American Business Law Journal

ACADEMY OF LEGAL STUDIES IN BUSINESS

American Business Law Journal
Volume 49, Issue 1, 63–124, Spring 2012

Blurred Boundaries: Social Media Privacy and the Twenty-First-Century Employee

Patricia Sánchez Abril, Avner Levin,** and Alissa Del Riego****

INTRODUCTION

In his groundbreaking book on social psychology, Erving Goffman proposed that human beings control others' impressions of them through performances within spatially defined social establishments.[1] He described a social establishment as "any place surrounded by fixed barriers to perception in which a particular kind of activity regularly takes place."[2] Through these performances, Goffman posited, individuals create and tailor their social identities for particular audiences. He argued that each performance's audience must be segregated from the others for the performances to succeed. That is, an individual must "ensure that those before whom he plays one of his parts will not be the same individual before whom he plays a different part in another setting."[3] Individuals preserve audience segregation by following the rules of decorum of each social situation and by filtering the information about themselves available

---

*Assistant Professor of Business Law, University of Miami School of Business Administration; B.A., Duke University, 1996; J.D., Harvard Law School, 2000.

**Associate Professor and Chair, Law & Business Department, Ted Rogers School of Management, Ryerson University. I wish to thank the Cegla Center for Interdisciplinary Research of the Law at the Buchman Faculty of Law, Tel Aviv University, where I worked on drafts of this article as a visiting scholar during 2011.

***J.D. Candidate, 2012 Harvard Law School; B.A., University of Miami, 2009.

[1] Erving Goffman, The Presentation of Self in Everyday Life (1959).

[2] *Id.* at 238.

[3] *Id.* at 49.

to each audience. When the veil of audience segregation is pierced, according to Goffman, social disruption ensues. The disclosure of information to unintended audiences discredits the construction of roles and identities within the group and causes "difficult problems in impression management."[4]

The workplace is perhaps the quintessential social establishment where performers "cooperate to present to an audience a given definition of the situation."[5] Professionalism is the language of the traditional workplace performance. It includes conduct and appearance that demonstrate good judgment, a respectable stature, and the maintenance of "an air of competency and a general grasp of the situation."[6] To that end, traditional professionalism demands audience segregation between the employee's professional and private personas.

Goffman's seminal text was written in 1959, well before the digital revolution changed our vehicles of social interaction. Today, technology makes the boundaries between the professional and personal more porous. The social establishments bounded by physical space about which Goffman wrote are no longer barriers for social performances and perceptions. Personal blogs, social media profiles, Tweets, and other online fora allow individuals to publicly express multiple facets of themselves, including their private lives and their opinions. Employer-provided laptops and mobile devices do not discriminate between private and professional communications or locations. These "boundary-crossing" technologies blur the already elusive line between the private and the public, the home and the workplace. Private information that was previously segregated now becomes easily accessible to employers, colleagues, recruiters, and clients, among other perhaps unintended audiences. By its nature, digital information is infinitely transferable and hard to control. This openness has far-reaching effects on personal privacy, reputation, and self-expression.

Privacy law in the United States has traditionally been defined by physical and social establishments like those described by Goffman. The reasonable expectation of privacy analysis, which is endemic to privacy jurisprudence, is firmly rooted in the experience of physical space and its

---

[4]*Id*. at 139.

[5]*Id*. at 238.

[6]*Id*. at 47.

surrounding normative circumstances. The evaluation of whether privacy expectations reasonably exist is present in nearly every assessment of privacy under U.S. law, from torts to statutory rights. In a recent case, *City of Ontario v. Quon*, the U.S. Supreme Court was charged with qualifying the privacy expectations of an employee in a social establishment not defined by physical boundaries: text messages.[7] Officer Quon claimed a violation of privacy when his employer searched the personal text messages he sent on his employer-provided pager.[8] The Court eschewed making what it deemed would be premature legal conclusions regarding privacy and technology, stating that "rapid changes in the dynamics of communication and information transmission [are] evident not just in the technology itself but in what society accepts as proper behavior."[9] It admitted having "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."[10]

Like the U.S. Supreme Court, other tribunals and lawmakers around the world are having trouble conceptualizing privacy in new technologies. In Europe, courts and legislatures alike are debating the wisdom of a proposed "right to be forgotten," an individual right that allows citizens to delete unwanted information online about them.[11] The Canadian Supreme Court has echoed the U.S. Supreme Court's reticence, opting to "leave the privacy implications of the more evolved technology to be decided when a comprehensive evidentiary record has been developed."[12]

The shared unease among lawmakers around the world suggests that they need more information to gauge privacy and behavioral norms for new technologies. Without clear instruction from the law or a crystal ball, indicators of normative views are the best way to forecast how expectations

---

[7]130 S. Ct. 2619, 2625 (2010).

[8]*Id*.

[9]*Id*. at 2629.

[10]*Id*. at 2630.

[11]Matt Warman, *Online Right "To be Forgotten" Confirmed by EU*, Telegraph (Mar. 17, 2011, 12:53 PM), http://www.telegraph.co.uk/technology/Internet/8388033/Online-right-to-be-forgotten-confirmed-by-EU.html.

[12]R. v. Gomboc, [2010] 3 S.C.R. 211, para. 40 (Can.); *see also* R. v. Tessling, [2004] 3 S.C.R. 432, para. 55 (Can.) ("Whatever evolution occurs in future will have to be dealt with by the courts step by step. Concerns should be addressed as they truly arise.").

of privacy are being shaped in new contexts and technologies. In this article, we canvass existing domestic and international jurisprudence on social media and related technologies in the workplace, in tandem with the self-reported privacy expectations of the emerging workforce. We analyze the findings of a survey conducted on two university campuses that asked various questions of business students who were imminently entering the workforce to ascertain their privacy expectations regarding social media in the workplace. While legislatures and courts have waffled in characterizing privacy expectations in social media, the rising generation of workers already manifests certain beliefs about the technology as it plays out in work life. Our findings suggest that Millennials[13] are cognizant of their reputational vulnerability on digital media but are not willing to sacrifice Internet participation to segregate their multiple life performances. Lacking the technological or legal ability to shield performances, Millennials rely on others, including employers, to refrain from judging them across contexts. Their stated expectations of privacy, therefore, appear to be somewhat paradoxical: employee respondents generally want privacy from unintended employer eyes, and yet they share a significant amount of personal information online, knowing it could become available to employers and others. What is at the core of this seemingly contradictory behavior? Is it just an adolescent "have my cake and eat it too" mentality, or does it reveal something deeper about privacy and social performances? Should legal doctrines and business practices acknowledge this expectation?

Informed by our empirical findings, we address these questions and offer recommendations about the future of law and business practices in a digital world. These recommendations strike a balance between employees' dignitary interests and employers' practical realities. The ways that law and society respond to the multiple issues presented by boundary-crossing technologies will certainly affect the evolution of technology, the demands of the twenty-first-century workplace, and individual autonomy.

In Part I, we provide an overview of the extant legal landscape with an emphasis on three general areas of employer activity related to employees' online activities: (1) monitoring and surveillance of employee social media profiles, (2) evaluation of applicants' social media profiles and online speech in making hiring decisions, and (3) limiting

---

[13]Neil Howe & William Strauss, Millennials Rising: The Next Great Generation 4 (2000) (defining Millennials as those "born in or after 1982").

employees' off-duty online activities. In Part II, we report the findings of an empirical project assessing young employees' expectations regarding the role of technology, particularly social media, in the workplace.[14] The survey asked respondents about a wide range of topics related to social media, such as the extent of personal information they post online, the privacy-protective measures they employ on social media sites, their level of concern regarding their privacy online, and their attitudes and expectations regarding the use of social media in the workplace. Despite granting employers access to information about their private lives by participating online, respondents expect that work life and private life should be generally segregated—and that actions in one domain should not affect the other. Guided by the survey findings and legal examples from international jurisdictions, in Part III we discuss the future of employee privacy in social media and offer workable recommendations designed to protect employees' desire to maintain some separation between personal and professional contexts.

I. The Law on Social Media in the Workplace

Whether it involves using employer computers to check personal e-mail and social network profiles or sending text messages on employer-provided communications devices, employee use of boundary-crossing technologies in the workplace for personal purposes is prevalent.[15] Social

---

[14]The findings discussed in this article are part of a larger research project we conducted regarding the basic questions of online conduct and social media usage. The same survey was administered to university students at Ryerson University, Canada, and the University of Miami in Coral Gables, Florida. The Canadian portion of the project was funded by the Privacy Commissioner of Canada's Contributions Program and those data were reported to the Privacy Commissioner of Canada. For the full Canadian report, see Avner Levin et al., Privacy and Cyber Crime Inst., The Next Digital Divide: Online Social Network Privacy (2008), *available at* http://www.ryerson.ca/tedrogersschool/privacy/Ryerson_Privacy_Institute_OSN_Report.pdf. In 2009, some of the aggregate Canadian and American data relating to general expectations of privacy were published in the *Vanderbilt Journal of Entertainment and Technology Law*. Avner Levin & Patricia Sánchez Abril, *Two Notions of Privacy Online*, 11 Vand. J. Ent. & Tech. L. 1001 (2009). This article focuses on the aggregate data particular to the employment context. We refer to and cite the 2009 article throughout for general propositions regarding the survey and its overall findings.

[15]*See, e.g.*, Corey A. Ciocchetti, *Monitoring Employee E-mail: Efficient Workplaces Vs. Employee Privacy*, 2001 Duke L. & Tech. Rev. 0026 (2001), *available at* http://www.law.duke.edu/

media, in particular, has permeated modern culture and the daily lives of the incoming workforce.[16] Both businesses and individuals view sites like Facebook and Twitter as valuable marketing and communication tools.[17] However, given these sites' relative newness and the ill-defined norms surrounding them, their use across work/life contexts raises numerous legal, ethical, and business-related questions.

Accounts of employees discrediting themselves and their employers via postings on social networking and media sites have become ubiquitous. A high school teacher was dismissed after posting on her Facebook page that she thought residents of the school district were "arrogant and snobby" and that she was "so not looking forward to another year [at the school]."[18] A flight attendant was fired for posting suggestive pictures of

---

journals/dltr/articles/2001dltr0026.html (discussing employee use of personal e-mail in the workplace); Cindy Krischer Goodman, *Cellphones Raise Workplace Issues*, Miami Herald, Feb. 2, 2011, at B6, *available at* http://www.miamiherald.com/2011/02/01/2045915/cellphones-raise-workplace-issues.html (discussing employee use of personal cell phones in the workplace); Cindy Krischer Goodman, *Social Networks Test Companies' Boundaries*, MiamiHerald.com (Jan. 19, 2011), http://www.miamiherald.com/2011/01/18/2022458/social-networks-test-companies.html (discussing the use of online social networks in the workplace).

[16]Facebook, MySpace, Twitter, and LinkedIn boast a combined 1045 million worldwide users, with Facebook accounting for seventy-two percent of that figure (despite first reaching 250 million users in just 2009). *See* Statistics, Facebook.com, http://www.facebook.com/press/info.php?statistics (last visited Aug. 11, 2011); *see also* About Us, Linkedin.com, http://press.linkedin.com/about (last visited Aug. 11, 2011); Nicholas Carlson, *Chart of the Day: How Many Users Does Twitter Really Have?* Business Insider (Mar. 31, 2011, 6:20 PM), http://www.businessinsider.com/chart-of-the-day-how-many-users-does-twitter-really-have-2011-3; *Company Timeline*, Facebook.com, http://www.facebook.com/press/info.php?timeline (last visited Aug. 11, 2011).

[17]*See* Robert Ball, *Social Media Marketing: What's the Payoff for Your Business*, Huffington Post (Feb. 24, 2011, 6:00 PM), http://www.huffingtonpost.com/robert-ball/do-you-know-how-social-me_b_826802.html (reporting a survey that found seventy percent of small businesses use social media for marketing); David Bayer, *Social Media Marketing—Using Twitter and Facebook to Grow Your Business and Maintain Relationships*, Mortgage News Daily (Nov. 12, 2009, 11:18 AM), http://www.mortgagenewsdaily.com/channels/community/118706.aspx (providing a primer for marketing on Facebook and Twitter and noting that "[s]ocial media marketing has been on the rise for the past several years"); Josh Halliday, *Twitter and Facebook Under Scrutiny as ASA Polices Online Marketing*, Guardian (Mar. 1, 2011, 6:01 AM), http://www.guardian.co.uk/media/2011/mar/01/twitter-facebook-online-marketing-asa (reporting that the United Kingdom's Advertising Standards Authority extended its regulatory oversight to include companies' online marketing).

[18]*H.S. Teacher Loses Job Over Facebook Posting*, BostonChannel.com (Aug. 18, 2010, 7:06 AM), http://www.thebostonchannel.com/r/24670937/detail.html.

herself in her company uniform.[19] A study reported medical students engaged in unprofessional banter and disclosure about patients on their social networking profiles.[20] Two pizza chain employees were fired after posting a "prank" video on YouTube that showed them preparing sandwiches at work while one put cheese up his nose and mucus on the food.[21] Whether these well-documented anecdotes reflect ill-advised judgment of employees or overly aggressive responses by employers, they exemplify the tension between employer interests and employee privacy and speech rights.

Employer intrusion into an employee's personal life threatens the employee's freedom, dignity, and privacy—and may lead to discriminatory practices. A considerable body of business research indicates that employer invasiveness may lead to higher levels of employee stress, lower levels of productivity, and worse employee health and morale.[22] Despite documented adverse effects, employee monitoring and surveillance remain pervasive in the business world.[23] Employers have compelling business

---

[19]Complaint, Simonetti v. Delta Airlines Inc., No. 1:05-cv-2321 (N.D. Ga. Sept. 7, 2005), 2005 WL 2897844 (stayed pending Delta bankruptcy proceedings).

[20]Katherine C. Chretien et al., *Online Posting of Unprofessional Conduct by Medical Students*, 302 J. Am. Med. Ass'n 1309 (2009).

[21]Stephanie Clifford, *Video Prank at Domino's Taints Brand*, N.Y. Times, Apr. 16, 2009, at B1.

[22]*See* Frederick S. Lane III, The Naked Employee: How Technology Is Compromising Workplace Privacy 11–16 (2003) (describing increased workplace surveillance as "inherently destructive of employee morale" and the Web as a "seductive" drain to employee productivity); Maureen L. Ambrose et al., *Electronic Performance Monitoring: A Consideration of Rights*, *in* Managerial Ethics: Moral Management of People and Process 61, 69–72 (Marshall Schminke ed., 1998) (discussing the fact that employer video surveillance, eavesdropping, and computer monitoring generally can lead to employee stress, worsening health, and declining productivity); Jeffrey M. Stanton, *Traditional and Electronic Monitoring from an Organizational Justice Perspective*, 15 J. Bus. & Psychol. 129, 130, 142–45 (2000) (discussing how employee monitoring and its particular use in the workplace can affect whether employees feel they are being treated fairly, which may affect job satisfaction).

[23]Although the terms "monitoring" and "surveillance" are used in the literature somewhat interchangeably, we use "monitoring" to refer to the automated, computerized collection of information. In contrast, we use "surveillance" to focus on the human review of activities or collected data. Monitoring of electronic communication is routine in the workplace, while surveillance is not. Surveillance is usually triggered by the employer's suspicion of employee misconduct. *See* Corey A. Ciocchetti, *The Eavesdropping Employer: A Twenty-First Century Framework for Employee Monitoring*, 48 Am. Bus. L.J. 285, 301 (2011); Avner Levin, *Big and Little Brother: The Potential Erosion of Workplace Privacy in Canada*, 22 Can. J.L. & Soc. 197, 197–98 (2007). *See generally* Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. Pa. L. Rev. 477, 487–90

reasons to surveil employees' and applicants' online activities. Aside from monitoring for productivity, security, and performance, firms have a vested interest in learning about their present and future employees' moral constitution and personality traits that may affect on-the-job duties.[24] Failure to uncover an obvious flaw in an employee's background or character could lead to negligent hiring[25] and negligent retention[26] lawsuits or malpractice claims having serious business repercussions.[27] Employers must also control employee behavior on company computers, as legal liability may result from employee wrongdoing. In one case, an employer faced liability for failing to act against an employee who used a company computer to post nude photographs of his daughter.[28] Finally, employers must protect their reputational interests, intellectual property, and trade secrets. Given the ease and low cost of widespread information

---

(2006) (discussing the harm resulting from those in a position of power collecting private or personal data through the use of monitoring); Am. Mgmt. Ass'n, 2007 Electronic Monitoring & Surveillance Survey 4 (2008), http://www.plattgroupllc.com/jun08/2007ElectronicMonitoringSurveillanceSurvey.pdf (surveying employer monitoring practices in various areas such as the Internet, e-mail, and computer usage).

