss, *supra* note 78, at 18 (citing Garcia v. Duffy, 492 So. 2d 435, 438 (Fla. Dist. Ct. App. 1986)) (internal quotations omitted).

127. *See supra* notes 51-54, 97-100 and accompanying text.

128. *See* Weiss, *supra* note 78, at 18 (arguing that "[w]ith the prevalence of search engine use to search for information, particularly information about a person, a plaintiff in a negligent hiring case might indeed argue that propensities leading to the employee harming the plaintiff could have been discovered by searching the web, SMS included").

easiest way to discover this information involves a bit of snooping, then employers should be given a bit of latitude to pursue such channels. Otherwise, employers will find themselves between a rock and a hard place—responsible for protecting the health and safety of their workforce and the public, but deprived of one of the most effective tools for implementing this protection.

C. Reputational Concerns as a Motivation for Snooping

Related both to the aforementioned financial motivations for snooping and to concerns about potential legal liability, a third motivation behind employers' decision to snoop stems from employers' reputational concerns. Most employers likely have little interest in the details of their employees' personal lives: they likely are not particularly intrigued by their employees' vacation photos, weekend plans, or Facebook posts about their children's latest witty statements. Rather, many employers may monitor their employees' out-of-work conduct out of a concern for how that employee may be *representing* the employer. Is an employee making disparaging statements about the employer? Is he or she disclosing information that the employer would prefer to keep secret? Is the employee mischaracterizing some part of the employer's operations? Such questions understandably would concern any employer.

The injection of technology into the workplace has raised the stakes with respect to these reputational concerns, rendering an employer's reputation even more vulnerable than it was in the past. In the past, employers could maintain tremendous control over virtually all communications made on behalf of the company. Simply by controlling employees' access to the company's pre-printed letterhead and stationery, employers could limit the ability of an unauthorized employee to send communications in the company's name.[129] Now, with email as the dominant form of workplace communication (and with email accounts that typically include an employer's domain name or other identifying information), employers have enabled virtually *every* employee to communicate with others in the workforce (and with the outside world) in a manner that bears the employer's imprimatur.[130] Moreover, in the past, communications themselves generally were handwritten or typed with deliberation and care, and were delivered by "snail mail" or, if urgent, by hand.[131] Now, with email emerging as the preferred form of

129. *See* Keane, *supra* note 51, at 91 (discussing how employers in the past could control access to the ability to speak on the company's behalf by controlling who could use company letterhead and stationery).

130. *See id.* at 91-92.

131. *See id.* at 91.

communication, employees communicate using far less care than in days gone by. Instead of carefully typed or handwritten communications, individuals frequently dash off email messages with far less reflection and prudence, and then can disseminate that those messages to innumerable outsiders with the mere push of a "send" button."[132] As one commentator has observed, "the days of true [employer] control [over employee communications] are relics of another era."[133]

For employers, the impact of such cavalier communications on their reputation can be devastating. In May 2008, for example, Angelo Mozilo, then-CEO of Countrywide Financial, mistakenly replied to a distressed debtor who had contacted Countrywide desperately seeking assistance with mortgage restructuring.[134] In his "misdirected" reply email, Mr. Mozilo wrote, "This is unbelievable. Most of these letters now have the same wording. Obviously they are being counseled by some other person or by the Internet. Disgusting."[135] When Mr. Mozilo's email ultimately was widely circulated on the Internet and in the news media, it led to significant embarrassment for Countrywide.[136] An equally destructive situation (not directly involving email) arose in April 2009, when two Domino's Pizza employees inflicted immeasurable damage upon their employer after posting online several videos of unsanitary and disgusting acts engaged in during the preparation of a customer's pizza.[137] After the video ultimately went viral, Domino's experienced a steep decline in its stock values.[138] In

132. *See id.* (stating that "[e]mployees are able to communicate instantaneously and with an audience of unlimited scope" and modern-day correspondence "is sent[] with the tap of the Send button, often only seconds after the email or document is composed").

133. *Id.*

134. *See* Janice Mac Avoy et al., *Think Twice Before You Hit The Send Button! Practical Considerations In The Use Of Email*, PRAC. LAW, Dec. 2008 at 45, 46 (citation omitted) (discussing the harm of inadvertently forwarding an impolite internal message to the original sender).

135. *Id.* at 46.

136. *See id* (discussing the spread of the email online). For an additional example of a negative email damaging an employer's reputation, *see* Kim States, *Oh the social lessons learned when internal email goes viral*, INSIDE TUCSON BUS (Feb. 3, 2012), http://www.insidetucsonbusiness.com/news/profiles/oh-the-social-lessons-learned-when-internal-email-goes-viral/article_e1343a86-4dc6-11e1-8f04-0019bb2963f4.html#.UTkeoXeTmyE.mailto (discussing the impact of a marketing firm's rude email exchange with a dissatisfied customer becoming public).

137. *See* Carlin, *supra* note 102 (discussing employers' need to protect their businesses against unlawful activity, including the fallout from two Domino's Pizza employees preparing a customer's pizza in an unsanitary manner).

138. *See id.* (discussing decline in stock value as the fallout from the Dominos viral video scandal); *see also* Kerry M. Lavelle, *Why Every Employer Should Adopt a Social Media Networking Policy*, CONSTR. EQUIP. DISTRIB. (Aug. 1, 2010), http://www.cedmag.com/article-detail.cfm?id=10926254 (describing damage to reputation of Burger King chain after video of Burger King employee taking bath in workplace sink was electronically distributed to YouTube, MySpace, the health department, and to Burger

this way, an employer's hard-earned reputation can be shattered by careless or malicious employee behavior, since email and other social media allow an isolated incident of misconduct or poor judgment to become public fodder. In the words of one commentator, "[n]ever before has so much damage been accomplished by low level employees through mindless behavior and social media."[139] By monitoring employee conduct in the workplace, as well as communications that employees make *about* the workplace, employers may be able to limit or even avoid this type of damage.

Concerns about protecting their own reputations seem particularly relevant in motivating employers to monitor their employees' social media postings.[140] As noted above, employees frequently exhibit little inhibition in posting a glut of information, including their employers' confidential or other proprietary information, on social media sites.[141] Employees' social media postings may also spread negative aspersions about an employer, such as in one recent case involving a police officer who posted accusations of department corruption on her Facebook page.[142] Employers have an interest in quelling this type of public disparagement Just as an employee would expect his or her employer not to publicize on its company Facebook page the results of the employee's negative performance review or the reasons for (or even mere fact of) the

---

King's management).

