OUTTEN & GOLDEN LLP

EMPLOYEE PRIVACY RIGHTS: LIMITATIONS TO MONITORING, SURVEILLANCE AND OTHER TECHNOLOGICAL SEARCHES IN THE PRIVATE WORKPLACE[1]

PLI Institute
June 23, 2011

Wendi S. Lazar and Lauren E. Schwartzreich*

Outten & Golden LLP
3 Park Avenue 29th Floor
New York, New York 10016
Telephone: (212) 245-1000
Facsimile: (212) 977-4005
www.outtengolden.com

[1] This paper is based on an earlier paper by the authors: Wendi Lazar, Lauren Schwartzreich & Seth Marnin, *Do Employees have Privacy Rights in the Digital Age?* Practicing Law Institute, Litigation and Administrative Practice Series Litigation, 828 PLI/Lit 217 (June 24, 2010).

* Wendi S. Lazar is a Partner at Outten & Golden, LLP where she co-heads the firm's Executive & Professionals Practice Group. Lauren E. Schwartzreich is an associate at Outten & Golden where she co-heads the firms Workplace Privacy, Technology and E-Discovery Practice Group. Carmel Mushin, a staff attorney at Outten and Golden also assisted in the research, editing and updating for this paper.

As cell phones, the Internet and social media[2] continue to define personal and professional communication, federal and state laws are redefining and, in many ways, broadening the concept of workplace privacy. For years, employers in the private sector paid little attention to concerns over workplace privacy, as few laws prevented employers from monitoring employees and employees had greater control over their personal communications. As technology developed however, employers quickly obtained resources to conduct sophisticated searches of employees' or prospective employees' backgrounds, to monitor employees in and outside the workplace and to track and access employees' Internet usage. Most recently, employers have begun to demand access to employees' personal communications through third party service providers, such as wireless cell phone providers and social networking sites.

Over the last decade, courts and legislatures have responded to these developments by applying existing laws in ways that protect employees' privacy rights and enacting new laws to provide a remedial effect. Nevertheless, private sector employees continue to face many challenges to their workplace privacy.

This paper addresses six important areas in which workplace privacy rights have developed over the last several years: (A) web-based background checks; (B) technology use policies; (C) access to employees' electronic communications without authorization; (D) employees' private communications with counsel; (E) unique state laws; and (F) international trends toward protecting privacy in electronic communications.

A. Limitations to Web-Based Background Checks

Existing law provides limited protections for employees and job applicants against improper web-based background checks by their prospective employer, current employer or their employer's agent. This section explores three areas of such protection: (1) Internet use monitoring (with or without authorization); (2) background checks by credit reporting agencies; and (3) prior arrest or conviction checks.

---

[2] Social media sites are "a popular distribution outlet for users looking to share their experiences and interests on the Web," which "host substantial amounts of user-contributed materials (e.g., photographs, videos, and textual content) for a wide variety of real-world events of different type and scale." Hila Becker, Mor Naaman, & Luis Gravano, *Learning Similarity Metrics for Event Identification in Social Media*, Proceedings of the third ACM international conference on Web search and data mining, WSDM '10, 291-300. This umbrella term encompasses social networking sites such as Facebook, LinkedIn and MySpace, and microblogging information networks, such as Twitter. *See* Lisa Thomas, Comment, *Social Networking in the Workplace: Are Private Employers Prepared to Comply with Discovery Requests for Posts and Tweets?*, 63 SMU L. Rev. 1373, 1379 (2010); What is Twitter and Why Does it Keep Following me Around?, http://www.tweeternet.com (last visited Mar. 6, 2011). Social networking sites are defined as "web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system. The nature and nomenclature of these connections may vary from site to site." D.M. Boyd & N. B. Ellison, *Social Network Sites: Definition, History, and Scholarship. Journal of Computer-Mediated Communication*, 13: 210–230 (2008) (The authors prefer the term social "network" site since in most cases these sites are geared toward existing networks, rather than creating new ones, as the term networking suggests; however, they note that these terms are used interchangeably. We will use the term social "networking" sites.).