[24]*See* Terry Morehead Dworkin, *Protecting Private Employees from Enhanced Monitoring: Legislative Approaches*, 28 Am. Bus. L.J. 59, 75 (1990); Don Mayer, *Workplace Privacy and the Fourth Amendment: An End to Reasonable Expectations?*, 29 Am. Bus. L.J. 625, 626 (1991).

[25]Lex K. Larson, 1 Employment Screening § 10-2.3 (2006) (defining negligent hiring). Negligent hiring is a tort claim recognized in more than half of the states in the United States. Timothy L. Creed, *Negligent Hiring and Criminal Rehabilitation: Employing Ex-Convicts, Yet Avoiding Liability*, 20 St. Thomas L. Rev. 183, 184 (2008). In jurisdictions where the tort exists, an employer can be held liable for the harm its employee causes a third party if the employer knew or should have known of the employee's potential risk or if reasonable investigation would have uncovered such a risk. *Id*. at 184–85.

[26]Creed, *supra* note 25, at 187. Negligent retention theories of liability involve an employer's duty to exercise reasonable care in the continued retention of an employee. The tort was the basis of liability for employers of priests accused of pedophilia and football players accused of crimes. *See* Joel Michael Ugolini, *Even a Violent Game Has Its Limits: A Look at the NFL's Responsibility for the Behavior of Its Players*, 39 U. Tol. L. Rev. 41 (2007); Kelly H. Sheridan, Note, *Staying Neutral: How Washington State Courts Should Approach Negligent Supervision Claims Against Religious Organizations*, 85 Wash. L. Rev. 517 (2010).

[27]Employers can also be held liable for the torts of their employees under the legal doctrine of respondeat superior. *See, e.g.*, Micah Echols, *Striking a Balance Between Employer Business Interest and Employee Privacy: Using* Respondeat Superior *to Justify the Monitoring of Web-Based, Personal Electronic Mail Accounts of Employees in the Workplace,* 7 Computer L. Rev. & Tech. J. 273, 294 (2003).

[28]Doe v. XYC Corp., 887 A.2d 1156 (N.J. Super. Ct. 2005).

dissemination online, digital communication can be a powerful tool for disgruntled employees seeking to harm their employers by divulging intellectual assets or tarnishing their employers' names or products.[29]

This part identifies three pressing legal issues regarding social media within the employment context: (1) employer monitoring and surveillance of employee speech in social media profiles, (2) employer evaluation of the online speech of applicants in making hiring decisions, and (3) employer-imposed limitations on employees' off-duty social networking activities.

A. Monitoring and Surveillance of Employee Social Media Profiles

Most of the academic literature on the privacy of electronic communication in the workplace focuses on e-mail.[30] The explosive increase in participation on social media sites warrants an analysis of the applicability of the current law. The Fourth Amendment, privacy torts, and statutes such as the Electronic Communications Privacy Act of 1986 (ECPA) address workplace privacy in this context. Their applicability to the monitoring and surveillance of employee social media profiles and other online activities is discussed in turn below.

1. The Reasonable Expectations of Privacy Analysis

U.S. law emphasizes that the workplace and its resources are the property of the employer. The employer is generally free to dictate permissible use of company property as the employer sees fit. Workplace privacy is not an employee right, but a restriction placed upon the employer's property rights. This restriction may arise constitutionally, legislatively, or in tort

---

[29]The American Management Association found that, of the twenty-eight percent of surveyed employers who reported terminating an employee for e-mail misuse, twenty-two percent of those violations involved a breach of confidentiality. *See* Am. Mgmt. Ass'n, *supra* note 23, at 8–9.

[30]*See, e.g.*, Bradley J. Alge, *Effects of Computer Surveillance on Perceptions of Privacy and Procedural Justice*, 86 J. Applied Psychol. 61 (2001); Ciocchetti, *supra* note 15; Barry A. Friedman & Lisa J. Reed, *Workplace Privacy: Employee Relations and Legal Implications of Monitoring Employee E-mail Use*, 19 Emp. Resp. & Rts. J. 75 (2007); Joan T. A. Gabel & Nancy R. Mansfield, *The Information Revolution and Its Impact on the Employment Relationship: Analysis of the Cyberspace Workplace*, 40 Am. Bus. L.J. 301 (2003); Jennifer L. Paschal et al., *Effects of Electronic Mail Policies on Invasiveness and Fairness*, 24 J. Managerial Psychol. 502 (2009); Janice C. Sipior & Burke T. Ward, *The Ethical and Legal Quandary of Email Privacy*, 38 Comm. ACM, Dec. 1995, at 48.

law, but in its essence it must be "reasonable" and not unduly erode the employer's property rights.[31] Accordingly, the inquiry into whether the employee had a reasonable expectation of privacy in the intruded space is at the core of the law governing workplace privacy. Because the expectations lack an independent normative basis, the evaluation of the reasonableness of privacy expectations can be a chicken-and-egg analysis in which normative behavior informs the law and the law, in turn, influences normative behavior. Furthermore, from a legal perspective, reasonable expectations of privacy are formed in a two-step process.[32] First, the claimant must have a subjective expectation of privacy. Second, there must also be an objective expectation of privacy that society accepts and legitimizes. Most employee arguments for privacy are foiled in step one by such instruments as employer communications and policies, but remain grounded in a widespread, societal norm the legal analysis hardly ever reaches.

For example, courts have generally held that employees do not have a reasonable expectation of privacy in the workplace, especially if using hardware provided by the employer[33] or if the employer has communi-

---

[31]*See infra* notes 32–65 and accompanying discussion of reasonable expectations of privacy. Other jurisdictions, most notably the member states of the European Union, understand workplace privacy differently. In these jurisdictions, employees have a right to dignity and to a private life that does not stop at the boundary of the workplace. While this right is not absolute and must be balanced with the employer's property rights, it does contain an inalienable core that protects the dignity of the employee as a human being. *See generally* James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151 (2004) (discussing these different approaches to understanding privacy).

[32]Katz v. United States, 389 U.S. 347, 360–61 (1967); *see also* Mayer, *supra* note 24, at 630–32. In the context of private employers, the analysis is the same. *See, e.g.*, Smyth v. Pillsbury Co., 914 F. Supp. 97, 101 (E.D. Pa. 1996) (finding that there is no "reasonable expectation of privacy in e-mail communications voluntarily made by an employee to his supervisor over the company e-mail system"); Dir. of Office of Thrift Supervision v. Ernst & Young, 795 F. Supp. 7, 10 (D.D.C. 1992) (applying the *O'Connor* standard to the question of employee privacy in diaries containing personal and company data). In *O'Connor v. Ortega*, 480 U.S. 709, 726 (1987), the Supreme Court held that an employee's reasonable expectation of privacy in the workplace should be judged under all the circumstances and must be reasonable both in inception and scope.

[33]*See, e.g.*, Bohach v. City of Reno, 932 F. Supp. 1232 (D. Nev. 1996); *Smyth*, 914 F. Supp. 97; Bourke v. Nissan Motor Corp., No. B068705 (Cal. Ct. App. July 26, 1993) (unreported decision); McLaren v. Microsoft, No. 05-97-00824-CV, 1999 Tex. App. LEXIS 4103, at *12 (Tex. App. May 28, 1999); Jay P. Kesan, *Cyber-Working or Cyber-Shirking?: A First Principles Examination of Electronic Privacy in the Workplace*, 54 FLA. L. REV. 289, 303 (2002).

cated to employees that they may be monitored (by written policy or otherwise).[34] The Supreme Court has also recognized that employers have a legitimate interest in monitoring their employees, especially for reasonable work-related reasons.[35] As a result of this legal validation, employee monitoring and surveillance has become a common practice.[36]

Despite the fact that organizations generally have a legal right to access and monitor employees' e-mail and online activities and that employees generally accept monitoring practices, employees still cling to certain expectations of privacy in the workplace.[37] Studies show that employees generally believe that it is illegal and unethical for employers to intrude into certain areas of their lives.[38] The manner in which reasonable expectations of privacy are legally constructed, both for constitutional and private law purposes, and the observable expectations of employees are thus disconnected.[39] For this reason, the debate over expectations of privacy in the workplace endures and is apparent in privacy jurisprudence, specifically relating to the Fourth Amendment and the privacy torts.

---

[34]*See, e.g.*, Muick v. Glenayre Elec., 280 F.3d 741, 743 (7th Cir. 2002) (finding no reasonable expectation of privacy in workplace computer files when the employer expressly reserved the right to inspect the computer); Thygeson v. U.S. Bancorp, No. CV-03-467, 2004 WL 2066746, at *20 (D. Or. Sept. 15, 2004) (finding no reasonable expectation of privacy in computer files and e-mail when the employee handbook explicitly warned of the employer's right to monitor files and e-mail); Kelleher v. City of Reading, No. Civ. A. 01-3386, 2002 WL 1067442, at *8 (E.D. Pa. May 29, 2002) (finding no reasonable expectation of privacy in workplace e-mail when the employer's guidelines "explicitly informed employees that there was no such expectation of privacy").

[35]*O'Connor*, 480 U.S. at 712.

[36]The American Management Association has reported that sixty-six percent of the largest U.S. companies monitor Internet connections. *The Latest on Workplace Monitoring and Surveillance*, Am. Mgmt. Ass'n (Mar. 13, 2008), http://www.amanet.org/training/articles/The-Latest-on-Workplace-Monitoring-and-Surveillance.aspx.

[37]*See* Jason L. Snyder, *E-mail Privacy in the Workplace: A Boundary Regulation Perspective*, 47 J. Bus. Comm. 266, 268 (2010) (citing Gary Gumpert & Susan J. Drucker, *The Demise of Privacy in a Private World: From Front Porches to Chat Rooms*, 8 Comm. Theory 408 (1998)).

[38]*See, e.g.*, Stanton, *supra* note 22, at 130 (discussing studies addressing employees' reactions to workplace monitoring).

[39]For more on the historical connection between the constitutional test as it was first set out in *Katz v. United States*, 389 U.S. 347 (1967), and tort law, see Mayer, *supra* note 24, at 632–37; Peter Winn, Katz *and the Origins of the "Reasonable Expectation of Privacy" Test*, 40 McGeorge L. Rev. 1 (2009).

The Fourth Amendment—via the Fourteenth Amendment[40]—grants individuals in the United States, including federal and state government employees, the right to "be secure in their persons, houses, papers, and effects" and protects them against "unreasonable searches and seizures."[41] Although the Fourth Amendment does not govern private-sector employers, judicial interpretation of the reasonableness of privacy expectations in the constitutional context validates new kinds of privacy interests and serves as a guide to judges and employers in the private sector.[42] As such, Fourth Amendment analyses of privacy inform privacy tort law, an area equally dependent upon the reasonableness of the plaintiff's desire for privacy.

Assessments of privacy expectations have traditionally hinged upon territorial and context-driven factors. In *O'Connor v. Ortega*, the leading Fourth Amendment employee privacy case, the U.S. Supreme Court concluded that a state hospital did not violate an employee's Fourth Amendment right to privacy when it searched his office drawers and cabinets as part of an inquiry into sexual harassment allegations against him.[43] The analysis, the Court reasoned, must first take into account whether the employee had a reasonable expectation of privacy in the invaded space given the "operational realities of the workplace."[44] Courts evaluating privacy claims in light of *O'Connor* have held that employees maintain a reasonable expectation of privacy in breakrooms,[45] restrooms,[46] and other

---

[40]Mapp v. Ohio, 367 U.S. 643, 654 (1961).

[41]U.S. CONST. amend. IV; *see also* O'Connor v. Ortega, 480 U.S. 709, 737 (1987) (stating that "individuals do not lose Fourth Amendment rights merely because they work for the government").

[42]Kevin J. Conlon, *Privacy in the Workplace*, 72 CHI.-KENT L. REV. 285, 289–91 (1996); Mayer, *supra* note 24, at 629.

[43]480 U.S. at 713.

[44]*Id*. at 717.

[45]State v. Bonnell, 856 P.2d 1265, 1279 (Haw. 1993) (holding that the defendants had a reasonable expectation of privacy in their break room because access to the room was limited to employees).

[46]*Cf*. Cramer v. Consol. Freightways, Inc., 209 F.3d 1122, 1131 (9th Cir. 2000) (holding that an employment contract that arguably allowed video surveillance of the employee bathroom could not supersede the mandatory provisions in state privacy laws), *rev'd en banc*, 255 F.3d 683 (9th Cir. 2001) (reversed in part on other grounds concerning the collective bargaining agreement in place). On review, the en banc Ninth Circuit found that the invasion of privacy

spaces normatively branded as private.[47] The analysis must also consider whether the purpose and scope of the employer's search was reasonable.[48] Searches conducted for "noninvestigatory, work-related purposes" and "investigations of work-related misconduct" are permissible exceptions to an employee's right to privacy so long as they are reasonable in light of the surrounding circumstances.[49]

Since *O'Connor*, the analysis into expectations of privacy in the workplace has become considerably dislodged from its spatial roots. In *City of Ontario v. Quon*, the Supreme Court revisited *O'Connor* in the context-challenged world of digital technology.[50] The case asked whether a police officer had a reasonable expectation of privacy in the personal text messages sent and received on his employer-provided pager.[51] Officer Jeff Quon claimed his Fourth Amendment right to privacy had been violated when his employer, the City of Ontario Police Department (OPD), requested an administrative review of his text messages for purposes of determining whether to upgrade its messaging plan.[52] Upon review, the OPD discovered that the preponderance of text messages sent by Quon were of a personal nature.[53] The review also revealed that Quon had sent sexually explicit text messages to a fellow OPD employee with whom he

---

claims were independent of the terms of the collective bargaining agreement and not preempted by the Labor Management Relations Act, 255 F.3d at 694; that any provision in the collective bargaining agreement that purported to authorize the use of two-way mirrors was illegal under state statute, *id*. at 695; and that such provision would thus be illegal and void. *id*.

[47]*See* Leventhal v. Knapek, 266 F.3d 64, 74 (2d Cir. 2001) (finding an employee had a reasonable expectation of privacy in the contents of his computer where the employee occupied a private office with a door, had exclusive use of the computer in his office, and did not share his computer with other employees or the public, notwithstanding the employer's policy prohibiting use of work equipment for personal purposes).

[48]*O'Connor*, 480 U.S. at 722–25.

[49]*Id*. at 725–26.

[50]130 S. Ct. 2619, 2625 (2010).

[51]*Id*. at 2632–33.

[52]*Id*. at 2626.

[53]*Id*. For example, of the 456 text messages Quon sent or received in the month of August 2002, no more than fifty-seven were work related. On an average business day, Quon sent or received twenty-eight text messages, only about three of which were work related. *Id*.

was romantically involved, and his then-wife.[54] Consequently, the OPD disciplined Quon for abuse of its policies.[55]

The Supreme Court held that the OPD did not violate Quon's Fourth Amendment right to privacy because the employer had a legitimate work-related purpose for conducting the search. The Court declined to decide whether Quon had a reasonable expectation of privacy in his text messages because it determined that the search was reasonable both in scope and purpose.[56] In reference to scope, the Court gave great weight to the fact that the OPD limited its search of Quon's text messages to those sent and received while he was on duty.[57] As to purpose, the Court found that the OPD's stated purpose for the search—to determine whether the current text-messaging service plan needed to be upgraded—was a "legitimate work-related rationale."[58]

A clear analogy can be drawn from text messaging on an employer-provided pager or telephone to the practice of communicating through social media sites on company computers. Both practices make use of employer hardware and systems for the social and personal purposes of the employee. In *Quon*, the Supreme Court displayed a surprising ambivalence regarding privacy on boundary-crossing technologies. On the one hand, the Court noted that the pervasiveness of the technology was suggestive of its essential role "for self-expression, even self-identification," which it reasoned "might strengthen the case for an expectation of privacy."[59] On the other hand, the technology's ubiquity suggested that it "is generally affordable, so . . . employees who need cell phones or similar devices for personal matters can purchase and pay for their own."[60] Ultimately, the Court refused to elaborate on privacy expectations on an

---

[54]*Id*. at 2626.

[55]*Id*. at 2626–27. The officers were instructed that messages sent and received from their issued devices would be treated as e-mails under the City's Computer Policy, which stated that the City "reserve[d] the right to monitor and log all network activity . . . with or without notice." *Id*. at 2625.

[56]*Id*. at 2630.

[57]*Id*. at 2631–32.

[58]*Id*. at 2632–33.