139. Carlin, *supra* note 102.

140. *See generally* Lawrence E. Dubé, *NLRB's Solomon Tackles Social Media Cases, Giving Wal-Mart Policy Revision a Green Light*, DAILY LAB. REP., May 31, 2012, at AA-1, *available at* http://www.bna.com/nlrbs-solomon-tackles-n12884909814/ (discussing the significant attention the National Labor Relations Board ("NLRB") has devoted to crafting guidelines for employers to use in setting workplace policies for social media use); *see also* Mercedes Colwin & Bran C. Noonan, *Navigating the Social Media Policy Minefield*, GORDON & REES LLP (June 2012), http://www.gordonrees.com/publications/viewPublication.cfm?contentID=2692 (advising "[e]mployers looking to implement policies governing the use of social media by employees in the workplace . . . to devise policies that do not conflict with the [NLRA], which may be challenging to accomplish"); Michael O. Loatman, *Attorney Says NLRB Appointments Dispute Doesn't Change Social Media Policies Advice*, DAILY LAB. REP., Mar. 6, 2003, at A-8 (citing the perspective of a practicing attorney in this area that the NLRB recently has been "'aggressive' in policing social media policies," frequently finding problems with confidentiality provisions appearing in such policies, as well as with provisions that regulate the "postings or public comments about [a] company," or that bar "negative or disparaging comments about [a] company").

141. *See supra* notes 110-11 (discussing a recent study that exposed employees' willingness to "friend" and discuss confidential business information with total strangers on a social media site).

142. *See* Gresham v. City of Atlanta, No. 1:10-CV-1301-RWS, 2012 WL 1600439, *1 (N.D. Ga. May 7, 2012) (holding that police department did not violate police officer's free speech rights when it denied officer a promotion after she posted accusations of department corruption on her Facebook page).

employee's termination, so too does the *employer* have the right to expect its employees not to disparage the company in the online community.

D. The "New Normal": Advances in Technology and Changing Employee Expectations as a Motivation for Snooping

One final reason for the increase in employer snooping is that this type of behavior has become significantly easier to implement. First, as noted above, technology has become an increasingly prevalent part of the modern workplace,[143] frequently making it less costly for employers to gather information about prospective and current employees. With the increasing availability of computer databases that contain millions of records of personal data about individuals, the cost of searching these sources drops for employers.[144] One recent study conducted by a University of Denver professor demonstrated just how easily (and inexpensively) a wealth of personal information can be accessed by a third party: By providing some minimal information and paying $29.95 to an online investigations company, this professor was able to receive—within a mere 15 minutes—an extensive personal dossier on himself.[145] With such a wealth of information available at such a low cost, searches that once resided in the toolbox of only large and resource-rich companies now may seem feasible to a broad range of employers.[146]

To a certain extent, these advances in technology create a cyclical phenomenon, culminating in an attrition of privacy rights: the more technology advances, the more that certain intrusions which once would have seemed astonishing now may appear mundane—and even expected. In the recent *Quon* case (discussed further below),[147] for example, the Supreme Court observed the extent to which social norms play a significant role in shaping the reasonableness of an individual's expectation of privacy.[148] According to the Court, "[r]apid changes in the dynamics of communication and information transmission are evident not just in the

143. *See supra* notes 51-71 and accompanying text (discussing employers' use of the Internet to gather information about prospective and current employees and to monitor the activities of employees); *see also* Bentzen, *supra* note 6, at 1293 (citations omitted) (internal quotation marks omitted) (stating that "[n]ew technology has been injected into the workplace at an exponentially increasing rate over the last few decades").

144. PRIVACY RIGHTS CLEARINGHOUSE, *supra* note 48.

145. Sprague, *supra* note 5, at 88 (citation omitted).

146. Fact Sheet 16, *supra* note 48.

147. *See infra* Part IV.A (discussing the impact of *City of Ontario v. Quon*).

148. Keane, *supra* note 51, at 114.

technology itself but in what society accepts as proper behavior."[149] In a similar vein, Professor Jeffrey Rosen, a noted scholar in the area of privacy law, has expressed surprise at the passivity with which Americans have acceded to encroachments into their private lives, wondering about the "tepid response to the increasing surveillance of our personal and private life."[150] Employees seem to expect—and accept—that their employers are engaging in some form of workplace monitoring. As technology makes it easier for companies to do so, their employees' expectations of privacy decrease even further.[151]

One additional and related result of this increase in technology in the workplace has been that areas of an employee's life once deemed entirely personal now have become fair game for employer scrutiny: the "personal" has begun to blur with the "professional."[152] Employees use their employer-provided cell phones to make personal calls or send personal texts; they send work-related email from their personal home computer; they may keep all of their appointments—personal and professional—on a single electronic calendar.[153] As one commentator observed, "[g]iven the ubiquity of electronic communications in both business and social life, it is unrealistic to expect that employees will never use employer-provided systems to communicate about personal matters."[154] Yet once personal data makes its way into the workplace—in particular, when such data is dragged into the workplace by the employee him or herself—does the employer have an obligation to ignore that information? While employees object strenuously to what they see as employers snooping into their personal lives, perhaps the problem is not an excessive snooping by employers, but

149. City of Ontario, California v. Quon, 130 S. Ct. 2619, 2629 (2010); *see also* Noyce, *supra* note 7, at 29 (stating that the "circumstances of the workplace and the actions taken by the employer will dictate whether an employee's expectation of privacy is reasonable"); Sprague, *supra* note 5, at 86-88 (observing that there is a link between the degree of surveillance Americans undergo and the increase in workplace monitoring).

150. Rosen, *supra* note 116, at 25.

151. Sprague, *supra* note 5, at 89.

152. *See generally* Kim, *supra* note 6, at 910-14 (citations omitted) (discussing how technological advances blur the distinction between work and home); *see also* Noyce, *supra* note 7, at 29 (noting the "growing use of technology in the workplace, [and] the feeble boundaries between work and home").

153. Kim, *supra* note 6, at 911-12 (citations omitted); *see also* Christine Neylon O'Brien, *The First Facebook Firing Case Under Section 7 of the National Labor Relations Act: Exploring the Limits of Labor Law Protection for Concerted Communication on Social Media*, 45 SUFFOLK U. L. REV. 29, 29 (2011) (discussing how "[s]martphones and other portable Internet data generators such as iPads, and even Internet hotspots incorporated into motor vehicles, have encouraged the blurring of work and personal time such that people are tethered to their devices, checking their work and personal messages wherever they are and whatever else they are doing"); Rosen, *supra* note 116, at 84 (discussing how technology has broken down boundaries between the home and the office).