1. Internet Use Monitoring

The Internet and social media tempt employers to investigate personal information about applicants or current employees. Human resource professionals turn increasingly to social media for background information on candidates. According to a 2009 survey by CareerBuilder.com, 45% of the 2,600 hiring personnel surveyed reported that they screen job applicants by viewing their social networking site profiles.[3] Thirty-five percent of these individuals reported that content found on social networking sites (SNS) caused them not to hire the candidate.[4] A 2010 survey by Jobvite.com, that included around 600 human resources and recruiting personnel, reveals that 80% of survey takers anticipate reviewing social media profiles in the future and 83% will actively recruit via social networking sites.[5] While this investigatory process may not be unlawful on its face, the manner in which an employer accesses an applicant's SNS content and the specific content that triggers an employer's adverse hiring decision may violate the Stored Communications Act (SCA)[6] and/or antidiscrimination laws.

Employers risk bad press and violating the SCA where they require applicants or employees to disclose their log-in and password information for their SNS accounts or other password-protected online accounts. Pursuant to the SCA, an employer may not obtain access to a stored communication (here SNS account messages) without authorization from the intended sender or recipient.[7] At least two public employers, the City of Bozeman, Montana and the Maryland Department of Corrections, were recently caught in public-relations debacles when they requested job applicants' social media affiliations and SNS log-in and password information. Both employers endured nationwide ridicule for engaging in what much of the public perceived to be inappropriate screening that violated common notions of privacy. The employers attempted to salvage their reputation by defending the policy to mass media, but in the end both acquiesced and ceased enforcement of the policy.[8]

---

[3] Forty –five Percent of Employers Use Social Networking Sites to Research Jobs Candidates, CareerBuilder Survey Finds, http://www.careerbuilder.com/share/aboutus/pressreleasesdetail.aspx?id=pr519&sd=8/19/2009&ed=12/31/2009&cbRecursionCnt=4&cbsid=ea1722cba741496eae69fc3ebc43b916-322351379-RD-4&ns_siteid=ns_us_g_survey_research_job_a_ (last visited Feb. 25, 2011).

[4] *Id.*

[5] *See* Jobvite Social Recruiting Survey 2010, http://recruiting.jobvite.com/resources/social-recruiting-survey.php (last visited Mar. 10, 2011) (The Jobvite Social Recruiting Survey 2010 was conducted online between May and June 2010; over 600 human resource and recruiting professionals participated in the survey. Respondents answered questions using an online survey tools and the response data is available only in aggregate form); *see also* Background Checking through Social Networks - Err on the Side of Caution, HireRight http://www.hireright.com/Blog/post/Background-Checks-Social-Media.aspx (citing Jobvite survey) (last visited Mar. 10, 2011).

[6] 18 U.S.C. §§ 2701-11.

[7] *See* 18 U.S.C. § 2702(b)(3) (private information can be released "with the lawful consent of the originator or an addressee or intended recipient of such communication . . . .").

[8] *See* Martha Neil, *Mont. Town Rescinds Rule Requiring Job Seekers to Reveal Social Web Passwords*, ABAJournal.com (Jun. 23, 2009), http://www.abajournal.com/news/article/mont._town_rescinds_rule_requiring_job_seekers_to_reveal_social_web_passwor/ (last visited Mar. 10, 2011); Molly McDonough, *Town Requires Job Seekers to Reveal Social Media Passwords*, ABAJournal.com (Jun. 19, 2009), http://www.abajournal.com/news/article/town_requires_job_seekers_to_reveal_social_media_passwords/ (last visited Mar. 10, 2011); Aaron C. Davis, *Md. Corrections Department Suspends Facebook Policy for Prospective Hires*, WASH. POST, Feb. 22, 2011, *available at* http://www.washingtonpost.com/wp-