[59]*Id*. at 2630.

[60]*Id*.

"emerging technology before its role in society has become clear,"[61] claiming that "[p]rudence counsels caution before the facts in the instant case are used to establish far-reaching premises that define the existence, and extent, of privacy expectations enjoyed by employees when using employer-provided communication devices."[62]

Although the Supreme Court sidestepped analyzing the reasonableness of Quon's privacy expectations, it opined in dicta that the employee's expectation of privacy should have been limited. A reasonable employee, according to the Court, "would be aware that sound management principles might require the audit of messages to determine whether the pager was being appropriately used."[63] The Court also noted that "employer policies concerning communications will of course shape the reasonable expectations of their employees, especially to the extent that such policies are clearly communicated."[64] This holding is consistent with previous lower court rulings.[65]

While shedding some light on employees' reasonable privacy expectations, current Fourth Amendment jurisprudence fails to define the reasonableness of those expectations as to modern technology and social media. Some foreign courts have displayed a more direct approach. For example, France's Supreme Court has long been famous for its protective stance toward employee privacy. In *Société Nikon France, S.A. v. M. Onof*, it

---

[61]*Id*. at 2629.

[62]*Id*.

[63]*Id*. at 2631.

[64]*Id*. at 2630.

[65]Courts customarily look at all of the circumstances surrounding the alleged consent to company monitoring policies in assessing whether the employee has a reasonable expectation of privacy. *See* Hernandez v. Hillsides, Inc., 211 P.3d 1063, 1078 (Cal. 2009) (holding that the plaintiffs had a reasonable expectation of not being videotaped in their offices, despite company policy indicating the employees had no reasonable expectation of privacy in their communications, because such policy never alluded to the possibility of video recording); Bourke v. Nissan Motor Corp., No. YC-003979 (Cal. Ct. App. July 26, 1993) (unreported decision), *available at* http://www.loundy.com/CASES/Bourke_v_Nissan.html (last visited Oct. 9, 2011) (holding that employees forfeit reasonable expectations of privacy on work computers by agreeing to the employer's policies providing that use of its computers was for business purposes only); Smyth v. Pillsbury Co., 914 F. Supp. 97, 101 (E.D. Pa. 1996) (holding that, despite an employer's failure to notify its employee that his communications were being monitored, the employer's "interest in preventing inappropriate and unprofessional comments or even illegal activity over its e-mail system outweigh[ed] any privacy interest the employee may have [had]").

held that employees have a robust right to privacy in their communications on work computers.[66] In that case, an employer was prohibited from terminating an employee based on evidence obtained from e-mails written by the employee on a work computer while at work.[67] Recently, in another case, *La Société Seit Hydr'Eau v. M. J-M*, the labor chamber of France's highest court found that employees had an expectation of privacy in electronic folders that had been marked "personal" on work computers.[68] It construed the expectation narrowly to conclude that an electronic folder marked with the employee's initials was not private.[69]

In Canada, courts have been walking a middle ground between the United States and the European Union (EU).[70] In *R. v. Cole*, a high school teacher was accused of storing nude images of a sixteen-year-old student on the laptop that the school board provided to him. He argued that he had a reasonable expectation of privacy in the laptop.[71] Cole was criminally prosecuted after a board technician discovered the offending images and other pornographic images on the laptop during a routine service of the school's information network.[72] Cole argued that the board and the police searched the laptop in violation of his rights under Section 8 of the Canadian Charter of Rights and Freedoms.[73] The Canadian court concluded the teacher had a subjective expectation of privacy in the laptop,

---

[66]Cour de Cassation [Cass.] [supreme court for judicial matters] soc., Oct. 2, 2001, No. 4164 (Fr.), *available at* http://www.courdecassation.fr/jurisprudena_2/chamber_sociale_576/arret_no_1159.html.

[67]*Id*.

[68]Cour de Cassation [Cass.] [supreme court for judicial matters] soc., Oct. 21, 2009, No. 2044 (Fr.), *available at* http://www.courdecassation.fr/publications_cour_26/arrets_publies_2986/chambre_sociale_3168/2009_3332/octobre_2009_3246/2044_21_13949.html.

[69]*Id*.

[70]*See* Avner Levin & Mary Jo Nicholson, *Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground*, 2 U. Ottawa L. & Tech. J. 357 (2005) (describing Canada's middle-ground position on privacy matters).

[71][2011] 105 O.R. 3d 253 (Can. Ont. C.A.), *available at* http://www.ontariocourts.on.ca/decisions/2011/2011ONCA0218.htm.

[72]*Id*. at para. 12.

[73]*Id*. at para. 3. Section 8 is roughly equivalent to the Fourth Amendment, stating, "Everyone has the right to be secure against unreasonable search or seizure." Canadian Charter of Rights and Freedoms, Part I of the Constitution Act § 8, 1982, *available at* http://laws.justice.gc.ca/eng/charter/page-1.html.

and absent a clear privacy policy or acceptable use policy or both, this expectation was reasonable. In particular, the court stated that

> based upon the totality of the circumstances in this case . . . the appellant had a reasonable expectation of privacy in the personal use of his work laptop. . . . The teachers used their computers for personal use, they employed passwords to exclude others from their laptops, and they stored personal information on their hard drives. There was no clear and unambiguous policy to monitor, search or police the teachers' use of their laptops.[74]

The Canadian court, however, found that Cole "knew that a school technician had a limited right of access to the hard drive as part of his duties to maintain the stability and security of the network system,"[75] and so concluded that Cole's reasonable expectation of privacy did not apply to the actions of the technician.[76] Accordingly, once the technician had stumbled upon the images, the technician's and school board's actions did not violate the Canadian Charter.[77]

Cole is notable for linking expectation of privacy to organizational norms and highlighting the important role that policies play in setting privacy expectations. Other Canadian cases have held that policies in collective bargaining agreements may also inform expectations of privacy in personal data.[78]

These cases indicate the Canadian and American courts' reluctance to recognize a strong workplace privacy right and their willingness to defer to employer policies and agreements as setting reasonable workplace and e-mail privacy expectations. At the same time, it is clear from these holdings that workplace policies are not entirely responsible for setting expectations of privacy. The French court's *Seit Hydr'Eau* decision demonstrates that it is possible to protect employer interests notwithstanding strong workplace privacy rights.[79] The Canadian and American courts'

---

[74]*Cole*, 105 O.R. 3d 253, para. 45.

[75]*Id*. at para. 47.

[76]*Id*. at para. 48.

[77]*Id*. at paras. 63, 66.

[78]*See, e.g*., France v. Tfaily, [2009] 98 O.R. 3d 161 (Can. Ont. C.A.) (finding that a collective bargaining agreement between a university and a faculty association granted a professor an objectively reasonable expectation of privacy in relation to his personal electronic data on university computers).

[79]*See supra* notes 68–69 and accompanying text.

unwillingness to render broader holdings has left employees and employers without a clear answer about which surveillance and monitoring practices violate an employee's reasonable expectation of privacy.[80]

2. The ECPA

The ECPA protects the private transmission and storage of electronic data.[81] Title I of the ECPA, known as the Wiretap Act, prohibits the interception, use, or disclosure of any electronic communication while in transit.[82] The significant exceptions to the Wiretap Act limit its applicability to employer monitoring and surveillance of employee social networking activities. First, the Wiretap Act does not apply to communications made through an electronic communication system that is readily accessible to the general public.[83] It appears, then, that if an employee makes her digital information accessible to the general public, her employer is not prohibited from monitoring, viewing, or intercepting such communication. This is true whether or not she was at work when the communication was made. Second, the Wiretap Act provides an exception for providers of the communication service who intercept, use, or disclose the communication in the ordinary course of business and when engaged in an activity incidental to the provision of such communication service.[84] As such, organizations providing mobile telecommunications service or Internet access to their employees for work-related purposes may access all employee communication transmitted thereby. Third, the Wiretap Act permits interception of a communication when one of the parties to the communication expressly or impliedly consents to it.[85] Individuals often expressly consent by accepting a written electronic communications policy or contract clause and

---

[80]It also has been argued that, with every U.S. Supreme Court case defining the reasonableness of an individual's expectation of privacy under the Fourth Amendment, the Court has become more vague and continued to narrow its holding in *Katz v. United States*, 389 U.S. 347 (1967). *See* Mayer, *supra* note 24, at 656–58.

[81]Pub. L. No. 99–508, Title I, 100 Stat. 1851, 1859 (codified at 18 U.S.C. §§ 2510–22 (2006)); Title II, 100 Stat. 1860 (codified at 18 U.S.C. §§ 2701–11 (2006)); Title III, 100 Stat. 1868 (codified at 18 U.S.C. §§ 3121–27 (2006)).

[82]18 U.S.C. § 2511(1).

[83]*Id*. § 2511(2)(g)(i).

[84]*Id*. § 2511(2)(a)(i).

[85]*Id*. § 2511(2)(c) & (d).

acknowledgment of monitoring by way of a login prompt or corporate policy are common ways of obtaining express consent. Courts infer consent from the conduct of workers who continue employment after having been notified that their communications are subject to surveillance and monitoring.[86] Finally, employees seem to have a claim under the Wiretap Act only if their communications are intercepted while in transit, rather than in storage.[87]

Title II of the ECPA, known as the Stored Communications Act (SCA), may offer more redress for the employee whose personal online information is accessed by an employer in an unsanctioned manner. The SCA forbids the intentional and unauthorized access of stored communications.[88] The SCA provides broader exceptions than the Wiretap Act because it excludes from liability those who have been authorized access by the entity providing the electronic communication service, a user of that service who is the intended recipient of the communication, or the author of the communication.[89]

Recently, courts have interpreted the meaning of "authorized access" to social media profiles in light of the employment relationship. In *Pietrylo v. Hillstone Restaurant Group*, two restaurant employees were terminated after their manager discovered their password-protected MySpace group, which contained personal information, also referenced illegal drug use, violence, and sexual remarks about the restaurant's management and customers.[90] Employee Brian Pietrylo had created the private online

---

[86]*See* Matthew Finkin, *Information Technology and Workplace Privacy: The United States Law*, 23 Comp. Lab. L. & Pol'y J. 471 (2002) (discussing the ECPA and U.S. workplace privacy in general); Sylvia Kierkegaard, *Privacy in Electronic Communication Watch Your E-mail: Your Boss Is Snooping*, 21 Computer L. & Sec. Rep. 226 (2005).

[87]*See* Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 114 (3d Cir. 2003) (holding that an employer accessing an employee's e-mail did not violate the Wiretap Act because the communication was in storage rather than in transit); Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 878 (9th Cir. 2002) (holding that an employer that accessed its employee's personal, password-protected Web site did not violate the Wiretap Act because the electronic communication was accessed when in storage, rather than when in transmission).

[88]18 U.S.C. § 2701(a).

[89]*Id*. § 2701(c).

[90]No. 06-5754-FSH, 2008 WL 6085437, at *1-2 (D.N.J. July 25, 2008); *see also* Dionne Searcey, *Employers Watching Workers Online Spurs Privacy Debate*, Wall St. J., Apr. 23, 2009, at A13.

forum to vent about work-related topics.[91] One of the online group members, a hostess at the restaurant, showed the site to a restaurant manager.[92] Another restaurant manager later requested the hostess divulge her MySpace login information and password to management so it could access Pietrylo's private group and review the postings.[93] The hostess testified that she gave the password to the manager for fear of retaliation.[94] Based on the content of the online postings, management terminated Pietrylo and another employee.[95] The employees filed suit, claiming the employer violated the SCA, wrongfully terminated them in violation of a clear mandate of public policy, and invaded their privacy.[96] The jury found that, because the employee who provided access to the private online forum did not act voluntarily, employer Hillstone had "knowingly or intentionally or purposefully accessed the [private MySpace group] . . . without authorization,"[97] in violation of the SCA, and awarded the plaintiff employees compensatory and punitive damages.[98] Regarding the privacy claim, the jury found that, even though Pietrylo created the private MySpace group as "a place of solitude and seclusion which was designed to protect the Plaintiff's private affairs and concerns,"[99] he did not have a reasonable expectation of privacy in the postings made on the group.[100]

---

[91]*Pietrylo*, 2008 WL 6085437, at *1.

[92]*Id*.

[93]*Id*.

[94]*Id*. at *4.

[95]*Id*. at *2.

[96]*Id*.

[97]Pietrylo v. Hillstone Rest. Grp., No. 06-5754 (FSH), 2009 WL 3128420, at *1 (D.N.J. Sept. 25, 2009).

[98]*Id*.

[99]Verdict and Settlement Agreement, Pietrylo v. Hillstone Rest. Grp., No. 2:06-cv-05754-FSH-PS (D.N.J. June 26, 2009) 2009 WL 2342553.

[100]*Id*. *Pietrylo* is consistent with the manner in which expectations of privacy on social networks have been analyzed in Canada. For example, in a recent labor arbitration decision on the dismissal of a unionized employee of a car dealer, the arbitrator found that the employee had no reasonable expectation of privacy in his Facebook postings because he had one hundred Facebook friends. Lougheed Imports, Ltd. v. United Food & Commercial Workers Int'l Union, Local 1518, [2010] CanLII 62482, para. 97 (Can. B.C.L.R.B.), *available at* http://www.canlii.org/en/bc/bclrb/doc/2010/2010canlii62482/2010canlii62482.html. Similar to *Pietrylo*, the

Pietrylo stands for the proposition that an employer cannot lawfully obtain access to stored information on an employee's social media profile by coercion. It remains clear that employers are free to access such information and to act upon it,[101] if granted access to the online forum voluntarily or if the online information is readily accessible to the public at large.

The court's application of the SCA in *Pietrylo* is consistent with previous cases in which employers surreptitiously accessed the personal e-mail accounts of their employees. In *Pure Power Boot Camp v. Warrior Fitness Boot Camp*, a New York district court found that an employer's unauthorized access to a former employee's personal Internet-based e-mail accounts was a violation of the SCA, despite the existence of a company policy, which stated that "e-mail users have no right of personal privacy in any matter stored in, created on, received from, or sent through or over the system."[102] Former employee Alexander Fell admitted he accessed his personal Gmail and Hotmail accounts on his work computer, but denied drafting or receiving e-mails at work.[103] Fell's employer reportedly obtained access to Fell's personal Internet e-mail accounts because some of the usernames and passwords to those accounts were stored on the company computer. The employer gained access to another one of Fell's personal Internet e-mail accounts by correctly guessing that the password was the same as the one used in his other two e-mail accounts.[104] While the court predictably found that the Wiretap Act did not apply because communications were not in transit,[105] it determined that the employer violated the SCA because the employee's personal Internet e-mails, administered through Google and Microsoft, were not stored on the company system, per the company policy's narrow scope.[106]

---

employer did not have direct access to the employee's Facebook page, but was granted access by an ex-employee. *Id*. at para. 22.

[101]*See infra* notes 152–62 and accompanying text (discussing whether employees' off-duty online speech is concerted activity under Section 7 of the National Labor Relations Act).

[102]587 F. Supp. 2d 548, 552 (S.D.N.Y. 2008).

[103]*Id*. at 553.

[104]*Id*. at 556.

[105]*Id*. at 557–58.

[106]*Id*. at 559.

The employer had also argued that the one-sentence company e-mail policy, advising employees that they had no right of personal privacy,[107] eviscerated any reasonable expectation of privacy that Fell might claim in his personal e-mail accounts and that leaving a username and password accessibly recorded on an employer-provided computer constituted implied consent to employer access to personal e-mail accounts.[108] The court concluded that this argument had "no support in the law" and proceeded to determine that the employee did indeed have a reasonable expectation of privacy in the passwords and usernames stored on company computers.[109] It analogized the situation to an employee leaving his house key on his work desk, reasoning that under no circumstance would the law interpret a mislaid house key as "consent to whoever found the key, to use it to enter his house and rummage through his belongings."[110] The court refused to accept that "carelessness equals consent" in the realm of privacy.[111] The court further found that spotty enforcement of the company e-mail policy reinforced the employee's reasonable expectation of privacy in his personal e-mail accounts while at work.[112]

With only a minor stretch of the imagination, *Pure Power Boot Camp* suggests that employees who access their Facebook profiles on the job and store their online social network (OSN) usernames and passwords on workplace computers may be protected by the SCA from unauthorized employer intrusion into their Internet profiles and accounts. The decision is also a warning for employers. Employee Internet and social media use policies must be explicit about what information is accessible to the employer and where it is located. The existence of an explicit policy is not always dispositive to a finding of a reasonable expectation of employee privacy.

While the SCA was not drafted with the intention of securing employee e-mail and Internet privacy, it seems to be in the process of

---

[107]*Id*. at 553.