154. *See* Kim, *supra* note 6, at 911 (citation omitted).

rather an *inability* by employers to separate irrelevant personal information from highly relevant, professional information.

Finally, not only has the amount of technology in the workplace increased (along with individuals' reaction to such technology), but the manner in which employees conduct themselves overall has also evolved in recent years. Individuals in all walks of life generally seem more willing to live their lives on display, not only tolerating others' efforts to monitor their behavior, but in fact often *encouraging* such attention. Many of the newest members of the workforce belong to the so-called "Facebook Generation," a group so identified because of its tendency to share the minutiae of daily life with all of their hundreds of Facebook "friends."[155] According to one self-proclaimed member of this cohort, "[m]y generation has long been bizarrely comfortable with being looked at, and as performers on the Facebook stage, we upload pictures of ourselves cooking dinner for our parents or doing keg stands at last night's party; we are reckless with our personal information."[156] Indeed, "[t]he new Internet generation doesn't seem to have the privacy hang ups or suspicions their parents had about sharing information with strangers over the net."[157]

In many ways, this over-sharing mentality facilitates and encourages employer snooping. Not only does this open and permissive attitude inherently make more information available to employers as employees more freely share their personal data, but this demeanor also actively *undermines* employees' objections to employer snooping. To a certain extent, individuals subject to monitoring seem to forget that the cameras or other surveillance devices are there: examples abound of employees who have been told that their email will be monitored, but who continue to send offensive or inappropriate messages,[158] or of individuals who "knew" that

155. *See What is the Facebook Generation?*, WISEGEEK, http://www.wisegeek.com/what-is-the-facebook-generation.htm (last visited Jan. 21, 2014) (stating that the "Facebook generation is a title used to identify those who are growing up in a world where the use of online social networking is common"); *see also* Kalena Jordan, *Social Networking and the Overshare Generation*, SITEPRONEWS (Aug. 24, 2010), http://www.sitepronews.com/2010/08/24/social-networking-and-the-overshare-generation/ (stating that "[t]he premise is that everyone in your social circle not only wants to know but NEEDS to know when you are buying that tall frappuccino from @starbucks. That they need to know precisely where you are and what you are doing every minute of the day.").

156. Alice Mathias, *The Fakebook Generation,* N.Y. TIMES (Oct. 6, 2007), http://www.nytimes.com/2007/10/06/opinion/06mathias.html?_r=0.

157. Jordan, *supra* note 155.

158. *See, e.g.*, Franklin v. MIQ Logistics, LLC, No. 10–2234–EFM, 2011 WL 3205774, at *1, *2 (D. Kan. July 28, 2011) (describing inappropriate emails sent by employee despite company policy informing employees that company could monitor computer usage, including emails, without prior notice); Ernst v. Sumner Grp., Inc., 264 S.W.3d 669, 670-71 (Mo. Ct. App. 2008) (noting that employee sent two inappropriate emails, including emails with photographs of a naked man, a picture of a woman with her breast and nipple exposed, and a racially-derogatory email, despite an email policy informing employees that they have

they were on camera but nonetheless behaved in objectively embarrassing ways.[159] Others have written about the "innate tension between an employee intentionally making information public and feeling that her information is private."[160] Employees cannot have it both ways. They cannot throw open the doors to their private lives, and then protest when they do not like who enters. While employees may claim not to be comfortable with employers monitoring their actions, their conduct often tells a different story.[161]

IV. ROLE OF THE COURTS IN PERMITTING – AND PERHAPS EVEN *ENCOURAGING* – SNOOPING

On top of the various legal and practical concerns that motivate employers to snoop, the courts themselves have played a significant role in encouraging this type of employer behavior. In some instances, the courts have adopted a surprisingly permissive attitude toward employer snooping, issuing decisions that leave employers with broad leeway to monitor employees without any legal sanction. In a handful of cases, the courts have gone even further, by actually creating strong incentives that encourage employers to snoop.

A. Uncertain Boundaries as Making Way for Employers to Snoop: The Impact of City of Ontario v. Quon

One way in which the courts contribute to many employers' decision to snoop relates to their failure to create clear legal guidelines regarding what employers can and cannot do in monitoring their workers. As discussed in detail above, the modern workplace abounds with new and

---

"no expectation of privacy" in emails sent from the employer's system).

159. In my Employment Law course, I refer to this as the "Real World Phenomenon," named after the popular MTV reality show. *See* MTV, http://www.mtv.com/search/?q=real+world (featuring a reality show documenting strangers selected to live together). *See also* Terry Morrow, *Melissa Howard talks about 'Real World,'* THECABIN.NET (Nov. 3, 2000), http://thecabin.net/stories/110300/sty_1103000054.html (commenting that despite knowing that cameras will record their every word and movement throughout the season, cast members of that show repeatedly have claimed that, after a while, they would "forget the camera is there."); Wayne Laepple, *Back in 'The Real World"* [sic], THE DAILY ITEM (June 21, 2007), http://dailyitem.com/0300_entertainment/x691265744/Back-in-The-Real-World (quoting a former cast member's advice that "[y]ou have to try to be real and forget the camera crew").

160. Noyce, *supra* note 7, at 28-29.

161. One recent study purports to find that the vast majority of workers do not mind being monitored by their employers. *See* Swisher, *supra* note 103, (claiming that "nine out of 10 workers accept or welcome having their computer activities monitored by their employers during work hours").

often cutting-edge technology—technology that has altered the manner in which many employers do business.[162] These technological developments have outpaced the law in many respects, and courts are grappling with how to fit these new devices and systems within their traditional "privacy" jurisprudence.[163] With respect to the hot-button issue of an employer's ability to monitor an employee's Facebook postings, for example, one federal judge recently observed that the courts "have not yet developed a coherent approach" for determining what expectations of privacy individuals may have in such postings.[164] This legal grey area frequently opens the door for employers to expand the extent to which they monitor their workers, either because they do not believe that there are any hard-and-fast rules that will prohibit this type of behavior, or because they simply do not know where to fix the outer boundaries of acceptable monitoring.