Even so, enforcement of either the Bozeman or Maryland Department of Corrections policy may have constituted a violation of the SCA. Where an employer coerces an employee's consent to access stored communications, the employer may not have obtained valid authorization under the SCA. In such a situation, acquiescence does not constitute consent.[9] As the American Civil Liberties Union explained in its letter of admonition to the Maryland Department of Corrections, an employer's policy of requesting access to password protected SNS accounts would violate the SCA even if compliance by the employee or applicant were not mandatory "given the disparate bargaining power of the employer and employee or applicant."[10]

Finally, even where an employer accesses an applicant's online information from sources not covered by the SCA, the employer still may violate antidiscrimination laws. This generally arises in situations where an employer learns of a prospective employee's protected status, such as an applicant's race, religion or sexual orientation, and based on this information takes an adverse action, such as declining to interview the candidate. In such situations, the job applicant may have a valid discrimination claim against that employer under various federal and/or state laws.[11]

---

dyn/content/article/2011/02/22/AR2011022207486.html) (last visited Mar. 10, 2011); Helen A.S. Popkin, *Gov't Agency Suspends Facebook Password Demands*, msnbc.com (Feb. 24, 2011), http://technolog.msnbc.msn.com/_news/2011/02/24/6124269-govt-agency-suspends-facebook-password-demands (last visited Feb. 25, 2011).

[9] *See* Pietrylo v. Hillstone Rest. Group, No. 06-5754, 2009 WL 3128420 (D.N.J. Sept. 25, 2009). In *Pietrylo*, an employee complied with her managers' demand for her log-in information, explaining that she did so out of fear that her refusal to cooperate would affect her job negatively. The jury concluded that this was not valid authorization and the district court affirmed, finding that a reasonable jury could conclude that the employee was coerced and that she turned over her log-in information under pressure. The *Pietrylo* case is discussed in greater detail in section C.2., below.

[10] Letter from Deborah A. Jeon, Legal Director, American Civil Liberties Union, to Gary D. Maynard, Secretary of Maryland Department of Public Safety and Correctional Services (Jan. 25, 2011), *available at* http://www.aclu-md.org/aPress/Press2011/collinsletterfinal.pdf (last visited Feb. 25, 2011). The ACLU also argued that the practice was an invasion of privacy "and arguably chills employee speech and due process rights protected under the First and Fourteenth Amendments . . . ." *Id.*

[11] *See, e.g.*, Title VII of Civil Rights Act of 1964 ("Title VII"), *as amended*, 42 U.S.C. § 2000e *et seq.*; the Sexual Orientation Non-Discrimination Act ("SONDA"), NY CLS Exec § 296 (2005); California Fair Employment and Housing Act ("FEHA"), CAL. GOV'T CODE § 12940(d); Employment Non-Discrimination Act ("ENDA"), Bill No. S. 1584/H.R. 3017 (prohibiting discrimination in employment against individuals based on their sexual orientation or gender identity); the Genetic Information Nondiscrimination Act of 2008 ("GINA"), 42 U.S.C.A § 2000ff-1 (effective Nov. 21, 2010) (employers may not "request, require, or purchase genetic information with respect to an employee or a family member of the employee"). Additionally, certain anti-discrimination laws prohibit inquiries that are likely to elicit information about an employee's status within a protected class. *See e.g.*, Americans with Disabilities Act ("ADA") Amendments Act of 2008, 42 U.S.C. § 12101, *et seq.* (Section 12112(d)(4)(A) prohibits inquiries into employees' disabilities unless job-related and consistent with business necessity). Employers may not make inquiries that are "likely to elicit information about a disability." *Equal Employment Opportunity Commission, EEOC Enforcement Guidance on Disability-Related Inquiries and Medical Examinations of Employees Under the Americans with Disabilities Act* (July 27, 2000).

2. Background Checks and Credit Reports

Even where employers conduct lawful background checks, the subjects of the background check retain some disclosure protections under federal and state[12] law. Employees are increasingly aware of these protections and may pursue claims against their employers for violations of these laws.