[108]*Id*. at 559.

[109]*Id*.

[110]*Id*. at 561.

[111]*Id*.

[112]*Id*. The policy was not enforced in a consistent manner "that would have alerted employees to the possibility that their private email accounts, such as Hotmail, could also be accessed and viewed by their employer." *Id*.

experiencing a resurgence for that purpose. This is consistent with developing approaches to employee Internet privacy internationally. As mentioned above, the French Supreme Court has held that employers cannot access employee communications that are clearly marked as "personal" without employee permission.[113]

In Israel, a recent National Labor Court decision similarly restricted employer access to employee e-mail and offered an innovative analysis based on the character of the e-mail account, not its owner, label, or location.[114] The scenario was a familiar one—the employer wished to use an employee's e-mails as evidence to support a termination decision, and the employee argued that the e-mails were private.[115] After reminding employers of the need to have clearly communicated policies as a precondition for any employer action, the Israeli Labor Court drew a distinction between private Internet-based e-mail accounts, which employees may access at work, and certain types of employer-provided e-mail accounts.[116] The court prohibited employers from accessing private Internet-based e-mail accounts without a court order, even if such accounts were accessed by the employee at work using employer-provided infrastructure.[117] It then distinguished among three types of workplace or employer-provided e-mail accounts: (1) those used exclusively for work-related purposes, (2) those used exclusively for personal purposes, and (3) those used by the employee for both work-related and personal purposes.[118] According to the court, employers may regularly monitor "exclusively-work-related" accounts, but may not access the content of personal e-mails sent from such accounts unless the employee freely consents.[119] This rule applies even if

---

[113]*See supra* notes 68–69 and accompanying text.

[114]File No. 90/08 National Labor Court, Tali Isakov Inbar v. Commissioner for Women Labor (Feb. 8, 2011), *available at* http://elyon1.court.gov.il/heb/dover/3082302.doc [in Hebrew]. For a case note in English, see Dan Or-Hof, *Israel—Monitoring Employees Email Severely Restricted*, Pearl Cohen Zedek Latzer (Feb. 10, 2011), http://www.pczlaw.com/news/2011/02/10/israel—monitoring-employees-email-severely-restricted.

[115]*Tali Isakov Inbar*, at para. 3.

[116]*Id*. at para. 2.

[117]The Israeli court explicitly stated that employee consent would be insufficient. *Id*. at para. 49.

[118]*Id*. at para. 2.

[119]*Id*. at para. 39.

the employee sends personal e-mails on work accounts in violation of corporate policies. Personal workplace accounts and dual-purpose workplace accounts are subject to further restrictions: employers must have an independent valid business reason for monitoring or accessing them, they must first resort to less-invasive methods, and they must obtain the employee's freely given consent.[120] While the Israeli decision offers employees strong protection, it is a default position. Employers are not obligated to offer employees personal e-mail accounts, and employers and employees may enter into collective agreements to regulate workplace privacy and the use of technology at work, which would supplant the Israeli Labor Court's default position.[121]

B. Employer Evaluation of Online Speech and Virtual Identity of Applicants

Organizations are increasingly monitoring social media for information that may provide insight on prospective hires.[122] One study recently found that forty-five percent of surveyed employers researched job candidates using online social networking sites.[123] More than a third of employers in that survey also reported having found publicly available content on applicants' social media profiles that caused them not to hire the applicants.[124] Objectionable content included inappropriate photographs or information, evidence of alcohol or drug use, and information revealing that the

---

[120]*Id*. at para. 41.

[121]*Id*. at para. 5. Employment in Israel is governed by collective agreements to a greater extent than in the United States because legislation enables the Ministry of Labor to apply such agreements to nonunionized workplaces as well. *See* Collective Agreements Law, 5717–1957 §§ 25-33G (Isr.), *available at* http://www.tamas.gov.il/NR/rdonlyres/DF31497A-297C-431A-8C63-7DB7CD653C1F/0/3.pdf.

[122]*See* Diane Coutu, *We Googled You*, Harv. Bus. Rev., June 2007, at 37, 44 (providing comments by chairman and chief executive officer of Manpower, an employment company, about the pervasiveness of the employee online screening practice); Brian Elzweig & Donna K. Peoples, *Using Social Networking Web Sites in Hiring and Retention Decisions*, SAM Advanced Mgmt. J., Autumn 2009, at 27, 28.

[123]*Career Experts Provide Advice on Dos and Don'ts for Job Seekers on Social Networking*, CareerBuilders.com (Aug. 19, 2009), http://www.careerbuilder.com/share/aboutus/pressreleasesdetail.aspx?id=pr519&sd=8/19/2009&ed=12/31/2009&siteid=cbpr&sc_cmp1=cb_pr519_&cbRecursionCnt=2&cbsid=c6bd4651f8e845f187ba45c9c3152747-316799338-RK-4.

[124]*Id*.

applicant had lied on the job application.[125] More information about candidates is desirable when that information is bona fide. The danger of "social media background checks" is that personal information presented out of context or inaccurately may lead employers to judge candidates unfairly without their knowledge or without providing an opportunity for rebuttal. Worse yet, the surreptitious quality of the information search may be a backdoor to illegal discrimination. This unregulated yet widespread practice has received some scholarly attention.[126]

There are two main legal issues surrounding social media background checks: the propriety of employer access to the candidate's online information and the permissibility of basing hiring decisions on the discovered digital information. Of course, employers are permitted to research candidates' lives and reputations as documented in their publicly available, non-password-protected social media profiles. However, accessing a candidate's password-protected social media profile in an unauthorized manner (such as surreptitiously or by coercion) violates the SCA.[127] These practices could also violate the social network site's terms of service.[128] Both Facebook's and MySpace's terms of service prohibit using their networks for commercial purposes or gains without users' consent.[129] A company's use of a social network to research its prospective hires may be characterized as a commercial use of the network.[130] Social media sites also generally prohibit accessing a member's account for the purpose of

---

[125]*Id*. (revealing that fifty-three percent of the employers that reported having found content that caused them not to hire candidates said they found candidates had posted inappropriate photographs or information, forty-four percent found evidence of candidates drinking or using drugs, and twenty-four percent discovered that applicants had lied about their qualifications).

[126]*See, e.g*., Alexander Wohl, *After Forty Years of Tinkering With Teachers' First Amendment Rights, Time for a New Beginning*, 58 Am. U.L. Rev. 1285, 1316–17 (2009); Carly Brandenburg, Note, *The Newest Way to Screen Job Applicants: A Social Networker's Nightmare*, 60 Fed. Comm. L.J. 597 (2008); Ian Byrnside, Note, *Six Clicks of Separation: The Legal Ramifications of Employers Using Social Networking Sites to Research Applicants*, 10 Vand. J. Ent. & Tech. L. 445 (2008).

[127]*See supra* notes 90–101 and accompanying text.

[128]Brandenburg, *supra* note 126, at 612–13.

[129]*MySpace.com Terms of Use Agreement*, MySpace.com, http://www.myspace.com/index.cfm?fuseaction=misc.terms (last visited Aug. 14, 2011); *Statement of Rights and Responsibilities*, Facebook.com, http://www.facebook.com/terms.php?ref=pf (last visited Aug. 14, 2011).

[130]Brandenburg, *supra* note 126, at 613.

obtaining information regarding another member or circumventing privacy settings.[131] However, no regulation forces employers to disclose their information-gathering practices on social networking sites.[132] In analogous contexts, the law suggests that regulating background checks of social media by prospective employers may be warranted. For example, the Fair Credit Reporting Act allows prospective employers to obtain a candidate's consumer report from consumer reporting agencies provided they inform the candidate in writing of the request and obtain the candidate's written authorization.[133]

Employers are currently free to judge candidates on the basis of all available information, unless prohibited or restricted by law. A candidate's recklessness, bad reputation, and unsound moral character are obviously justifiable reasons for denial of employment. Employers may not, however, discriminate on other bases. Title VII of the Civil Rights Act of 1964 (Title VII) covers most private employers with fifteen or more employees and prohibits discrimination in the workplace "with respect to . . . compensation, terms, conditions, or privileges of employment, because of [an] individual's race, color, religion, sex, or national origin."[134] Various state statutes have broadened the scope of hiring and employment discrimination. New York, for example, bars employers from basing employment decisions on a candidate's legal recreational activities, political activities, union membership, and consumption of legal products provided that the candidate's behavior does not conflict with the employer's genuine business interest.[135] By covertly obtaining personal candidate information to

---

[131]*MySpace.com Terms of Use Agreement*, MySpace.com, *supra* note 129; *Statement of Rights and Responsibilities*, Facebook.com, *supra* note 129.

[132]*See generally* Donald Carrington Davis, *MySpace Isn't Your Space: Expanding the Fair Credit Reporting Act to Ensure Accountability and Fairness in Employer Searches of Online Social Networking Services*, 16 Kan. J.L. & Pub. Pol'y 237 (2007) (discussing the general lack of regulation requiring employers to disclose the source or process by which they obtained information on job candidates, which in turn makes them more likely to engage in surreptitious practices).

[133]15 U.S.C. §§ 1681a–b (2010).

[134]42 U.S.C. § 2000e-2(a)(1) (2006). While restrictive of some speech, Title VII has been considered compatible with the First Amendment as it protects the individual's autonomy of consciousness promoted through the First Amendment. *See* O. Lee Reed, *A Free Speech Metavalue for the Next Millennium: Autonomy of Consciousness in First Amendment Theory and Practice*, 35 Am. Bus. L.J. 1, 36–38 (1997).

[135]N.Y. Lab. Law § 201-d (Consol. 2011).

which they would not otherwise be privy, employers may be more likely to discriminate illegally and less likely to get caught.

C. Employer-Imposed Limitations on Employee Private Life

Conventional wisdom dictates that an employee is a representative of his or her organization in all areas of life.[136] This is especially true when an employee uses a company logo, wears a company uniform, or purports to speak for or about the company as an insider. In extreme cases, employers have dismissed employees whose extracurricular activities could have a negative impact on their organizations' reputations.[137] Some companies have contended that employees' aberrant, off-duty behavior can even affect the bottom line.[138] For these reasons, private employers have often sought to control the risks of off-duty employee conduct by way of specific contractual clauses such as morality clauses, confidentiality agreements, and off-duty codes of conduct.[139]

---

[136]Patricia Sánchez Abril & Ann M. Olazábal, *The Celebrity CEO: Corporate Disclosure at the Intersection of Privacy and Securities Law*, 46 Hous. L. Rev. 1545, 1575–76 (2010). As some have noted, "as employees move up the organizational hierarchy, so does the expectation of conformity with organizational expectations in one's private life." Rafael Gely & Leonard Bierman, *Workplace Blogs and Workers' Privacy*, 66 La. L. Rev. 1079, 1107 (2006).

[137]*See* Levin et al., *supra* note 14, at 68; Terry Morehead Dworkin, *It's My Life—Leave Me Alone: Off-the-Job Employee Associational Privacy Rights*, 35 Am. Bus. L.J. 47, 47–49 (1997) (providing examples of companies in the past that made employment decisions based on the employee's personal life, if they found aspects of the employee's personal life to conflict with the image the company wanted to portray to the public).

[138]In one case, a low-level supermarket employee was terminated when his supervisors learned he enjoyed dressing like a woman in private. Oiler v. Winn-Dixie La., Inc., No. 00-3114, 2002 U.S. Dist. LEXIS 17417, at *4–9 (E.D. La. Sept. 16, 2002). Company representatives maintained, in their defense, that the employee's aberrant behavior would certainly drive away customers in their small town. *Id*. at *9–10.

[139]*See* Brian Van Wyk, Note, *We're Friends, Right? Client List Misappropriation and Online Social Networking in the Workplace*, 11 Vand. J. Ent. & Tech. L. 743, 754–55 (2009) (discussing the employment of a confidentiality and noncompetition agreement to prevent client misappropriation). *See generally* Terry Morehead Dworkin & Elletta Sangrey Callahan, *Buying Silence*, 36 Am. Bus. L.J. 151 (1998) (discussing the use of employee secrecy agreements in various contexts); Marka B. Fleming et al., *Morals Clauses for Educators in Secondary and Post-Secondary Schools: Legal Applications and Constitutional Concerns*, 2009 BYU Educ. & L.J. 67 (2009) (discussing the inclusion of morals clauses in teachers' employment agreements); Fernando M. Pinguelo & Timothy D. Cedrone, *Morals? Who Cares About Morals? An Examination of Morals Clauses in Talent Contracts and What Talent Needs to Know*, 19 Seton Hall J. Sports & Ent. L. 347

The growing use of interactive social media significantly complicates this already elusive line between the private individual and the company representative. A more public digital existence can threaten the privacy of both employees and their employers. An amalgamation of all of the elements and characters in a person's life, social media profiles allow for unprecedented transparency of an employee's private dealings, which can then be associated with his organization with minimal inference. A disgruntled employee can easily divulge trade secrets, intellectual property, or confidential information—or can harm the organization's reputation with disparaging commentary. Even a well-intentioned but reckless employee can tarnish an organization by disseminating potential evidence of the organization's negligence, immorality, or incompetence.

Some organizations have restricted their employees' off-duty use of social networking sites or have prohibited using them altogether. For example, the National Football League has prohibited players' access to social media immediately before, during, and after football games.[140] College athletic programs also restrict their student athletes' online participation to avoid damaging the reputations of their host universities.[141] Employer restrictions on off-duty speech and conduct are troubling in that they squelch expression and individual autonomy and may compromise the employee's right to a private life, especially when restrictions are unilaterally imposed after employment commences.

The First Amendment offers limited protection against speech restrictions in the employment context.[142] It does not shield private

---

(2009) (discussing the more traditional use of morals clauses in contractual agreements involving talent, including endorsement contracts).

[140]Mark Maske, *League Issues New Twitter Policy*, Wash. Post: The League (Aug. 31, 2009, 4:53 PM), http://views.washingtonpost.com/theleague/nflnewsfeed/2009/08/league-issues-new-twitter-policy.html.

[141]Autumn K. Leslie, Note, *Online Social Networks and Restrictions on College Athletes: Student Censorship?* 5 DePaul J. Sports L. & Contemp. Probs. 19, 20 (2008) (explaining that closer monitoring and restrictions upon student athletes has traditionally been accepted because the acts of those athletes could implicate or tarnish the moral character of the school).

[142]*See generally* Reed, *supra* note 134 (arguing for an interpretation of free speech values in the new millennium more compatible with the human individual's autonomy of consciousness).

employees,[143] and rights afforded to public employees are limited to speech regarding matters of public concern,[144] which are balanced against their employers' business interests.[145] The U.S. Supreme Court has held that, if the employee's speech "cannot be fairly considered as relating to any matter of political, social, or other concern to the community, government officials should enjoy wide latitude in managing their offices, without intrusive oversight by the judiciary in the name of the First Amendment."[146] As such, internal office matters generally are not issues of public concern[147] and, by logical extension, neither are pictures of drunken employees or sexual remarks about coworkers. Employers in the public sector, like the private sector, are not required to "tolerate action which [they] reasonably believ[e] would disrupt the office, undermine [their] authority, and destroy close working relationships."[148] The Supreme Court also has found that an employer may lawfully base an adverse employment action on an employee's off-duty, off-premises speech.[149] In *City of San Diego v. Roe*, a police officer filed a First Amendment claim after he was fired for selling on eBay videos of himself stripping off his police uniform and masturbating.[150] The Supreme Court held that the officer's speech was not protected under the First Amendment, because it was sufficiently

---

[143]Dixon v. Coburg Dairy, Inc., 369 F.3d 811, 817 n.5 (4th Cir. 2004); Pietrylo v. Hillstone Rest. Grp., No. 06-5754-FSH, 2008 WL 6085437, at *5–6 (D.N.J. July 24, 2008); Laura B. Pincus & Clayton Trotter, *The Disparity Between Public and Private Sector Employee Privacy Protections: A Call for Legitimate Privacy Rights for Private Sector Workers*, 33 Am. Bus. L.J. 51, 53–54 (1995) (discussing the difference in First Amendment and other privacy rights between private and public sector employee); David C. Yamada, *Voices from the Cubicle: Protecting and Encouraging Private Employee Speech in the Post-Industrial Workspace*, 19 Berkeley J. Emp. & Lab. L. 1, 4–5 (1998).

[144]Connick v. Myers, 461 U.S. 138, 147 (1983).