One telling example of the courts' failure to set boundaries with respect to employer monitoring arose in the Supreme Court's 2010 decision in *City of Ontario, California. v. Quon*. In *Quon*, the plaintiff, Jeff Quon, was employed as a police sergeant and member of the Special Weapons and Tactics Team of the City of Ontario, California Police Department.[165] In 2001, the City provided Quon and several coworkers with alphanumeric pagers to use in executing their work duties.[166] Prior to acquiring and distributing these pagers, the City had communicated to all employees a "Computer Usage, Internet and E-Mail Policy" that stated, *inter alia*, that the City "reserves the right to monitor and log all network activity including e–mail and Internet use, with or without notice."[167] While this policy did not explicitly apply to text messages, the City made clear to employees, including Quon, that it would cover text messages as well.[168]

Shortly after the City distributed these pagers, Quon exceeded his monthly text message character allotment, resulting in an additional fee for

162. *See supra* notes 51-71.

163. *See, e.g.*, Kim, *supra* note 6, at 914 (noting that "[t]he current law of privacy is not well equipped to address these developments in the workplace"); Carlin, *supra* note 102, at 1 (asserting that "[s]tate and federal common law and statutory protections developed during the past twenty years . . . fail to provide adequate protection in light of technological advances that make employer monitoring simple, cheap, and surreptitious."); Sprague, *supra* note 5, at 89-90 (focusing on "what happens when technology outstrips the law's ability to protect employees from it"); *cf.* Byrnside, *supra* note 34, at 459 (observing that "[t]his new method of employer information gathering is extremely different from its predecessors").

164. Ehling v. Monmouth Ocean Hosp. Serv. Corp., 872 F. Supp. 2d 369, 373 (D.N.J. 2012).

165. *Quon*, *supra* note 149, at 2624-25.

166. *Id.* at 2625.

167. *Id.* (citations omitted) (internal quotation marks omitted).

168. *Id.*

the City – a practice that continued in subsequent months.[169] While Quon's superior verbally represented that the City would not monitor employees' text messages so long as the employees themselves paid any overage fees,[170] the City eventually requested and reviewed the transcripts of messages sent by Quon and others (purportedly to determine the sufficiency of the existing character limit associated with the pagers).[171] Upon finding that the vast majority of messages sent by Quon during work hours were not work-related, the Police Department disciplined Quon.[172] Quon subsequently sued, claiming, *inter alia*, a violation of his privacy rights under both the Stored Communications Act and the Fourth Amendment to the Constitution.[173]

In examining the validity of Quon's claims, the Supreme Court significantly declined to decide a very basic question: Whether Quon actually *possessed* any "reasonable expectation of privacy in the text messages sent" over his employer-provided pager.[174] Noting that "[t]he Supreme Court must proceed with care when considering the whole concept of privacy expectations in communications made on electronic equipment owned by a government employer[,]"[175] the Court simply *assumed* that such a reasonable expectation of privacy existed and proceeded accordingly, ultimately holding that the City's conduct did not violate Quon's supposed "reasonable expectation of privacy" in the pager because the City's search was motivated by a legitimate work purpose and was not excessive in scope.[176]

In some respects, one can understand the Supreme Court's reluctance to stake out a position regarding whether an employee *in fact* should be deemed to have a reasonable expectation of privacy in an employer-provided pager or similar device. Noting the "[r]apid changes in the

169. *Id.* at 2625-26.

170. *Id.* at 2625.

171. *Id.* at 2626.

172. *Id.*

173. Notably, *Quon* arose in a government workplace, where employees' privacy rights may differ substantially from those applicable to private sector workers. *See supra* note 6. However, as many have observed, this case can be seen as a signal for how a court would analyze a similar dispute in the private sector. *See, e.g.*, *Unanimous U.S. Supreme Court Ruling in "Quon" Highlight Importance of Employer Technology-Usage and Privacy Policies*, GIBSON, DUNN & CRUTCHER LLP (June 18, 2010), http://gibsondunn.com/publications/Pages/USSupremeCourtRulinginQuon.aspx, (noting that "[a]lthough *Quon* involved a government employer, the importance of employment policies clearly eliminating expectations of privacy in communications made on employer-owned devices or systems is equally applicable to private-sector employers"); *cf.* Secunda, *supra* note 6 (arguing that the Court's decision in *Quon* functions to reduce privacy rights of public sector employees to the level of employees in the private sector).

174. *Quon*, *supra* note 149, at 2630.

175. *Id.* at 2629.

176. *Id.* at 2630-33.

dynamics of communication and information transmission[,]" the Court correctly observed that it likely would encounter "difficulty predicting how employees' privacy expectations will be shaped by those changes or the degree to which society will be prepared to recognize those expectations as reasonable."[177] Yet by failing to make clear to employers and employees what amount of privacy (if any) they should expect in these types of devices, the Court arguably made it easier for employers to increase their scrutiny in this area: If employers can assume that employees may *not* have a reasonable expectation of privacy in an employer-provided device, then they likely will exhibit less hesitation in monitoring its use. In other words, given the numerous very real concerns that motivate employers to snoop, many employers–in the absence of a "no" from the Supreme Court-will choose to take their chances and expand their monitoring of employees.

This idea that ambiguity from the Supreme Court could lead to increased monitoring by employers is more than mere academic speculation. In the wake of the *Quon* decision, various law firms that represent employers sent updates to their clients, advising them regarding how the Court's decision in *Quon* might enable them to engage in a similar type of monitoring. Citing the Court's observation that "employer policies concerning communications will . . . shape the reasonable expectations of their employees, especially to the extent that such policies are clearly communicated,"[178] many employer-side law firms simply advised their clients to do things like "expressly include all forms of electronic communications in written technology-usage and privacy policies, and to ensure that these policies are clearly communicated and consistently applied."[179] According to these advisors, it seems, the Court's failure to draw a clear line in *Quon* regarding the actual scope of an employee's reasonable expectation of privacy in employer-provided devices means that employers wishing to snoop into communications made on such devices simply must draft, publish and disseminate a clear warning to employees that such monitoring will occur – not a particularly heavy burden for

177. *Id.* at 2629-30.

178. *Quon*, *supra* note 149, at 2630.

179. GIBSON, DUNN & CRUTCHER, *supra* note 173; *see City of Ontario vs. Quon: The Supreme Court Weighs In On Employee Privacy Expectations*, DORSEY & WHITNEY LLP (June 23, 2010), http://www.dorsey.com/eu_le_ontariovsquon_062310/ (including in its "practical guidance" for employers advice regarding how effectively to expand the scope of an employer's communications/ monitoring policy); *Supreme Court Unanimously Upholds Employer Ability to Access and Search Employee Messages Under Reasonable Circumstances*, SIDLEY AUSTIN LLP (June 23, 2010), http://www.sidley.com/Supreme-Court-Unanimously-Upholds-Employer-Ability-to-Access-and-Search-Employee-Messages-Under-Reasonable-Circumstances-06-23-2010/ ("Clear policies should be established and implemented to ensure that monitoring and searches are reasonable in the given circumstances").

employers.[180] All it takes to strip employees of their privacy rights is a bit of notice.