The federal Fair Credit and Reporting Act ("FCRA"),[13] regulates employers' use of background reports, including those created by individuals or entities as well as those produced by for-profit credit reporting agencies ("CRAs"), such as Experian, Trans Union, and Equifax.[14] Background check reports fall into one of two categories under FCRA, "consumer reports" and "investigative consumer reports."[15] The type of report sought by an employer will affect the employer's obligations under FCRA.[16]

Under FCRA, regulated background check reports include those covering employment history, educational history, driving record, credit history, credit worthiness and criminal background. For example, under FCRA, CRAs may not include certain types of obsolete information in a report.[17] FCRA may also require report content to reflect whether information contained therein was obtained through SNS content.

Regardless of the type of report sought, however, an employer may not obtain a report unless it is for an "employment purpose," such as hiring, promotion, reassignment or retention; nor may an employer use the report for retaliatory purposes or hide the fact that it has requested

---

[12] New York and California have state laws concerning background checks. *See* N.Y. GEN. BUS. L. § 380-b(b) and c(d) (employer may request an "investigative consumer report" for an applicant, not a regular consumer report, as long as the applicant receives notices and upon request is provided the name and address of the consumer reporting agency that furnished the report); CAL. CIV. CODE § 1786 *et seq*. Additionally, most states have a cause of action for "public disclosure of private facts" or "false light." Improper reference and background checks may trigger liability under these causes of actions. *See*, Machleder v. Diaz, 801 F.2d 46, 52 (2d Cir. 1986), *cert. denied*, 479 U.S. 1088 (1987) (holding that false light invasion of privacy claims are governed by the law of the state in which plaintiff resided and in which defendant conducted and disseminated information that formed the subject of the lawsuit).

[13] 15 U.S.C. §§ 1681 *et seq*.

[14] Anyone or any entity that regularly engages in assembling or evaluating information about a consumer is considered to be a CRA, including outside investigators, auditors, and outside counsel. FCRA does not apply to information an employer obtains through means other than a CRA.

[15] "Consumer reports" cover any information that bears on an applicant or employee's "credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living." 15 U.S.C. § 1681a(d). "Investigative consumer reports" include information obtained by interviews with neighbors, friends, or associates of the applicant or employee. 15 U.S.C. § 1681a(e).

[16] Each report type imposes specific disclosure obligations on the employer. See Wendi Lazar, Lauren Schwartzreich & Seth Marnin, *Do Employees have Privacy Rights in the Digital Age?* Practicing Law Institute, Litigation and Administrative Practice Series Litigation, 828 PLI/Lit 217 (June 24, 2010), for a more in depth discussion of employers' obligations for each type of report.

[17] This includes, for example, bankruptcies predating a report by more than fourteen years; civil lawsuits and judgments entered more than seven years prior or until the statute of limitations has expired (whichever is longer), among other things. 15 U.S.C. § 1681c.

the report.[18] The employee or applicant must receive notice that a report has been requested[19] and give consent in writing before it is run.[20] If an employer intends to take an adverse action[21] based in whole or in part on the report, the employer must comply with FCRA's two-step disclosure obligation: (1) provide a copy of the report to the employee or applicant along with a description of the individual's rights under FCRA so that he or she has the chance to clarify or correct any inaccuracy;[22] and (2) provide notice of the adverse action, the contact information for the agency that provided the report and a description of the individual's rights under FCRA, including the right to obtain a free report and dispute its content.[23] An employer's failure to adhere to these requirements may result in liability for the employer.[24]

FCRA is not the only law providing credit check protections for employees. An increasing number of states are introducing measures to further limit employer use of this information.[25] While only four states have enacted such laws,[26] newly introduced measures in eight states[27] brings the number of states considering legislation to nineteen.[28] The measures vary from state to state and range from creating a private right of action for damages if the law is violated, to punishing violations as a misdemeanor and imposing fines of not less than $200 or more than $400 per violation.[29] The 112th Congress is also considering legislation that would amend FCRA to restrict employer use of consumer credit reports for the purposes of making adverse employment decisions.[30]

---

[18] An employer may violate FCRA if it obtains a report for a reason other than one of the "permissible purposes" specified by the statute. *See*, Russell v. Shelter Financial Services, 604 F. Supp. 201, 203 (W.D. Mo. 1984) (employer improperly requested report summarizing employee's credit history after employee had resigned).