[145]*See* Garcetti v. Ceballos, 547 U.S. 410, 418 (2006); City of San Diego v. Roe, 543 U.S. 77, 82–83 (2004); *Connick*, 461 U.S. at 142; Pickering v. Bd. of Educ., 391 U.S. 563, 568–70 (1968) (holding that a public school teacher could not be dismissed from his job for writing a letter to the newspaper criticizing the school board's treatment of revenue measures for the school because the teacher's First Amendment rights outweighed the school's business interests).

[146]*Connick*, 461 U.S. at 146.

[147]*Id*. at 143.

[148]*Id*. at 154.

[149]*City of San Diego*, 543 U.S. 77.

[150]*Id*. at 78–79.

"linked to his official status as a police officer" and "detrimental to the mission and functions of [his] employer."[151]

The National Labor Relations Board (NLRB) has attempted to bring employers' restrictions of employees' off-duty speech and conduct under the purview of the National Labor Relations Act (NLRA).[152] The NLRA guarantees both union and nonunion employees the right to self-organization and to "engage in other concerted activities for the purpose of collective bargaining or mutual aid or protection."[153] In late 2010, the NLRB issued a complaint against an ambulance service, claiming it unlawfully terminated an employee for violating its Internet posting policy, which forbade employees from making disparaging or defamatory comments about the company or its supervisors at any time online.[154] The employee had posted remarks on Facebook angrily implying that her supervisor was mentally ill and disparaging him with expletives.[155] The case eventually settled, and in the settlement agreement, the employer agreed to alter its Internet policies and standards of conduct, which "improperly restricted" employees' rights to "discuss [their] wages, hours, and working conditions with [their] fellow employees and others."[156]

The NLRB recently filed additional complaints against employers who terminated employees based on their online speech.[157] The NLRB

---

[151]*Id*. at 84–85.

[152]Congress passed the NLRA in 1935 to protect workers' right to unionize, and it created the National Labor Relations Board to enforce the rights created under the Act. 29 U.S.C. §§ 151–69 (2006). Before the passage of the NLRA, employers could freely spy on, interrogate, and fire union members. *See generally* Coppage v. Kansas, 236 U.S. 1 (1915) (upholding an employer's right to fire its employee for refusing to sign a document stating the employee would withdraw from the union.).

[153]29 U.S.C. § 157.

[154]*See* Complaint and Notice of Hearing, *In re* Am. Med. Response of Conn., Inc., No. 34-CA-12576 (N.L.R.B. Oct. 27, 2010), *available at* http://www.jdsupra.com/post/documentViewer.aspx?fid=daf37177-f935-4fe0-be1f-82c65d0f2ac3.

[155]*See id*.

[156]Settlement Agreement, *In re* Am. Med. Response of Conn., Inc., No. 34-CA-12576 (N.L.R.B. Feb. 7, 2011), *available at* www.minnesotaemploymentlawreport.com/NLRB%20Facebook%20Settlement.pdf.

[157]Melanie Trottman, *NLRB Faults Company for Firing Workers Over Facebook Posts*, WALL ST. J. (May 18, 2011, 7:08 PM), http://online.wsj.com/article/SB10001424052748703509104576331861559033254.html.

filed a complaint against a car dealership that fired an employee who posted critical photos and comments on Facebook.[158] The employee complained that sales commissions were likely to drop because a promotional event sponsored by the dealership served only water and hotdogs.[159] As a result, the employee was terminated despite the fact that he had complied with his employer's request to delete his online rant.[160] The NLRB also has taken action against Hispanics United of Buffalo, a nonprofit organization in New York, after the organization fired five workers for Facebook postings that criticized working conditions.[161] It remains to be seen, however, whether the scope of "concerted activities" will eventually be broadened to include insulting rants about an employer.[162]

In addition to federal protections, a few states such as California, Colorado, Connecticut, New York, and North Dakota have passed legislation attempting to protect employees from reprisal for lawful off-duty conduct.[163] For example, the California statute prohibits demoting, suspending, or discharging an employee for lawful conduct occurring during nonworking hours away from the employer's premises.[164] Colorado and North Dakota's statutes provide an exception for conduct that has a relation to the employer's business interests.[165] Despite these protections,

---

[158]Press Release, NLRB, Chicago Car Dealership Wrongfully Discharged Employee for Facebook Post, Complaint Alleges (May 24, 2011), *available at* http://www.nlrb.gov/news/chicago-car-dealership-wrongfully-discharged-employee-facebook-posts-complaint-alleges.

[159]*Id*.

[160]*Id*.; Dave Jaimeson, *Facebook Posting Led to Worker's Unfair Firing: Feds*, Huffington Post (May 24, 2011, 3:15 PM), http://www.huffingtonpost.com/2011/05/24/facebook-posting-worker-fired_n_866353.html.

[161]Trottman, *supra* note 157.

[162]Settlement Agreement, *supra* note 156; *Company Settles Case in Firing Tied to Facebook*, N.Y. Times, Feb. 7, 2011, at B7.

[163]*See* Marisa A. Pagnattaro, *What Do You Do When You Are Not at Work?: Limiting the Use of Off-Duty Conduct as the Basis for Adverse Employment Decisions*, 6 U. Pa. J. Lab. & Emp. L. 625, 629 (2004). For a general discussion of free speech in America for employees both in and out of the workplace, see Bruce Barry, Speechless: The Erosion of Free Expression in the American Workplace (2007).

[164]Cal. Lab. Code § 96(k) (Deering 2011).

[165]Colo. Rev. Stat. §§ 34-402.5(1)(a)–(b) (2011); N.D. Cent. Code § 14-02.4-03 (2011).

employers who can prove a legitimate business interest in regulating their employees' off-duty conduct are generally given a free pass.[166] Case law interpreting lifestyle protection statutes reveal that courts tend to err on the side of employers when any business interest is at stake. Courts have permitted dismissals arising out of conduct such as employee extramarital affairs and criticism of an employer in the newspaper.[167]

In Canada, employers seeking to dismiss employees on the basis of unsavory off-duty conduct have often opted to terminate them with compensation to avoid litigation.[168] For example, one employer dismissed an employee with compensation after learning from a customer that the employee moonlighted as an actor in the adult film industry.[169] Labor arbitration standards for the evaluation of off-duty conduct have a long history in Canada. A 2011 decision from Nova Scotia, *Cape Breton-Victoria Regional School Board v. Canadian Union of Public Employees, Local 5050*, applied labor arbitration principles dating back to 1967 to evaluate the conduct of a school caretaker who had a sexual relationship with a student and ultimately married her.[170] In the 1967 precedent, *Re Millhaven Fibres Ltd. and Ontario O.C.A.W., Local 9-670*, the court determined the following factors to be relevant when evaluating off-duty conduct: (1) whether a crime had been committed, (2) the harm to the employer's reputation or product, (3) the ability of the employee to continue to perform his duties satisfactorily, (4) the effect on other employees, and (5) whether the employer is able to continue managing and directing employees efficiently.[171] Presumably, labor arbitrators in Canada will

---

[166]*See* Aaron Kirkland, Note, *You Got Fired? On Your Day Off?!: Challenging Termination of Employees for Personal Blogging Practices*, 75 UMKC L. Rev. 545, 552–57 (2006) (discussing how the presence of a legitimate business interest in regulating or monitoring employee conduct could provide employers with a defense against various different state law claims).

[167]For a discussion of these examples and others, see Robert Sprague, *From Taylorism to the Omnipticon: Expanding Employee Surveillance Beyond the Workplace*, 25 J. Marshall J. Computer & Info. L. 1, 30–31 (2007).

[168]*See* Levin et al. *supra* note 14, at 68.

[169]*Id*.

[170][2011] 298 N.S.R. 2d 258 (Can.), *available at* http://www.canlii.org/en/ns/nsca/doc/2011/2011nsca9/2011nsca9.html.

[171][1967] 18 L.A.C. 324 para. 20 (Can.).

reformulate and apply these traditional factors when evaluating online off-duty conduct and setting appropriate boundaries in employer policies.

In summary, U.S. law currently provides feeble protection to the electronic social communications of employees—whether on or off the job. Fourth Amendment case law suggests that, while expectations of privacy in digital communication may be recognized as reasonable in the future, several factors usually cut against a finding of reasonableness, including employer interests, the logistical demands of the workplace, and the general accessibility of the information. In fact, every U.S. law touching upon employee privacy grants significant deference to the legitimate business interests of employers.[172] Statutes that specifically govern the intersection of social media and workplace privacy have yet to be enacted. In their absence, it seems that U.S. employers may legally canvass social media sites for information on employees and candidates and act on the basis of the information found therein. Employers do not have an obligation to disclose their methods of gaining information, but they may not obtain access to digital profiles by coercion. Internationally, courts are similarly struggling with blurred boundaries between work and home. On the one hand, the French and Israeli courts, guided by an inalienable right to privacy in each jurisdiction, are more generous toward employees and their digital communications. Canadian courts, on the other hand, acknowledge that workplace policies play a role, but not an exclusive one, in shaping reasonable employee expectations. Against this uncertain legal backdrop, an analysis of current workplace practices and attitudes regarding social media participation is instructive. As the U.S. Supreme Court has asserted, these burgeoning norms will dictate the future of the law governing privacy in communication technologies.[173]

---

[172]*See* French v. United Parcel Serv., Inc., 2 F. Supp. 2d 128, 131 (D. Mass. 1998); Marsh v. Delta Air Lines, Inc., 952 F. Supp. 1458, 1462 (D. Colo. 1997).

[173]*See* City of Ontario v. Quon, 130 S. Ct. 2619, 2629–30 (2010).

II. The Privacy Expectations of Millennial Employees: A Survey

Whether referred to as Millennials,[174] the MySpace Generation,[175] Digital Natives,[176] or Generation Me,[177] the rising workforce is marked by its presence on the Web and its digital world view. Much has been forecast about the role this demographic will play in shaping the workplace of the twenty-first century.[178] Scholars have described the new generation of employees as ambitious—having high expectations for salary and career promotions—while perhaps incongruously placing a premium on private life, flexibility, and work/life balance.[179] They are reported to value a "fun" and relaxed workplace atmosphere[180] and tend to perplex employers with the "casualness of their e-mail and texting language" and their furtive participation on social media while on company time.[181] Regarding

---

[174]Howe & Strauss, *supra* note 13. The term Millennial is typically used to describe the cohort after Generation X and extends, according to Howe and Strauss, from those born from 1982 to 2002. *Id*. at 15. These authors posit that Millennials "are redefining the purpose of information technology," which involves communicating with networks of friends and "almost uninterrupted contact with each other." *Id*. at 272–75.

[175]Jessi Hempel, *The MySpace Generation*, Bus. Wk., Dec. 12, 2005, at 86 (describing the MySpace Generation as living comfortably in both the online word and the real world simultaneously, using online social networks as a community center), *available at* http://www.businessweek.com/magazine/content/05_50/b3963001.htm.

[176]John G. Palfrey & Urs Gasser, Born Digital: Understanding the First Generation of Digital Natives 346 (2008) (defining Digital Natives as those born after 1980 and discussing their presence on the Internet).

[177]Jean M. Twenge, Generation Me: Why Today's Young Americans Are More Confident, Assertive, Entitled—And More Miserable Than Ever Before (2006) (defining Generation Me as a generation growing up in the 1980s, 1990s, and 2000s). Twenge describes this generation as a self-important generation that believes everyone should follow and accomplish their dreams. The generation also has an extremely high focus on individuality. *Id*. at 4–7.

[178]Stephanie Armour, *Generation Y: They've Arrived at Work with New Attitudes*, USA Today, Nov. 6, 2005, at 1B; *The "Millennials" Are Coming*, CBS News (Feb. 11, 2009, 3:54 PM), http://www.cbsnews.com/stories/2007/11/08/60minutes/main3475200.shtml; Steve Tobak, *Gen Y: Solve Your Own Damn Workplace Issues*, BNET (May 13, 2010), http://www.bnet.com/blog/ceo/gen-y-solve-your-own-damn-workplace-issues/4604.

[179]Twenge, *supra* note 177, at 216–21.

[180]*Id*. at 218.

[181]Palfrey & Gasser, *supra* note 176, at 235.

privacy, they have been characterized as having "few qualms about sharing information that [others] might consider sensitive or private,"[182] as evidenced by their copious digital dossiers. For them, identity seems to be a "synthesis of real-space and online expressions of self."[183] Paradoxically, as a whole this group reports being unnerved by the idea of "someone aggregating, searching through, and acting on the basis of [the] information" they share online.[184]

The empirical project discussed in this part was undertaken to define attitudes about online privacy, specifically with regard to participation in OSNs.[185] We discuss and analyze that part of the survey pertaining to the respondents' usage of OSNs and their attitudes about online privacy vis-à-vis their employment context. Approximately 2500 Canadian and American undergraduate students answered questions relating to their employment status, privacy expectations concerning employer access to their OSN profiles, and the existence of and adherence to OSN workplace policies, among other things. These questions were close ended, as respondents chose from a list of various answer choices in multiple choice and Likert-scale format.[186]

Most respondents (94%) were between the ages of eighteen and twenty-four. Females (51%) and males (49%) were equally represented. Two-thirds of respondents (67%) were employed in paid positions and worked shifts while pursuing an undergraduate degree, as presented in Figure 1. Few respondents (less than 10%) were employed full time.

Ninety-two percent of respondents indicated that Facebook was their preferred OSN,[187] while only 2% reported belonging to LinkedIn, a business-oriented OSN mainly used for professional networking. The project's general findings suggest that respondents post a significant

---

[182]Twenge, *supra* note 177, at 217.

[183]Palfrey & Gasser, *supra* note 176, at 36.

[184]*Id*. at 51.

[185]*Supra* note 14 (discussing the findings); *see also* Levin et al., *supra* note 14 (providing a full report on the Canadian findings); Levin & Sánchez Abril, *supra* note 14 (offering general propositions regarding the survey and its overall findings).

[186]For a detailed discussion of the methodology as well as the complete survey instrument, see Levin et al., *supra* note 14, 80–92; Levin & Sánchez Abril, *supra* note 14, at 1048–51.

[187]*Id*. at 1023–24.

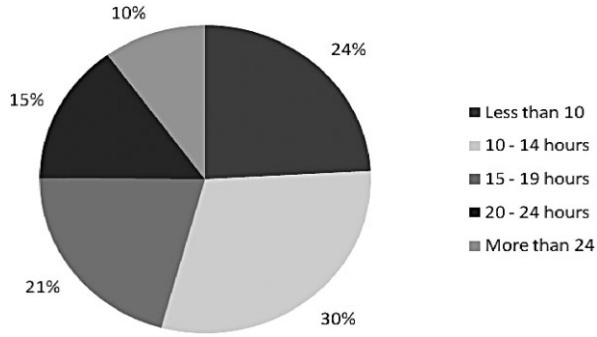

Figure 1. Hours respondents worked each week.

amount of truthful information about themselves online.[188] The most commonly shared pieces of information were pictures of themselves (77%), their hometown (76%), and their real full name (68%).[189] Respondents expressed some concern over their information reaching unintended audiences.[190] Seventy-two percent of respondents reported restricting access to their profiles by use of the privacy settings offered by the OSN Web sites.[191]

This part presents the findings related to the employment context to draw conclusions regarding the views of both current and future employees. The findings have been categorized into three thematic groups: (1) employer monitoring of OSNs, (2) work and personal life separation, and (3) workplace restrictions on OSN usage.

A. Employer Monitoring of Employee OSN Profiles

The data suggest a general ambivalence regarding employer access to employee OSN profiles. Most respondents reported being truthful about facts relating to their identities (such as full name, portrait photograph, hometown, etc.). In all likelihood, employers already enjoy access to these

---

[188]*Id*. at 1024–25.

[189]*Id*.

[190]*Id*. at 1026–27.

[191]*Id*. at 1034.

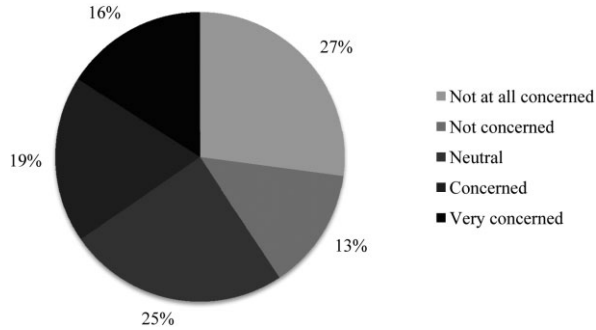

Figure 2. How concerned would you be if your employer accessed your social network profile information?

bits of identifying information without monitoring OSNs. However, some respondents reported voluntarily posting information about traditionally private or sensitive topics such as political preferences (24%) or their partner's name (25%). Interestingly, 62% posted their relationship status and 40% disclosed dating interests.[192] Perhaps Millennials consider that sharing such information, which is traditionally shared "at the water cooler," does not unduly compromise their privacy. It is unsurprising that this cohort, which has been characterized as valuing a casual and social work environment, would be inclined to share facts relating to private life with employers. This sharing reflects perhaps a population that does not construct the traditional segregation between social or home and work contexts on the basis of such facts.