B. Court-Created Incentives for Employers to Snoop: The Court's Hostile Environment and Third-Party Retaliation Jurisprudence

While the courts' failure to establish concrete limits on monitoring in cases like *Quon* arguably make it *permissible* for employers to snoop, several decisions by the Supreme Court have gone even further. In some instances, the Court has rendered decisions and established legal doctrines that not only have "opened the door" to snooping by employers, but in fact have provided strong *incentives* for employers to snoop.

1. How Hostile Environment Cases Encourage Employer Snooping

One way in which the courts actively have encouraged employers to monitor employees relates to the courts' jurisprudence in cases dealing with workplace sexual harassment. As previously discussed, many employers harbor concerns about employees using the employers' equipment in an inappropriate manner. Employees may use their workplace email account or Internet access to post pornographic, obscene

180. *See* Lazar, *supra* note 51, at 387 (stating that in applying the *Quon* Court's analysis to the private sector, "courts looking at privacy policies will likely assess whether the policy is written and communicated clearly, with appropriate notice to employees"). Notably, the Supreme Court is not the only entity guilty of injecting ambiguity into the scope of employee's privacy rights and employers' ability to monitor employees. The NLRB recently has been grappling with a similar issue, focusing on whether and how employers can regulate their employees' social media usage. *See* Dubé, *supra* note 140 (describing the NLRB's report regarding employees' social media activities). Among other guidance, the NLRB warned against overbroad social media policies and advised employers not to implement policies that might "chill" employees in their right to engage in concerted activities. *See id.* However, several commentators (generally practitioners representing employers) have criticized the NLRB's position as unnecessarily ambiguous and inconsistent in its application of the NLRA to these social media policies. *See* Parent, *supra* note 68, at *7 (arguing that "[t]here has been some inconsistency with respect to the NLRB's decisions in this area"); *see also Social Media Policies And The NLRB: What Employers Need To Know*, FENWICK & WEST LLP (Mar. 1, 2013), http://www.fenwick.com/Publications/Pages/Social-Media-Policies-And-The-NLRB-What-Employers-Need-To-Know.aspx (stating that "the NLRB's memoranda and decisions provide the only real guidance regarding the intersection between social media and Section 7 rights; unfortunately, this guidance is not intuitive for employers, at times seems inconsistent, and can be difficult to interpret"); Christopher P. Calsyn & Kris D. Meade, *Uncertain Advice In NLRB's Social Media Memorandum*, LAW360 (June 26, 2012), http://www.crowell.com/files/Uncertain-Advice-In-NLRBs-social-Media-Memoranda.pdf (observing that "[a] close review of the [NLRB's] May 30 report reveals continued inconsistent treatment of employer policies, both within this report and when compared to Solomon's earlier reports").

or other otherwise harassing images and messages.[181] Employees likewise may use social media sites to send sexually explicit or otherwise inappropriate messages to coworkers.[182] This type of conduct not only could create distractions in the workplace and undermine employee morale, but it also might create liability for the employer under Title VII's[183] prohibition against workplace harassment by creating a "hostile working environment" for employees.[184]

Under Title VII, employers have a legal obligation to take various steps to prevent and eliminate harassing behavior in the workplace.[185] In many cases, employers must do more than simply wait for employees to come forward with complaints about harassing behavior before reacting to those complaints. Rather, employers frequently possess an *affirmative obligation* to prevent and eliminate harassing behavior. In its twin decisions of *Faragher v. City of Boca Raton*[186] and *Burlington Industries, Inc. v. Ellerth*,[187] the Supreme Court held that an employer may have vicarious liability to an employee who is subjected to unlawful harassment by a supervisor with authority over that employee.[188] According to the Court, however, if the supervisor's conduct did not result in a tangible employment action for the employee in question (i.e., a termination, demotion, or other negative change in the terms and conditions of employment), the employer may be able to avoid some or all of its liability *if* the employer can show (i) that it exercised reasonable care to prevent and promptly correct any sexually harassing behavior; and (ii) that the employee unreasonably failed to take advantage of any preventative or corrective opportunities provided by the employer or otherwise to avoid the harm.[189] In other words, an employer taking this type of preventative action can assert an affirmative defense against sexual harassment liability.

But, if an employer's defense in these types of hostile environment cases will depend, *inter alia*, on its efforts to "prevent and promptly correct" any sexually harassing behavior, how should the employer go about availing itself of this defense? What steps should the employer take

181. *See supra* notes 15-16 and accompanying text.

182. *See id.*

183. 42 U.S.C. §§ 2000e-2000e-17 (2005), amended by Civil Rights Act of 1991, 42 U.S.C. § 1981a (2005) ("Title VII").

184. *See* Sprague, *supra* note 5, at 112-13 (citations omitted); *see also* Ciocchetti, *supra* note 13, at 285 (citation omitted).

185. *See generally Enforcement Guidance for Vicarious Employer Liability for Unlawful Harassment by Supervisors*, EQUAL EMPLOYMENT OPPORTUNITY COMMISSION, June 18, 1999, *available at* http://www.eeoc.gov/policy/docs/harassment.html.

186. 524 U.S. 775 (1998).

187. *Id*.

188. *See* Sprague, *supra* note 5, at 112.

189. *Id*.

to learn about this inappropriate behavior in the first place, and then to ensure that the behavior does not continue? The most effective way for an employer to do so will be by monitoring employee behavior.

Notably, in his dissent in *Ellerth*, Justice Thomas seemed to predict the extent to which this affirmative defense could incentivize employers to monitor their employees. Thomas argued that "[s]exual harassment is simply not something that employers can wholly prevent without taking extraordinary measures – constant video and audio surveillance, for example – that would revolutionize the workplace in a manner incompatible with a free society."[190] Privacy scholar Jeffrey Rosen has expressed a similar concern, arguing that "[b]ecause it is difficult to know in advance what kind of sexually related behavior or speech a reasonable juror might find hostile or offensive, prudent employers have a strong incentive to monitor and punish far more private speech and conduct than the law actually forbids."[191] Indeed, according to Rosen, the courts have "creat[ed] a liability regime where monitoring of employees' speech and behavior is a matter of corporate self-interest."[192]

If employers have an obligation to prevent harassing behavior in the workplace – and in fact, can avoid liability by showing that they took appropriate steps to do so – then one would expect them to use all readily available tools to fulfill this obligation. In many instances, that may mean monitoring employees' email, Internet usage, social media posts and other behaviors, to make sure that inappropriate language and/or conduct is not entering the workplace. In this way, by providing employers with a tremendous legal advantage (and thus, indirectly, a financial benefit) linked to finding out about inappropriate workplace conduct, the Court actively encourages employers to monitor their employees.