[19] The disclosures should provide the applicant or employee information about the agency providing the report and the individual's rights under FCRA. 15 U.S.C. §§ 1681b(b)2, 1681d(a).

[20] An adverse action taken against an employee for refusing to consent to the release of a report is not actionable under FCRA. Kelchner v. Sycamore Manor Health Ctr., 135 Fed. Appx. 499 (3d Cir. 2005).

[21] An adverse action is defined as "a denial of employment or any other decision for employment purposes that adversely affects any current or prospective employee." 15 U.S.C. § 1681a(k)(1)(B)(ii).

[22] 15 U.S.C. § 1681b(b)(3)(A).

[23] 15 U.S.C. § 1681b(b)(3)(B). The employer must also provide notice that the CRA did not make the decision and cannot provide specific reasons why the employer took the adverse action. 15 U.S.C. § 1681m(a)(2)(B).

[24] *See*, *e.g.*, Woodell v. United Way, 357 F. Supp. 2d 761 (S.D.N.Y. 2005).

[25] Employment Discrimination Report, *Five More States Seek Limits on Credit Checks*, BNA, 36 EDR 217 (Feb. 23, 2011).

[26] Hawaii, Illinois, Oregon, and Washington have enacted legislation limiting employer use of credit report information for employment purposes. *Id.*

[27] Colorado, Florida, Georgia, Michigan, Montana, Maryland, Ohio, and Pennsylvania are now considering similar measures. *Id.*; Joseph Lazzarotti, *Florida, Michigan, and Montana Follow National Trend and Consider Banning the Use of Applicant Credit History Background Checks in Hiring Decisions*, Workplace Privacy Data Management & Security Report, March 14, 2011, *available at* http://www.workplaceprivacyreport.com/2011/03/articles/background-checks/florida-michigan-and-montana-follow-national-trend-and-consider-banning-the-use-of-applicant-credit-history-background-checks-in-hiring-decisions/ (last visited Mar. 15, 2011).

[28] In addition to the five states above, the eleven states also considering measures to limit employer use of credit report information for employment purposes are California, Connecticut, Indiana, Kentucky, Missouri, Nebraska, New Jersey, New Mexico, New York, Texas, and Vermont. *Id.*

[29] *Id.*

[30] *Id. See* "Cohen Introduces Bill to Prevent Employers From Using Credit Checks to Hire or Fire Employees." State News Service (Jan. 20, 2011), HighBeam Research, http://www.highbeam.com/doc/1G1-247063148.html (last visited Feb. 25, 2011).

3. Prior Arrests and Convictions

Federal and state laws impose specific restrictions on employers' use of prior criminal records to screen applicants. FCRA prohibits employers from obtaining a report that reflects arrest, indictment or conviction records that precede the report by more than seven years for an employee or prospective employee whose annual salary is or is reasonably expected to be less than $75,000 a year.[31] In some states, employers are also prohibited from inquiring into arrests that do not lead to convictions altogether.[32] Employers may also invite Title VII liability if they base adverse employment decisions on an applicant or employee's prior arrest or conviction record, as such a policy may adversely impact a protected group of employees.[33]

Under the federal standard, an employer who considers arrest records in making adverse employment decisions may only consider the *conduct* underlying the charge, rather than the arrest or conviction *per se*.[34] If there is no relationship between the charges and the position sought, or if there is a likelihood that the applicant did not commit the alleged conduct, an employer may face liability for an adverse employment decision based on the charges. A blanket exclusion of individuals with arrest records will almost never withstand scrutiny.[35] Although using criminal convictions as a *per se* bar to employment may be unlawful,[36] a *per se* bar on convictions with a demonstrable job nexus may be valid in circumstances involving a recent conviction, a repeated history of convictions or where evidence suggests rehabilitation has not occurred.[37]

---

[31] 15 U.S.C. §§ 1681c(a)(2), c(a)(5), c(b)(3). *See also* Serrano v. Sterling Testing Sys., 557 F. Supp. 2d 688 (E.D. Pa 2008).