Respondents generally acknowledged that posting information on social media sites makes it more accessible to many audiences. When asked how they would react to an employer accessing their social network profile information, respondents had mixed responses: 41% reported they would not be concerned if their employer accessed information on their OSN profiles, 35% indicated they were concerned or very concerned, and 25% were neutral. These findings, displayed in Figure 2, suggest that respondents were almost equally divided in their tolerance for employer access to their social media profiles. It may be that the less concerned group is not privacy wary, or it may be that they have made efforts to cleanse their profiles of private information and information that could cast them in a negative or unprofessional light in the eyes of employers.

---

[192]*See id*. at 1025 (providing a chart representing this data).

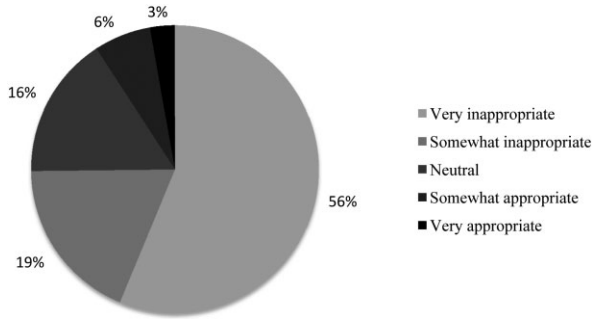

Figure 3. How appropriate would it be for you as a manager to use a social network to check up on what your employees do during personal time without them knowing?

Despite what seems like overall ambivalence toward employer intrusion into employees' social networking activities, 54% agreed with the statement, "It is not right when people can have access to information not intended for them."[193] This response suggests that respondents generally disapprove of unintended audiences learning information about them posted on social media profiles.

Overall, respondents disapproved of employer monitoring or accessing employees' OSN profiles. Seventy-five percent found this practice to be somewhat or very inappropriate (see Figure 3). This indicates that the respondents perceive an employer's monitoring of their private life as a breach of trust, especially in light of the fact that they tend to be willing to share certain private information openly with employers.

Respondents were slightly less perturbed, however, by employers checking on job applicants online without the applicant's knowledge. Fifty-six percent of respondents considered it somewhat or very inappropriate for employers to access OSNs to check the character of a job candidate (see Figure 4). The greater disapproval of intrusions in the private life of employees versus applicants may stem from a shared sentiment that judging a person based on his or her private life is more appropriate before hiring. After all, the purpose of the hiring process is to vet applicants based in part on their character and reputation.

Almost half (49%) of respondents found it somewhat or very inappropriate for employers to proactively search OSNs with the purpose of

[193] *Id*. at 1027.

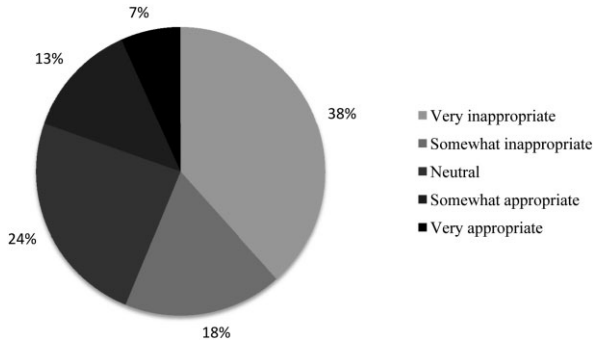

Figure 4. How appropriate would it be for you as manager to use a social network to check out the character of someone who has applied for a job?

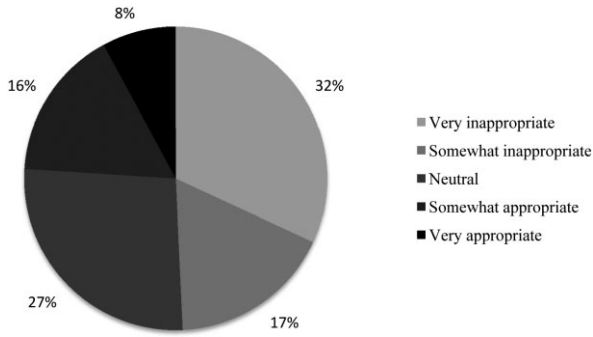

Figure 5. In your opinion, how appropriate would it be for you as a manager to proactively research social networks to identify potential high quality candidates for future positions?

identifying potential candidates for future positions (see Figure 5).[194] This figure suggests that individuals do not expect to be assessed as job candidates in their capacity as OSN members and that at least half of them are uncomfortable with the blurring of those boundaries.

Figure 5 further underlines the conclusion above: Respondents demonstrated clearly defined expectations of the uses and interpretations of their online profiles. While they are apt to share their profiles with many

[194]For a discussion of automated processes developed for such purposes, see, for example, Saul Hansell, *Let Your Boss Find Your Facebook Friends*, N.Y. Times (Dec. 15, 2008, 3:28 PM), http://bits.blogs.nytimes.com/2008/12/15/let-your-boss-find-your-facebook-friends.

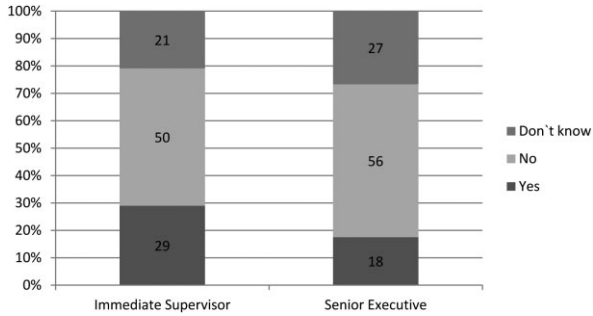

Figure 6. In your current or most recent workplace, which of the following belongs to your online social network?

and disparate audiences, they reject one audience evaluating them on the basis of information intended for another audience. Elsewhere, we have labeled this attitude "network privacy."[195] Below we elucidate network privacy in the employment context.

B. Work/Personal Life Separation

While a majority of respondents reported not inviting their employers or supervisors to be part of their OSN, many respondents considered it appropriate to blend worlds in that manner. Nearly one-third (29%) of respondents included their immediate supervisor as an online "friend." As discussed below, some welcomed their employers' participation in their social networks; others reported being required to give their employers access to their profiles. These data are consistent with the conclusion above regarding the openness and transparency of Millennial employees vis-à-vis their workplace cohorts, as well as the characterization of Millennials as valuing casual and social work environments.

In what seems like a significant departure from traditional workplace practices, 18% of respondents reported the participation of a senior company executive in their OSN (see Figure 6). The survey did not define "senior company executive," but made it clear this was a person with which offline socialization would not occur, someone senior to the immediate supervisor. The data indicate, therefore, the internal blurring of bound-

[195]Levin & Sánchez Abril, *supra* note 14, at 1045–46.

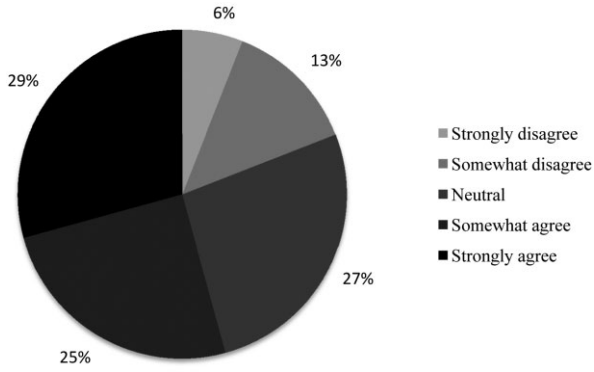

Figure 7. Work life is completely separate from personal life, and what you do in one should not affect the other.

aries, or flattening of hierarchies, that digital media facilitate. Rather than waiting for the "elevator pitch" that may never come, some young employees now have access to higher-level executives and are willing, perhaps eager, to interact with these superiors in a digital context. The data also indicate the willingness of some senior corporate executives to communicate with junior employees through OSNs.

Respondents were divided in their opinions on the propriety of supervisors socializing with employees through a social network. Thirty-six percent opined that superior-to-employee socialization is somewhat to very appropriate, 33% were neutral, and 31% found it to be somewhat to very inappropriate. The equal distribution signals that respondents' opinions may depend on other factors, such as the ages and genders of the parties, the workplace culture, the industry, and the unsettled norms that are still actively forming in this area. Despite the fact that approximately one-third of respondents included supervisors or senior company executives or both in their OSNs, respondents tended to disassociate work life from personal life. As shown in Figure 7, 54% of those surveyed strongly or somewhat agreed that "work life is completely separate from personal life, and what you do in one should not affect the other." Eighteen percent of respondents somewhat or strongly disagreed with that statement. Further, 56% disagreed that "knowing how a person behaves outside of work hours gives managers insight into whether that person is ready for a promotion." Only 16% of respondents agreed that off-duty behavior is evidence of career readiness or potential, which is highly consistent with a separatist

view of professional and personal life. The plurality of those surveyed did not believe that their participation on social media would significantly impede their professional development. Over half (52%) somewhat or strongly disagreed with the following statement: "People wanting to move up the career ladder should not be part of OSNs because [they] can't completely control what is posted about [them]." Nineteen percent agreed with the foregoing statement, despite their own admitted participation on OSNs, which indicates that the need to be connected may supersede any perceived threat to privacy or reputation. Perhaps it indicates that identity presentation and audience segregation should be facilitated by other legal and technological means.

One of our hypothetical scenarios probed the relationship between online behavior and workplace consequences. We asked respondents if they had heard of the scenario occurring or if it had occurred to them personally. Putting themselves in the place of the hypothetical actor, respondents were also asked to attribute responsibility for the consequences of the scenario to the various parties involved. Finally, they were asked whether they believed real harm could arise from the event. The hypothetical involved an employee who was caught in a lie when his employer found incriminating information about him on a social media Web site. The scenario read as follows:

> You called in sick to work because you really wanted to go to your friend's all day graduation party. The next day you see several pictures of you having a great time at the party. Because the pictures are dated you start to worry about whether you might be caught in your lie about being sick. You contact the developers of the social network and ask that the pictures be taken down because the tagging goes so far, it would take you too long to find all the pictures. There was no response from the network. You are stunned to be called in by your supervisor a week later to be advised that you were being "written up" for taking advantage of sick leave and put on notice that if it happened again you would be terminated.

When attributing responsibility to the various parties for the adverse consequences, 78% assumed personal responsibility, while the rest laid blame on the "snooping" supervisor.[196] Nearly half (47%) of respondents were concerned that material *about* them was not posted *by* them.[197] Seventy-one percent respondents agreed that "real harm"—defined as

---

[196]*Id*. at 1033.

[197]*Id*. at 1037.

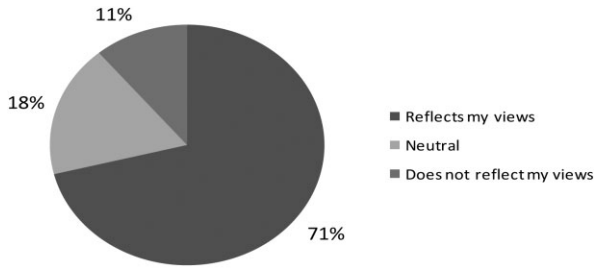

Figure 8. This scenario could result in physical, economic, or reputational injury in the offline world.

physical, economic, or reputational injury—could arise from this occurrence (see Figure 8).[198] Respondents reported experiencing an invasion of privacy when information moved, uncontrolled by participants, across networks and contexts.

These statistics suggest the same contradiction that we have seen above: the respondents were willing to give digital access to their personal lives but resists being judged on the basis of what they disclose. They expect their work and personal lives to be segregated regardless of their unified and publicly accessible digital identity.

C. Workplace Policies on Employee Participation in Social Media

The survey results show that the preponderance of the respondents' employers did not adopt clear policies regarding social media use in the workplace. Sixty-two percent of respondents indicated that their workplaces did not have formal policies on social networking (see Figure 9). Nineteen percent of respondents did not know if their employers had a policy on social media usage. Respondents' lack of clarity as to the existence of a policy and its contents has clear implications on their expectations of privacy both in and out of the workplace.

One-fifth of respondents were subject to a formal workplace policy on social media. Of respondents whose employers have a formal workplace policy, 32% reported that the policy banned employee access to social media during company time. Others only forbade any association with or mention of the company name on the employee's profile. Respondents

---

[198] *Id.* at 1043.

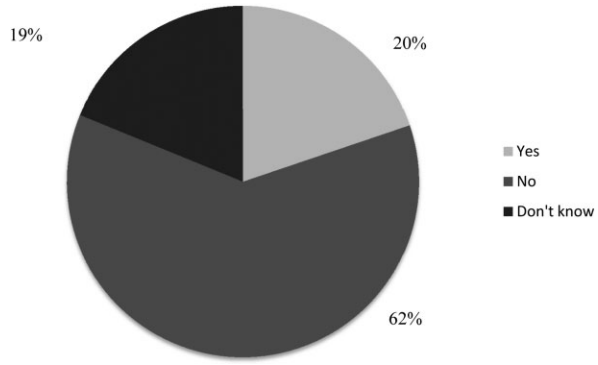

Figure 9. Does your workplace have a formal policy related to use of OSNs during company time?

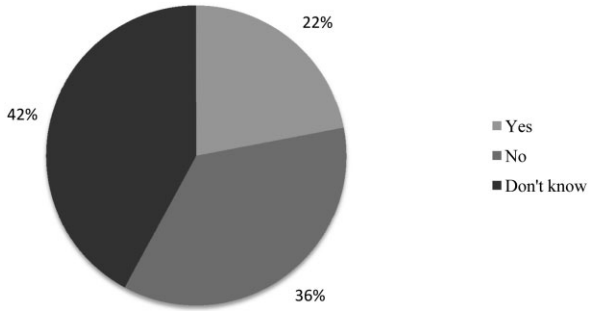

Figure 10. If there is a policy that forbids all use of OSNs during work time, do employees generally abide by the policy?

whose employers had formal policies admitted adherence to such policies was generally poor. Only 22% of respondents working for an employer with an OSN policy stated that employees abided by the policy (see Figure 10). Another recent survey found that nearly half of office employees access Facebook during work hours.[199]

---

[199]Nucleus Research, Facebook: Measuring the Cost to Business of Social Networking (2009), http://nucleusresearch.com/research/notes-and-reports/facebook-measuring-the-cost-to-business-of-social-notworking/.

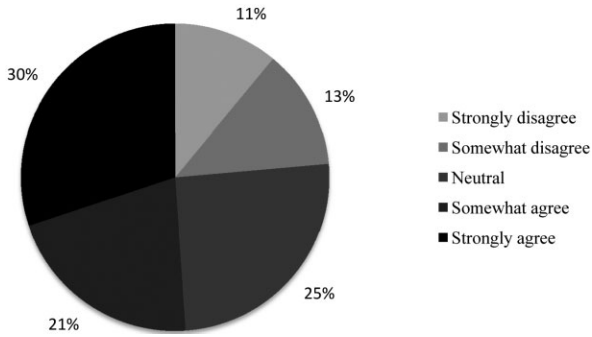

Figure 11. In my opinion, accessing OSNs should not be allowed during work hours.

At the same time, when asked to answer in the role of manager, 51% of respondents agreed that "accessing OSNs should not be allowed during work hours" (see Figure 11). This indicates that, although employees habitually access their OSNs during working hours, there is a generalized acknowledgment that such practice is counterproductive and that employer restrictions on this practice during work hours are reasonable.[200]

Some businesses have begun policing their employees' online behavior by way of requiring employees to add superiors to their OSN profiles.[201] As noted above, 18% of respondents reported a senior executive requested to (and was) added as a friend or connection to an OSN profile. If employer access is obtained by implicit or explicit coercion, this practice clearly contravenes the SCA and other laws.[202] Eighty-one percent of respondents considered it inappropriate for employees to be required to invite their supervisor to their OSN profile. Considering that only 31% of respondents believed it inappropriate for managers to socialize with employees via a social network after work hours and that 29% of respondents included their immediate supervisor, it is likely a considerable

[200]It is possible that some respondents may have interpreted "work time" and "work hours" broadly, to include breaks and meal times.

[201]*See* Jared Sandberg, *OMG—My Boss Wants to "Friend" Me on My Online Profile*, WALL ST. J., July 10, 2007, at B1.