2. How the Court's Third-Party Retaliation Jurisprudence Encourages Employer Snooping

A more subtle example of the Supreme Court providing employers with an incentive to snoop arose in the January 2011 case *Thompson v. North American Stainless, LP*.[193] In *Thompson*, the plaintiff, Eric

190. *Ellerth*, 524 U.S. at 770, (Thomas, J., dissenting) (citation omitted); *see also* Rosen, *supra* note 116, at 80 ("Most people are surprised to learn that sexual harassment law does not impose liability on sexual harassers. Instead, it puts the full weight of responsibility on their employers").

191. Rosen, *supra* note 116, at 13.

192. *Id.* at 79.

193. Thompson v. N. Am. Stainless, LP, 131 S.Ct. 863 (2011) (rev'd S.Ct. 863 (2011)). This Section draws upon ideas previously explored in this author's earlier work, Jessica Fink, *Protected by Association? The Supreme Court's Incomplete Approach to Defining the Scope of the Third-Party Retaliation Doctrine*, 63 HASTINGS L.J. 521 (2011) (examining

Thompson, worked for the defendant North American Stainless, LP ("North American"), as did his then-fiancée Miriam Regalado.[194] Thompson claimed that shortly after Regalado filed a discrimination charge against North American, North American terminated Thompson's employment.[195] According to Thompson, North American fired him solely in retaliation for Regalado's protected activity.[196]

Thompson's claim implicated an area of jurisprudence under Title VII known as the "third-party retaliation doctrine." In a "typical" retaliation case, a plaintiff will claim (i) that he or she engaged in some "protected activity" for purposes of Title VII;[197] (ii) that he or she suffered some adverse employment action; and (iii) that there is some causal connection between the protected activity and the adverse action.[198] Thus, an employee might assert a retaliation claim if he was fired or denied a promotion because he had engaged in some "protected activity," perhaps by filing a charge of discrimination or bringing a Title VII lawsuit against his or her employer.[199]

Third-party retaliation claims are slightly different. Third-party retaliation claims generally arise when an employee claims to have received adverse treatment from an employer *not* due to any conduct engaged in by that employee himself, but rather due to conduct engaged in by another employee. "For example, Joe Senior gets fired because his son, Joe Junior, filed a discrimination charge against their mutual employer;

Thompson and its potential impact on both employers and employees).

194. *See Thompson*, 567 F.3d at 806 (holding that employee who was terminated after his fiancée filed gender discrimination charge was not a member of a protected class and Title VII does not create a cause of action for third-party retaliation for persons who have not personally engaged in protected activity).

195. *Id.*

196. *Id.*

197. There are two categories of "protected activity" recognized for purposes of a retaliation claim under Title VII. First, the "participation clause" within Title VII's retaliation provision prohibits employers from taking adverse action against employees who "ha[ve] made a charge, testified, assisted, or participated in any manner" in the investigation or litigation of any discrimination complaint. 42 U.S.C. § 2000e-3(a). Second, the "opposition clause" of the statute protects employees who have "opposed any practice made an unlawful employment practice" under Title VII. 42 U.S.C. § 2000e-3(a).

198. *See* Fogleman v. Mercy Hosp., Inc., 283 F.3d 561, 567-58 (3rd Cir. 2002) (citation omitted) (reversing lower court dismissal because plaintiff presented a cognizable claim against his employer); Little v. Windermere Relocation, Inc., 301 F.3d 958, 969 (9th Cir. 2002) (citation omitted) (holding that employee established a prima facie case of retaliation under Title VII by showing a causal connection between involvement in a protected activity and adverse employment action).

199. *See e.g.*, Decker v. Andersen Consulting, 860 F. Supp. 1300 (N.D. Ill. 1994) (allowing retaliation claim to proceed where employee presented genuine issue of material fact that employer reduced her responsibilities and terminated her employment in response to her filing EEOC charge of discrimination and informing employer of intent to pursue discrimination claim).

Wendy Wife is demoted because her spouse and coworker, Harry Husband, called the EEOC to report workplace discrimination."[200] These situations represent a twist on the traditional retaliation claim that Title VII allows.

Thompson's claim in suing North American was essentially this: Thompson did not claim that he personally engaged in any protected activity, such as by assisting Regalado in filing her discrimination charge or otherwise opposing North American's alleged treatment of Regalado.[201] Rather, Thompson explicitly alleged in his complaint "that his 'relationship to Miriam Thompson [nee Regalado] was the sole motivating factor in his termination.'"[202] While many courts – including every federal court of appeals to consider the issue – previously had held that claims of "third-party retaliation" fell outside of Title VII's retaliation provision,[203] the U.S. Supreme Court in *Thompson* ultimately decided that this claim could proceed, finding that Thompson could allege a third-party retaliation claim based upon Regalado's protected activity.[204]

In reaching this conclusion, however, the Court inadvertently may have created a strong incentive for employers to snoop. While the Court held that Title VII would permit third-party retaliation claims, it expressly declined to provide *any* specific guidance regarding what *types of relationships* that could support these types of claims.[205] Instead, the Court merely stated that lower courts should examine the "particular circumstances" in any given case to determine whether to recognize a claim of third-party retaliation,[206] emphasizing only that "the provision's standard for judging harm must be objective," as opposed to relying upon a plaintiff's subjective feelings.[207] In other words, the Court held that Title VII (sometimes) would permit third-party retaliation claims, without outlining any guidelines defining the scope of such claims.[208]

Ironically, the Court adopted this rather broad view despite the fact

---

200. *See* Fink, *supra* note 193, at 526-27 (discussing the assertion of third-party retaliation claims under Title VII).

201. *See Thompson*, *supra* note 194, at 805-06 (observing that Thompson did not claim that he personally engaged in any protected activity).

202. *Id.* at 806; *see also id.* at 808 (observing that Thompson's "Statement of the Issue" on appeal and "Statement of Facts" also made clear that Thompson's retaliation claim was based upon the protected activity of his *fiancée*, as opposed to any activity that he engaged in himself).

203. *See* Fink, *supra* note 193, at 527-28 (citations omitted) (discussing the approach taken by federal courts prior to *Thompson* in denying third-party retaliation claims).

204. *Thompson*, *supra* note 193, at 867.

205. *See id.* at 868. ("We must also decline to identify a fixed class of relationships for which third-party reprisals are unlawful.").

206. *Id.*

207. *Id.* (citations omitted) (internal quotation marks omitted) (parenthesis in original).

208. *See* Fink, *supra* note 193, at nn.52-56 and accompanying text (citations omitted) (explaining the Court's decision in *Thompson*).

that, during the oral argument of this case, several justices appeared to fret about the boundaries of the third-party retaliation doctrine. For example, Justice Alito questioned Thompson's counsel, asking "[s]uppose Thompson were not Regalado's fiancée at the time. Suppose they were . . . just good friends . . . . The way the company wanted to get at her was by firing her friend. Would that be enough?"[209] Advocating for what he referred to as a "clear line" in this area, Justice Alito observed, "I can imagine a whole spectrum of cases in which there is a lesser relationship between these two persons, and . . . unless there's a clear line there someplace, this theory is rather troubling."[210] Chief Justice Roberts expressed similar concerns, inquiring of the Deputy Solicitor General (who also was arguing in favor of Thompson), "[h]ow are we supposed to tell, or how is an employer supposed to tell, whether somebody is close enough or not?"[211]

Among the many possible ramifications from the Court's intentional lack of clarity in this case regarding the scope of the third-party retaliation doctrine,[212] one notable concern is the extent to which this ambiguity has the potential to erode employee privacy. By merely stating that employers might be liable for taking adverse action against an employee if the employee has a "sufficiently close relationship" with a coworker who has engaged in protected activity – and by not elaborating on *what types* of relationships will satisfy this criterion – the Court forces employers to potentially make important employment decisions based upon incomplete information. A cautious employer might want to assume that a court will give this doctrine the broadest possible scope, encompassing even relatively casual relationships within the ambit of the doctrine. Thus, in order to assess the risk of taking adverse action against an employee, such a risk-averse employer may want to know, *prior* to taking adverse action against an employee, *all* of the workplace relationships of that employee—whether the employee is married to, dating, or perhaps mere lunchroom buddies with a coworker who previously engaged in some protected activity. As Justice Alito observed during the oral arguments in *Thompson* (despite ultimately signing on to the Majority's decision):

> Put yourself in the – in the shoes of an employer, and you . . . want to take an adverse employment action against employee A. You think you have good grounds for doing that, but you want –

209. Transcript of Oral Argument at 10-11, Thompson v. N. Am. Stainless, LP, 131 S. Ct. 863 (2011) (No. 09-291) [hereinafter "Thompson Oral Argument Transcript"].

210. *Id.* at 12.

211. *Id.* at 20.

212. *See generally* Fink, *supra* note 193, at 561-66 (arguing that the Court should have provided a more detailed framework regarding the factors to be used in conducting analyses of third-party retaliation claims).

> before you do it, you want to know whether you're potentially opening yourself up to a retaliation claim. Now, what is the employer supposed to do then? They say . . . we need to survey everybody who is engaged in protected conduct, and now we need to see whether this person who we're thinking of taking the adverse employment action against has a . . . 'close relationship' with any of those people.[213]

In this way, the Court's failure to set clear boundaries regarding the scope of the third-party retaliation doctrine gives employers a strong incentive to snoop. Those employers who are able to ferret out their employees' personal workplace relationships may minimize (or at least get an early handle on) the potential liability associated with some contemplated adverse action – a high-value result for many employers. While employees may find these inquiries into their private lives troublesome and intrusive, the Supreme Court has created a framework that actively encourages this type of behavior by employers.

V. OBLIGATIONS IMPOSED ON SNOOPING EMPLOYERS

While employers frequently possess strong incentives to snoop and often do so for legitimate reasons, that does not mean that they should have unfettered access to all aspects of their employees' private lives. To the contrary, in permitting some monitoring by employers, the courts should establish clear limits on when and how employers can monitor lawfully.

Perhaps the most significant limit that should be placed on monitoring by employers relates to employers' motivations for snooping: Simply because employers *can* snoop does not always mean that they should. Rather, employers wishing to investigate prospective or current employees should have to provide a legitimate justification for doing so. Indeed, courts could adopt the analytical framework used in disparate impact discrimination claims. There, once an employee has shown that an employer has a policy or practice that has a disparate impact on members of a particular racial group (or other protected class), the employer has the burden of proving that the policy or practice in question is job related for the particular position at issue and consistent with business necessity.[214] If the employer meets this burden, then the burden will shift to the plaintiff to show that there is a less discriminatory alternative that meets the business need and that the employer refuses to adopt that alternate approach.[215]

Courts could adopt a similar approach to claims of unwarranted

213. *Thompson* Oral Argument Transcript, *supra* note 209, at 17-18.

214. EEOC Compliance Manual § 15-V.B at 21, EQUAL EMP'T OPPORTUNITY COMM'N, Mar. 19, 2006, *available at* http://www.eeoc.gov/policy/docs/race-color.html#VB.

215. *Id.* at 21-22 (citation omitted).

employer snooping. Once an employee demonstrated that a policy or practice by his or her employer intruded into an area in which the employee possessed a reasonable expectation of privacy, the court could require the employer to show that the intrusion was related to the position in question and that the monitoring was serving a real business need. If the employer could satisfy this burden, then the plaintiff could only prevail by establishing a less intrusive manner for gathering the information in question and showing that the employer had declined to adopt this less restrictive approach.

For example, a private high school might adopt a policy barring teachers and other staff from "friending" any current students on Facebook, and might require covered employees to allow the school administration to review periodically the complete list of their Facebook "friends." If a teacher or staff member claimed that this policy violated his or her reasonable expectations of privacy, the school could argue a legitimate business need to avoid any appearance of impropriety or favoritism by staff. The objecting employee then would have to argue that the school could accomplish this goal through less intrusive means (such as by including in the contracts for applicable teachers and staff a provision in which they agreed not to "friend" any students).

In addition to justifying the reason for an intrusion, employers should also be required to take steps to verify any information that they receive before acting on it, particularly when gathering information as part of the hiring process. While technological advances and increased monitoring may greatly expand the amount of information available to employers, the quality of that information is often questionable at best.[216] As discussed above, "traditional" information gathering tools such as honesty tests and other psychological exams are of dubious reliability.[217] Moreover, background checks or general Internet searches may turn up information about the wrong individual, especially if the candidate or employee has a fairly common name.[218] In one case, a woman interviewing for a job as a sales clerk was denied the position after a criminal record check turned up arrest records for criminal prostitution and drug possession – arrest records that actually belonged to a different individual with the same name.[219] In another incident, a man on the brink of being hired for a truck driving job

216. *See, e.g.*, Wells, *supra* note 49 (describing the denial of employment to an applicant based on an erroneous shoplifting report).