[202]*See supra* notes 90–101 (discussing the anti-coercion principle as applied in *Pietrylo v. Hillstone Rest. Grp.*, No. 06-5754(FSH), 2009 WL 3128420 (D.N.J. Sept. 25, 2009)).

number of employers may already have access to their employees' information on an OSN and would, therefore, not violate the SCA. Given these employee practices, the current legislative framework does not offer meaningful protection for employee information online.

D. Summary

The data suggest that Millennial employees maintain an expectation of privacy regarding information disclosed on social media, especially in relation to their current and prospective employers. They acknowledge the increased accessibility and transparency of their private lives when memorialized on social networks. They also understand that they lack control over the information posted about them, the way such information is interpreted, and the unintended audiences that may access the information.

Despite these realizations, Millennial respondents displayed a clear discomfort with the idea of information flowing across contexts. Three-fourths found it inappropriate for an employer to check employee off-duty conduct via social networks. More than half (56%) objected to the practice of social media background checks. More than half also expressed that work and personal life should not be commingled and that individuals should not be judged across these contexts. When researchers posed a scenario in which an employee was caught lying via a social network posting, most respondents agreed that the employer invaded the employee's privacy—even though the employee was engaged in wrongdoing.

Millennials seem to take for granted that their work and personal lives do *not* intersect and that their actions in one should *not* affect the other, as marked by their overwhelming belief that an employee's conduct outside the office should not be used as a basis for making promotion determinations. Their objection to this increasingly common practice[203] reflects an expectation that they would not be discriminated against on the basis of their online identities. However, the practice of trawling the web

---

[203]*See* Deloitte, 2009 Ethics and Workplace Survey 6 (May 21, 2009), http://www.deloitte.com/assets/Dcom-UnitedStates/Local%20Assets/Documents/us_2009_ethics_workplace_survey_220509.pdf (reporting that, while 53% of employee respondents said their social networking pages are none of their employer's business, 40% of business executive respondents disagreed and 30% admitted to informally monitoring social networking sites).

for information about applicants and employees—and perhaps discriminating on that basis—will no doubt continue to become the norm unless restricted by law or technology.

Although many respondents expressed unease at the lack of control they exercise over the information about them available on OSNs,[204] it is clear that respondents were not willing to forgo participation in social networks to achieve privacy or separation of work and personal life. They displayed a strong desire to socialize, to interact, and to share truthful information about themselves on social networks. The majority believed participation on social networks is worth the risk; only a small percentage agreed that participation in social media can impede professional development because individuals cannot fully control what is posted about them.

There are indeed indications in our findings that Goffman's traditional theories on audience segregation may no longer hold, because a fair number of respondents welcomed the blurring of work and personal boundaries. Roughly a third invited the participation of their bosses in their OSNs, with even more reporting that employer access to their social networking profile would not cause them concern. Somewhat surprisingly, a small percentage responded that work and personal life should not be separate. This may indicate a growing trend favoring casual work environments, it may reflect a lack of concern toward transitory "student jobs," or it may be indicative of the naiveté of a young demographic with respect to the business world.

Overall, the findings are consistent with what we have labeled network privacy,[205] which can be defined as privacy within the information's intended network and context.[206] An invasion of privacy is experienced when information moves, uncontrolled by participants, across networks and contexts.[207] The information then loses what Professor

---

[204]Levin & Sánchez Abril, *supra* note 14, at 1037.

[205]*Id*. at 1045–46.

[206]*Id*.

[207]*See generally* Lior Jacob Strahilevitz, *A Social Networks Theory of Privacy*, 72 U. Chi. L. Rev. 919 (2005) (arguing the harm and measure of privacy breaches actually occurs upon the information dissemination outside or beyond the certain social networks to which the victim of the breach reasonably expected the information to travel).

Helen Nissenbaum has called its "contextual integrity."[208] Relevant to the discussion here, employers access and interpret information meant for employees' social friends, sometimes leading to adverse consequences. Network privacy appears to carry with it a paradox: Millennial employees generally want privacy from unintended employer eyes and yet share a significant amount of personal information online, knowing it could become available to employers and others. The following part will discuss this ostensible paradox and suggest a framework for the continued discussion of network privacy in law and business.

III. The Future of Digital Privacy in the Workplace

Prior to the phenomenon of online participation, Goffman's notion of audience segregation shielded employees from employers' judgment of their private lives. Information about employee performances outside the work sphere was less readily available to employers. Our findings suggest that Millennials understand digital media and that cross-performance access (i.e., employer access to Millennials' "personal" performances) may occur, but they are not willing to sacrifice Internet participation to segregate their multiple life performances. Because it is technically and legally unfeasible to hide their multiple life performances, Millennials rely on employers to refrain from judging them across contexts.

With minimal technological, contractual, or statutory barriers, it is not reasonable for an individual to expect others to refrain from judging him or her based on publicly accessible information, especially in the business world, where organizations have legitimate and compelling legal and economic reasons to protect their reputations, trade secrets, and workplace environments. U.S. law drives employers to evaluate applicants and employees on all available, legally permissible information. While a majority of the surveyed Millennials found employer monitoring of employee online profiles inappropriate, an employee's remedy in U.S. law is contingent on whether the information obtained by the employer was

---

[208] *See* Helen Nissenbaum, *Privacy As Contextual Integrity*, 79 Wash. L. Rev. 119, 136–43 (2004) (defining the concept of "contextual integrity" and arguing that it is the "benchmark of privacy").

publicly available. The "reasonable expectations of privacy" bar is high.[209] More often than not, the large number of OSN friends with whom Millennials share information would clearly eliminate any reasonable expectation of privacy. Computer usage policies, which employers broadly adopt and employees often thoughtlessly accept, also inform the reasonable expectation analysis.[210] Though our survey respondents generally expect the information they post on their OSNs will remain private from unauthorized parties, their expectation is not currently recognized by U.S. law as reasonable and legally protectable.

Millennials' online participation appears inconsistent with their stated expectations of privacy and audience segregation. However, what seems at first glance as incongruous is readily understandable as an attempt to achieve some control in a world where individuals will inevitably amass a public digital dossier. The only way to control the dossier is to participate actively in shaping it, rather than to renounce entirely online participation.[211]

A picture emerges of a society that is, surprisingly, less free, in which tools for self-expression turn oppressive in the absence of normative, technological, and legal controls. Normative controls may come in the form of social acceptance of certain types of disclosures or skeletons in the online closet. Some have suggested that businesses and society in general will necessarily become more forgiving of unseemly personal disclosures eventually, because so many individuals will have online evidence of some purportedly inappropriate behavior.[212] Technological controls, which have not yet been widely perfected, could one day give individuals the capacity to shield unwanted audiences from their online expression and identities. As we wait for normative and technological controls to mature, the law should protect individuals from employers who are intrusive, discriminatory, or quick and unforgiving in their judgments based on unsubstantiated online information.

---

[209] *See supra* notes 31–65.

[210] *See supra* Part I.A.

[211] Clive Thompson, *The See-Through CEO*, WIRED (Mar. 2007), http://www.wired.com/wired/archive/15.04/wired40_ceo.html.

[212] *See* Lew McCreary, *What Was Privacy?* HARV. BUS. REV., Oct. 2008, at 126, 129 (citing David Weinberger from the Berkman Center for Internet & Society as proposing such a "forgiveness" principle and indicating that its development may result over time as the digital-native generation ages).

As discussed above, the law does not currently offer meaningful protections. Statutory protections, such as the ECPA, were enacted long before the emergence of online social technologies.[213] Updating these and other statutes to reflect the current technological reality is essential.[214] While some initiatives have already gained some traction in Congress,[215] this messy, reactionary lawmaking is poor guidance for businesses and individuals.

A continued absence of legal protection will eventually lead to a life that Goffman called "unbearably sticky."[216] We find such a transparent future untenable and contrary to the stated wishes of network privacy expressed by our survey respondents. As such, we propose below a series of recommendations for legal and business practices. These recommendations are drawn from domestic and international case law and informed by the empirical results of our survey. They are designed to protect employees who participate online from discrimination, intrusion, harassment, and other dignitary harms, while balancing the reasonable business and reputational interests of employers.

Because social media privacy encompasses so many facets of the complex employment relationship, it is clear that there can be no one-size-fits-all solution. Instead, initiatives should be tailored to specific unwanted outcomes, take into account the nature of digital information and communication,[217] and give both employees and their employers the latitude to set

---

[213]Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 878 (9th Cir. 2002) ("The ECPA was written prior to the advent of the Internet and the World Wide Web. As a result, the existing statutory framework is ill-suited to address modern forms of communication like Konop's secure website.").

[214]While a worthwhile and important task, making specific recommendations regarding the modernization of U.S. privacy statutes is beyond the scope of this article.

[215]In May 2011, Senator Patrick Leahy introduced the Electronic Communications Privacy Act Amendments Act of 2011, which would update the ECPA and introduce some new safeguards for consumers. Press Release, U.S. Senator Patrick Leahy, Leahy Introduces Benchmark Bill to Update Key Digital Privacy Law (May 17, 2011), http://leahy.senate.gov/press/press_releases/release/?id=b6d1f687-f2f7-48a4-80bc-29e3c5f758f2.

[216]Goffman, *supra* note 1, at 49 ("Urban life would become unbearably sticky for some if every contact between two individuals entailed a sharing of personal trials, worries, and secrets.").

[217]*See generally* Ciocchetti, *supra* note 23, 324–57 (categorizing employee surveillance and monitoring practices and prescribing analysis based on a more specific than one-size-fits-all approach).

the tone for their employment relationship in context- and firm-specific ways. The following subsections will address these recommendations in turn.

A. Clear and Communicated Employer Policies on Technology and Internet Participation

Even though social media have become pervasive in the lives of employees, their use in the workplace remains legally ungoverned and normatively unsettled. Employees bring to the shared workplace diverse and often paradoxical attitudes toward social media. Without legal or normative guidance, employers are in the best position to set parameters for behavior and expectations that reflect and honor the realities of the modern world.

What legal guidance there is points to employer responsibility. All of the international cases on workplace privacy that we canvassed stressed the importance of explicit workplace privacy policies. In Israel, where courts have been extremely protective of employee privacy, the existence of clear privacy policies is a precondition for any employer action.[218] Recent decisions from Canadian courts illustrate how the absence of understandable workplace privacy policies affects employer action.[219] In the United States, much depends on the language and communication of the corporate policies that regulate the employer–employee relationship.

Our survey shows that a striking 82% of respondents either were not subject to a workplace policy on social media or did not know if they were. Of the remaining 18% who reported being subject to a workplace OSN policy, most reported the policies were ineffectual, and compliance was poor. These statistics provide evidence that employees are unlikely to take the time to read and understand written policies or to condition their employment on the content of such policies. This is consistent with the literature and empirical reports on click-wrap agreements and form policies.[220] Employee-respondents' lack of attention to these policies may result from some combination of the incomprehensibility, legalistic style, or

---

[218] *See supra* notes 114–21 and accompanying text.

[219] *See supra* note 74 and accompanying text.

[220] *See* Adam Gatt, *Electronic Commerce—Click-Wrap Agreements: The Enforceability of Click-Wrap Agreements*, 18 Comp. L. & Security Rep. 404 (2002); *see also* Ryan J. Casamiquela, *Contractual Assent and Enforceability in Cyberspace*, 17 Berkeley Tech. & L. J. 475 (2002).

overbreadth of the policies and employees' perception that the policies are inapplicable or underenforced. To achieve buy-in from employees, and thereby establish a uniform privacy culture with clear expectations, technology and Internet participation policies must be specific and clearly articulated in a manner consistent with the organization's culture, while reflecting emerging society-wide norms. Meaningful Internet participation policies should contain a high level of detail specific to the type of communication (cell phones, text messages, computer), the character of the medium (company e-mail versus Internet-based e-mail), the nature of the online forum (chat rooms, blogs, etc.), the location of the message sender (on the employer premises versus at home, on employer time or off duty), and the effect of the hardware and transmitting systems' ownership on the message's privacy. Employees also should be informed about the types of information they are prohibited from transmitting (such as harassment or libel about a coworker, confidential and proprietary information, unauthorized expressions of endorsement using the company logo or affiliation, and the like). Further, such policies should remind employees that digital information is fluid and difficult to control and that employees must comply with Web sites' terms of service.

An employer also should articulate and justify its technology and Internet participation policy in terms of the organization's purpose and mission. Compelling policies will have a nexus to a shared purpose among employees and the general nature of the business. For example, employees of a private school, who are charged with being role models to children, are much more likely to understand and abide by limitations on certain off-duty online behavior than employees whose public personas do not logically affect their workplace role.

Finally, technology and Internet participation policies should realistically reflect the stated perceptions and common expectations of employees. Employers should consider polling employees regarding their views or inviting representative employees to give input on proposed policies. Surveys detailing the privacy climate and biases of the incoming workforce, such as the one reported in this article, may be particularly instructive in the formulation of employer policies.

However, as both domestic and international courts have found, the mere existence of a policy is not sufficient to support privacy expectations among employees. For example, *Pure Power Boot Camp v. Warrior Fitness Boot Camp* admonished that a blanket e-mail policy stating that employees have no privacy in any matter flowing through the employer's system may

not be enough to eviscerate an employee's expectation of privacy.[221] Courts have reasoned that the totality of circumstances, including both implicit and explicit messages sent by employers, informs whether a reasonable expectation of privacy exists.[222] Employers should be cognizant that written policies must be carried through, enforced consistently, and incorporated into the organization's culture to form the rational foundation of employees' privacy expectations.

B. An Employee's Right to Designate Private Spaces

Throughout this examination of workplace privacy concerning social media, several recurring themes emerge. One is the individual's real or imagined construction of what Goffman termed "fixed barriers to perception."[223] Another is the complexity of creating those fixed barriers we call "privacy" within an employer's physical domain.

In the face of these challenges, courts have repeatedly remedied the employee's inequity by acknowledging the realities of the employment relationship and allowing employees to burrow holes of privacy within their employer-controlled spaces. ECPA jurisprudence has acknowledged that an employer's mere request for access to an employee's password-protected sites can constitute coercion, given the context of the employment relationship.[224] The U.S. Supreme Court has held that certain areas of the office can be deemed private, subject to the "operational realities of the workplace."[225] The French Supreme Court has gone further, giving employees a right to create certain private spaces by labeling them as such.[226] In these decisions, the French Supreme Court recognized that

---

[221]587 F. Supp. 2d 548, 559 (S.D.N.Y. 2008) (finding that an employer's e-mail policy, which stated that "e-mail users have no right of personal privacy in any matter stored in, created on, received from, or sent through or over the system," was not enough to eviscerate an employee's expectation of privacy in his personal e-mail even if accessed at work).

[222]*Id*. at 561.

[223]Goffman, *supra* note 1, at 238.

[224]*See, e.g*., Pietrylo v. Hillstone Rest. Grp., No. 06-5754(FSH), 2009 WL 3128420, at *1 (D.N.J. Sept. 25, 2009).

[225]O'Connor v. Ortega, 480 U.S. 709, 717 (1987).

[226]*See, e.g*., X v. Y-Z, Cour de Cassation [Cass.] [supreme court for judicial matters] soc., Dec. 15, 2009, No. 2561 (Fr.); La Société Seit Hydr'Eau v. M. J-M, Cour de Cassation [Cass.]

employees may legitimately store certain private information on their workplace computers and that boundary crossing is inevitable.

The French Supreme Court's approach is compatible with our survey respondents' stated expectations and behaviors. Our survey results suggest that young employees are likely to disregard traditional work–home boundaries by intermingling audiences and accounts. Defining online behavior with territorial distinctions is simply impracticable. Most people do not have separate devices for different types of digital communication. As such, we propose the creation of a right of employees to designate certain spaces as private within the workplace or employer-provided spaces. This can be in the form of a tag on a picture labeled "confidential," the subject line of an e-mail reading "private," or the label on a digital folder. Employees should, however, bear the burden of shielding what they want to keep private. This is a well-established tenet of trade secret and privacy tort law. Moreover, protecting information prospectively—that is, before a leak or a breach—by labeling it as private both reduces the potential risk of disclosure and simplifies the messy ex post facto evaluation of an employee's subjective expectations. In addition to resonating with emerging technological and social practice, such a right allows employees some reasonable and circumscribed freedom to act within their employer's policies.