217. *See* Stabile, *supra* note 42 and accompanying text.

218. *See* Josh Brodesky, *Background Checks Prone to Mistakes, Can Shut Out Jobs*, USA TODAY (Nov. 20, 2012, 1:20 PM), http://www.usatoday.com/story/money/business/2012/11/20/background-screening-gone-wrong/1716439/ (highlighting the question of the accuracy of background checks especially in cases where a person has a common name).

219. *See* Wells, *supra* note 49 (describing the case of Katrina Haines).

lost the position after a background check incorrectly labeled him a convicted pedophile.[220] Even an individual's own Facebook account may contain misleading or inaccurate information, given the ability of anyone to "tag" another individual in a posting or photograph, often without that individual's knowledge or consent.[221]

In the context of employee references, as discussed above, employers enjoy a qualified privilege to *provide* information to another employer, so long as the employer does not communicate false information about an employee "with malice."[222] However, perhaps the courts should impose more stringent obligations on the employer-recipients of this and other information, requiring employers to make reasonable efforts to confirm the accuracy of any information before using it as the basis for an adverse employment decision. In so doing, the courts could strike a proper balance between allowing employers broad latitude to gather information about their employees and applicants, while providing some protection against employees suffering harm from false or misleading information.

CONCLUSION

The debate over the proper scope of employee privacy in the workplace will continue to attract significant attention in years to come. According to a recent study by the U.S. Department of Labor Wage and Hour Division, laws addressing worker privacy were among the most common new pieces of labor and employment legislation enacted by states in 2012.[223] As a competitive business climate renders employers

220. *See* Olivera Perkins, *Errors in Background Checks Cost Job Seekers*, PLAIN DEALER (Dec. 15, 2012, 8:03 PM), http://www.cleveland.com/business/index.ssf/2012/12/job_applicants_lose_out_as_err_1.html.

221. Paul Boutin, *How to Block Facebook Photos of Yourself*, N.Y. TIMES GADGETWISE (May 5, 2009, 7:40 PM), http://gadgetwise.blogs.nytimes.com/2009/05/05/how-to-block-facebook-photos-of-yourself/ ("There is no way to prevent someone from tagging a photo with either your username, or your name as a tag. What's possible is you can prevent other users from searching for photos of you."); *see also* Jenna Wortham, *New Facebook Location Feature Sparks Privacy Concerns*, N.Y. TIMES BITS BLOG (Aug. 18, 2010, 9:44 PM), http://bits.blogs.nytimes.com/2010/08/18/new-facebook-location-feature-sparks-privacy-concerns/ (highlighting an application called Facebook Places that allows users to "tag" an accompanying friend and post his or her location to Facebook).

222. *See* Befort, *supra* note 45 and accompanying text.

223. *See* John J. Fitzpatrick, Jr. & James L. Perrine, *State labor legislation enacted in 2012*, MONTHLY LAB. REV. 24 (Feb. 2013) (tabling all enacted state labor legislation for 2012); *see also States Targeted Worker Privacy, Trafficking In Labor Legislation Last Year, DOL Reports*, 47 DAILY LAB. REP. A-7 (Mar. 5, 2013) ("For the second consecutive year, the most legislative activity came in the worker privacy category, as 30 bills related to the subject were passed in 20 states during 2012."). Legislators passed 31 worker privacy-related laws in 20 states in 2011. *Id.*

increasingly more concerned about protecting their financial assets, proprietary information, reputation, and other resources—and as technological advancements make it progressively easier for employers to engage in novel methods of monitoring their employees—questions about the limits on employer snooping will continue to occupy a dominant place in our legal, social, and political conversations.

This article is not intended as a defense of every action that an employer may take to gather information about a prospective or current employee. Without a doubt, abuses of employee privacy can and do occur. The limited privacy rights applicable to private sector employees means that employers have significant latitude with respect to the actions that they legally can take in monitoring their workers. However, there may be many situations where simply because an employer legally *can* engage in a particular type of monitoring, it might not be prudent or proper for the employer to do so. This article has not discussed the negative impact on morale that might result from extensive employer snooping—an impact that might be substantial in some cases.[224] Nor has this article discussed whether there are certain areas of an employee's private life that simply should remain off limits to snooping from a moral perspective.[225]

The purpose of this article is to put the "problem" of employee snooping in a more realistic and nuanced context. With the media in an uproar over alleged privacy invasions by employers, with legislators responding with predictable bluster, and with members of the public predictably confused about their rights, there is some benefit to putting this putative problem in perspective. Concerns about employees' rights must include consideration of the rights and responsibilities of employers as well—the right of an employer to protect itself from financial injuries or legal exposure; the responsibility to protect its shareholders from unnecessary loss; the responsibility to protect its employees from a host of

224. *See* Jay P. Kean, *Cyber-Working or Cyber-Shirking?: A First Principles Examination of Electronic Privacy in the Workplace*, 54 FLA. L. REV. 289, 320 (2002) (detailing the impact of monitoring on employees' psychology and on overall morale, stating that monitoring "takes its toll on workers and companies in terms of stress, fatigue, apprehension, motivation, morale, and trust; this results in increased absenteeism, turnover, poorer management, and lower productivity, not to mention higher health-care costs. Thus, monitoring may spoil the workplace environment, and it can have a detrimental effect on productivity") (citations omitted) (internal quotation marks omitted).

225. *See* Frank J. Cavico, *Invasion of Privacy in the Private Employment Sector: Tortious and Ethical Aspects*, 30 HOUS. L. REV. 1263 (1993) (addressing the legal and moral issues developing in the field of employee privacy); *see also* Bahaudin G. Mujtaba, *Ethical Implications of Employee Monitoring: What Leaders Should Consider*, J. APPLIED MGMT. & ENTREPRENEURSHIP, July 2003, at 22, *available at* http://www.huizenga.nova.edu/Jame/articles/employee-monitoring.cfm (examining the ethical implications of employee monitoring and recommending employers exercise restraint).

physical, mental, and other harms; and the responsibility to protect the public from what might result if employers were to make important hiring and other work-related decisions based upon dangerously incomplete information. We cannot maintain a framework where a lack of information subjects employers to significant risks and potential liability, and then stymies employers' reasonable efforts to gather that information in a reasonable manner.