C. An Applicant's Right to Transparency

Fifty-six percent of our survey respondents disapproved of employers using social networks to perform background checks on job applicants,[227] while 49% found it inappropriate for employers to trawl social network profiles for job candidates.[228] Despite these findings, reports suggest that surreptitious Internet searches of job candidates and employees have

---

[supreme court for judicial matters] soc., Oct. 21, 2009, No. 2044 (Fr.), *available at* http://www.courdecassation.fr/publications_cour_26/arrets_publies_2986/chambre_sociale_3168/2009_3332/octobre_2009_3246/2044_21_13949.html; Société Nikon France SA v. M. Onof, Cour de Cassation [Cass.] [supreme court for judicial matters] soc., Oct. 2, 2001, No. 4164 (Fr.), *available at* http://www.courdecassation.fr/jurisprudena_2/chamber_sociale_576/arret_no_1159.html.

[227]*See supra* Part II.A, Fig. 4.

[228]*See supra* Part II.A, Fig. 5.

become widespread.[229] In fact, employers are often reluctant to acknowledge their use of online resources for selection processes and reluctant to disclose the manner in which they gain access to information applicants seek to disclose exclusively to their friends online.[230] The informal, clandestine quality of the practice may disadvantage applicants who participate online. The practice may also provide employers with a secret backdoor for illegal employment discrimination.

Regulations on employers' screening of social media profiles could serve to placate the concerns of social media users in the workforce. Some have called for the application of statutory standards of fairness and transparency for social media background checks and employer evaluation of employee off-duty conduct.[231] Such proposals would require employers to disclose their screening practices, including the ways they use online information in making employment decisions. This disclosure requirement would significantly deter employers with a penchant for illegal discrimination and would simultaneously alert applicants who may not know the effect of their online reputation or behavior on their employment prospects.

D. An Employee's Right to Respond and Rebut

Similarly, employees who are adversely affected by employment decisions based on online information or off-duty online conduct should have the opportunity to know the contents of the information and should have the right to respond regarding the information's integrity and veracity. Online information, by nature, is often presented in a contextual vacuum. A photograph or comment that may seem inappropriate to unintended audiences can easily belie the real circumstances under which it occurred. Our survey revealed that most students are uncomfortable with others viewing information about them out of context. Fifty-two percent of respondents agreed that "it is not right when people can have access to

---

[229]*See* Alan Finder, *When a Risque Online Persona Undermines a Change for a Job*, N.Y. Times, June 11, 2006, at 1.

[230]These uses of online resources may violate an OSNs' terms of service. *See* Brandenburg, *supra* note 126, at 612–13; Byrnside, *supra* note 126, at 465–67.

[231]*See, e.g.*, Davis, *supra* note 132; Byrnside, *supra* note 126.

information not intended for them."[232] Further, individuals often cannot control what is said about them or what images of them are "tagged" in online fora. While some facts about a person may prove to be true, digital information's vulnerability to abuse cannot be overlooked.

In the event online information either suggests employee involvement in criminal or unethical activity or evidences a breach of loyalty, employers should be free to take action against the employee only after revealing the source of the discrediting information and offering the employee a meaningful opportunity to respond or to prove the information inaccurate. This type of process would be similar to what the courts have required of government employers under the Fifth Amendment's Due Process Clause. For example, in *Perry v. Sindermann*, the U.S. Supreme Court held that, when a public employee's continued employment was implied and subject only to a for-cause dismissal, such employee had the procedural due process right to contest the legitimacy of the claims brought against him when fired.[233]

E. An Individual's Right to Delete

About half of respondents in our survey (47%) were concerned that material posted about them was not posted by them, and 71% of respondents believed that online posts that cast them in a negative light could adversely affect them physically, economically, or reputationally in the offline world.[234] In response to this sentiment, the European Commission recently introduced into the European Parliament legislation that seeks to create a "right to delete" or "right to be forgotten."[235] This proposed legislation

---

[232]*See* LEVIN ET AL., *supra* note 14, at 41.

[233]408 U.S. 593 (1972).

[234]*See supra* notes 197–98 and accompanying text.

[235]Press Release, European Union, European Commission Sets Out Strategy to Strengthen EU Data Protection Rules (Nov. 4, 2010), http://europa.eu/rapid/pressReleases Action.do?reference=IP/10/1462. In Spain, the country's robust laws protecting individual honor, intimacy, and privacy have already been interpreted as granting such a right, but Spanish lawmakers remain baffled regarding how to implement it. *See* Agencia Española de Protección de Datos, *Study on the Privacy of Personal Data and on the Security of Information in Social Networks*, 62–67 (2009), *available at* http://www.inteco.es/Seguridad/Observatorio/Estudios/est_red_sociales_es. Article 18.4 of the Spanish Constitution of 1978 directs the law to "regulate information technology in order to guarantee individual honor and personal and

would allow users to compel Web sites, including social networking sites and possibly even search engines, to delete users' personal information upon request, essentially giving users a right to be "forgotten" online.[236] If passed, individuals would obtain the right to request any personal information that is not in the public interest be deleted from a Web site.[237]

Armed with this right, employees would be able to request the deletion of images and information about themselves on a site-by-site basis, allowing for significant reputation cleansing or correcting. On the one hand, this proposal grants the Millennial generation nothing more than the right of forgetting that the natural frailty of the human memory gave past generations.[238] On the other hand, it is an opportunity to rewrite the past and potentially (yet figuratively) get away with murder. From an employer's perspective, employees' ability to delete negative information about themselves from the Internet provides an alternative solution to resolve instances of inappropriate online conduct, without having to resort to termination.

Although the proposed right has yet to be fleshed out from a practical perspective, a system akin to the notice and takedown procedure under the United States' Digital Millennium Copyright Act of 1998 may be applicable.[239] Among other things, that copyright statute limits the infringement liability of Internet service providers who expeditiously take

---

familial intimacy and the exercise of individual rights." C.E., B.O.E. n. 311, Dec. 29, 1978 (Spain), *available at* http://noticias.juridicas.com/base_datos/Admin/constitucion.t1.html#a18 (as translated by author); *see also* L.O.P.J. 15/1999, Dec. 13, 1999 (Spain) Protección de Datos de Carácter Personal, *available at* http://www.boe.es/boe/dias/1999/12/14/pdfs/A43088-43099.pdf.

[236]Matt Warman, *Online Right 'To be Forgotten' Confirmed by EU*, Telegraph (Mar. 17, 2011, 12:53 PM), http://www.telegraph.co.uk/technology/Internet/8388033/Online-right-to-be-forgotten-confirmed-by-EU.html. The proposal would grant national privacy bodies in EU member nations the power to investigate and prosecute offending websites. *Id*.

[237]For example, individuals would be able to request that Facebook delete an unflattering photograph of them, provided the photograph's presence online is not in the public interest. *Id*.

[238]*See* Viktor Mayer-Schönberger, Delete: The Virtue of Forgetting in the Digital Age 2 (2009) (discussing the effects of modern technology and the Internet specifically on humans' newfound inability to forget as content remains pervasively available online).

[239]17 U.S.C. § 512(c)(3) (2006).

down infringing material upon receipt of proper notification from the copyright owner. The statute builds in certain safeguards to protect against fraud, error, and abuse. For example, all representations in the notices are made under penalty of perjury,[240] and the process allows the initial uploader of the allegedly infringing material to file a counter notification in response to the takedown.[241] In theory, this procedure is workable in the privacy context, where individuals (like copyright owners) could petition Web sites to take down reputation-tarnishing material.

In reality, Web sites do not have the economic or legal incentives to establish this costly procedure because they are not liable for invasions of privacy as they would be for copyright violations.[242] Further, establishing copyright ownership and infringement, although difficult, is a more comfortably objective task than establishing whether a piece of information is public or the subject of legitimate public interest. For legal reasons as well, the introduction of a right to be forgotten (and an accompanying takedown system) seems highly unlikely to pass muster under U.S. law. In Europe, the archetypal advocate for this right is a Spanish woman whose drug conviction was pardoned in 1995.[243] The woman petitioned Google to remove all information about her past because she objected to the inevitable association a search of her name would produce with news of her pardon (which was published in an official national bulletin and previously accessible to a limited few by virtue of its format).[244] While this request may not seem extreme to European eyes, it is outlandish to American observers. U.S. law unequivocally holds that any information that is accessible or available to the public cannot be private. As such, there

---

[240]*Id*.

[241]*Id*. § 512(g)(2).

[242]*See* Communications Decency Act, 47 U.S.C. § 230 (2006); Jeff Kosseff, *Defending Section 230: The Value of Intermediary Immunity*, 15 J. Tech. L. & Pol'y 123, 149 n.151 (2010) (collecting example cases); Molly Sachson, Note, *The Big Bad Internet: Reassessing Service Provider Immunity Under § 230 to Protect the Private Individual from Unrestrained Internet Communication*, 25 J. Civ. R. & Econ. Dev. 353, 366–67 (2011).

[243]Rosario G. Gomez, *Quiero que Internet se Olvide de Mi*, El Pais (Jan. 7, 2011), http://www.elpais.com/articulo/sociedad/Quiero/Internet/olvide/elpepisoc/20110107elpepisoc_1/Tes.

[244]*Id*.

is a meager right to privacy in public places,[245] public documents,[246] and truthful-yet-shameful histories.[247]

However, the spirit of this proposed European right should be adopted privately to safeguard individual dignitary interests. Employer policies could include grandfather clauses to forgive past reputational scars evidenced online before the date of hire, and employers could help their employees manage their individual reputations online in a mutually satisfactory and beneficial way.

F. An Employee's Right to an Off-Duty Private Life

As noted above, the EU's privacy paradigm is more in line with the reported online privacy expectations of our respondents. European employees have a right to dignity and a private life that does not stop at the employer's doorstep. This right balances the employer's property rights against the employee's dignitary protection.[248] Canadian courts have simi-

---

[245]*See, e.g.*, Daly v. Viacom, Inc., 238 F. Supp. 2d 1118 (N.D. Cal. 2002) (finding no expectation of privacy with respect to kissing in a bathroom stall because the couple also kissed on a street corner in plain sight); Wilkins v. Nat'l Broad. Co., Inc., 84 Cal. Rptr. 2d 329 (Cal. Ct. App. 1999) (holding that, because the plaintiff agreed to attend a meeting at a public restaurant, no invasion of privacy occurred when the plaintiff was secretly audio- and videotaped); Helen Nissenbaum, *Protecting Privacy in an Information Age: The Problems of Privacy in Public*, 17 Law & Phil. 559, 565 (1998) (offering a philosophical justification for "privacy in public" in the face of "the inconsistencies, discontinuities and fragmentation, and incompleteness in the framework of legal protections and in public and corporate policy").

[246]Florida Star v. B.J.F, 491 U.S. 524 (1989) (reversing an award of damages to a rape victim whose name was published in a newspaper because the name had been reported in a police report and was a matter of public significance).

[247]Melvin v. Reid, 112 Cal. App. 285, 290–91 (Cal. Ct. App. 1931) ("When the incidents of a life are so public as to be spread upon a public record they come within the knowledge and into the possession of the public and cease to be private."). Despite this proclamation, the California Court of Appeals held in this famous 1931 case that a reformed prostitute could sue for invasion of privacy when producers of a film revealed she was a former prostitute who had been tried for murder. The court relied on the fact that the woman had reformed her life and that the producers revealed other private information. *Id*. at 292–93; *see also* Hall v. Post, 372 N.E.2d 711 (N.C. 1988) (holding no recovery for injury caused by a newspaper's publication of family secrets, which included the abandonment of a child at a carnival and her illicit adoption).

[248]For more on dignity as a basis for workplace privacy, see generally Avner Levin, *Dignity in the Workplace: An Enquiry into the Conceptual Foundation of Workplace Privacy Protection Worldwide*, 11 ALSB J. Emp. & Lab. L. 63 (2009). For more detailed discussions of the differences between

larly developed rubrics for drawing the elusive line between the employer's rights and the employee's private life.[249]

For practical and free speech reasons, it would be futile to focus regulatory efforts on suppressing the online information itself. Any proposal to protect individuals from the unjust consequences of an employer's privacy intrusion should focus on imposing reciprocal duties on the employer. One publicly accepted model of limiting action on the basis of publicly available information is found in the prohibited grounds model of Title VII. Under Title VII, employers are prohibited from acting against individuals based on their sex, color, race, national origin, or religion.[250] Title VII does not seek to hush the information (e.g., the fact that an employee is of a certain race or religion) but rather to regulate the permissible actions that can legally result from the information's consideration.

A more aggressive proposal would limit employer action to situations in which online information reveals evidence of criminal conduct, conduct that implicates the employee's performance, or activity that financially harms the employer. In other words, information that merely reveals aspects of an employee's private life or off-duty conduct should not alone be grounds for adverse employment decisions. While this proposal finds its format in Title VII, its substance is also well established in Canadian law, which utilizes the previously discussed five-factor analysis for evaluating off-duty conduct.[251]

Limiting the basis of employment decisions strikes an even balance. On the one hand, we do not want to protect individuals who have been involved in nefarious affairs, and we believe that society benefits from

---

privacy laws and jurisprudence in the United States and the EU, see generally Nancy J. King et al., *Workplace Privacy and Discrimination Issues to Genetic Data: A Comparative Law Study of the European Union and the United States*, 43 Am. Bus. L.J. 79 (2006); Levin & Nicholson, *supra* note 70.

[249]*See* R. v. Cole, [2011] 105 O.R. 3d 253 (Can. Ont. C.A.), *available at* http://www.ontariocourts.on.ca/decisions/2011/2011ONCA0218.htm.

[250]42 U.S.C. § 2000e-2(a)(1) (2006). Similar protection exists in other countries. *See, e.g.*, Canadian Human Rights Act, R.S.C. 1985, c. H-6, § 3.

[251]*See supra* text accompanying note 171 (listing the factors as (1) whether a crime had been committed, (2) the harm to the employer's reputation or product, (3) the ability of the employee to continue to perform his or her duties satisfactorily, (4) the effect on other employees, and (5) whether the employer is able to continue managing and directing employees efficiently).

having more information. On the other hand, we do not want to unjustly harm individuals because online media have made their information accessible across contexts and boundaries.

Ultimately, the foregoing recommendations are a first step in developing legal and normative tools to simulate territorial privacy rights online. Our survey respondents confirmed that online participation should not translate, at least in their ethos, to unlimited publicity. How we, as a society, set limits on online information—as imagined by the Millennial respondents—will define the role of privacy in the future workplace.

Conclusion

In his dissent in *O'Connor v. Ortega*, Justice Blackmun argued that defining privacy by physical space is illusory, in that "the tidy distinctions . . . between the workplace and professional affairs, on the one hand, and personal possessions and private activities, on the other, do not exist in reality."[252] Indeed, this is especially the case whenever digital social fora meet the workplace—contexts collapse, intermingling relationships and information unrestricted by time and space. As with other historical breakdowns in public/private boundaries, the incursion of social media in the workplace calls for an evaluation of burgeoning societal expectations and an assessment of the compatibility of these expectations with existing law and business practices.

The Supreme Court has recently displayed reluctance in determining whether expectations of privacy can reasonably exist in modern communication technology, stating that, "[a]t the present, it is uncertain how workplace norms, and the law's treatment of them, will evolve."[253] To clarify this uncertainty, we have analyzed data regarding these emerging norms as reported by the incoming workforce. In light of the ubiquity of social media, employers and employees need guidance on how to view social media in the workplace context and how to shape appropriate policies on their use. Recent international debates and decisions have also provided instruction on privacy expectations in the workplace. The foreign decisions discussed highlight the need for courts and lawmakers to

---

[252]O'Connor v. Ortega, 480 U.S. 709, 739 (1987) (Blackmun, J., dissenting).

[253]City of Ontario v. Quon, 130 S. Ct. 2619, 2630 (2010).

grasp the normative realities of communication technology in making and enforcing laws. As the United States waits for workplace privacy norms to evolve, relevant international case law provides a potential normative point of reference. Such analysis also provides the necessary insight to lawmakers and judges, especially those who are not personally immersed in the technologies.

We have shown that Millennials crave to live out in the open, offering traditionally private information online. Despite this transparency, our findings suggest that Millennial respondents maintain an expectation of network privacy, or of audience segregation. Our survey respondents displayed strong reactions against being forced to share with unintended audiences and objected to being judged across contexts. In line with Goffman's observations, it appears that Millennials share the need of all healthy individuals to engage in performances bound in social establishments and directed at distinct audiences, in order to shape their identities. Although the rising workforce desires network privacy, technology, law, and prevailing business practice do not currently support that approach. Other jurisdictions have successfully begun regulating the intersection of social media and the workplace. By shedding light on the legal vacuum and defining burgeoning societal expectations, we hope that clarity can emerge and employee dignity and autonomy can be preserved.