[32] *See, e.g.*, N.Y. EXEC. L. § 296(16) (employers may not inquire into "any arrest or criminal accusation . . . not then pending against that individual which was followed by a termination of that criminal action or proceeding in favor of such individual"); CAL. LAB. CODE § 432.7(a) (employers may not ask for "information concerning an arrest or detention that did not result in conviction, or information concerning a…pre-trial or post-trial diversion program").

[33] *See, e.g.*, Gregory v. Litton Sys., Inc., 316 F. Supp. 401, 403 (D.C. Cal. 1970) *modified on other grounds*, 472 F.2d 631 (9th Cir. 1973) (The policy of Defendant under which Plaintiff was denied employment, i.e., the policy of excluding from employment persons who have suffered a number of arrests without any convictions, is unlawful under Title VII. It is unlawful because it has the foreseeable effect of denying black applicants an equal opportunity for employment.).

[34] Some state laws impose broader restrictions barring adverse employment decisions based on an employee or applicant's criminal record that might otherwise survive scrutiny under federal law. *See* NY CLS Correc. § 752 (prohibits adverse employment decisions based on a person's criminal conviction record unless employer can show a direct relationship between the record "and the specific license or employment sought or held by the individual" or that the position "would involve an unreasonable risk to property or to the safety or welfare of specific individuals or the general public"). *See also*, Lazar, et. al., *supra* at 5.

[35] *See, e.g.*, Gregory, 316 F. Supp. 401; Carter v. Gallagher, 452 F.2d 315 (8th Cir. 1971), *cert. denied*, 406 U.S. 950 (1972); Reynolds v. Sheet Metal Workers Local 102, 498 F. Supp. 952 (D.C. Cir. 1980); Dozier v. Chupka, 395 F. Supp. 836 (S.D. Ohio 1975); U.S. v. City of Chicago, 411 F. Supp. 218 (N.D. Ill. 1976), *aff'd. in rel. part*, 549 F.2d 415 (7th Cir. 1977); City of Cairo v. Illinois Fair Employment Practice Comm'n, 315 N.E.2d 344 (Ill. App. Ct. 1974).

[36] *See, e.g.*, Green v. Missouri Pac. R.R., 523 F.2d 1290 (8th Cir. 1975).

[37] *See, e.g.*, EEOC v. Carolina Freight Carriers Corp., 723 F. Supp. 734, 752 (S.D. Fla. 1989).

B. Workplace Technology Policies

Once hired, private sector employees may have privacy protections concerning their work computers, laptops, cellular phones and other electronic devices, even where an employer maintains a policy stating otherwise. Historically, courts have recognized employees' reasonable expectations of privacy in their use of employer equipment. For example, in 2001, the Second Circuit determined that an employee had a reasonable expectation of privacy in the content of his work computer, notwithstanding the employer's technology policy prohibiting usage of its equipment for personal matters.[38] In *Levanthal v. Knapek*,[39] the court found, among other things, that the employer failed to institute a clear policy or practice concerning regular monitoring of computers. In this context, the court concluded that the employee maintained an expectation of privacy in his computer, where he occupied a private office with a door and had exclusive use of the computer. Of course, this view on expectations of privacy in the workplace has not been widely adopted among U.S. courts.[40] However, it has pressed some courts to reexamine monitoring policies when deciding these cases.

Consistent with the Supreme Court's recent decision in *City of Ontario v. Quon*, courts should consider whether an employer's privacy policy is clear and clearly communicated, with an eye to the operational realities of the workplace.[41] Although the *Quon* Court did not rule on the issue since it concluded that the employer's search was reasonable under the Fourth

---

[38] Leventhal v. Knapek, 266 F.3d 64, 74 (2d Cir. 2001). *See also*, Curto v. Med. World Commc'ns, Inc., No. 03 Civ. 6327 (DRH)(MLO), 2006 WL 1318387, at *9 (E.D.N.Y. May 15, 2006) (employee who worked mostly from home had a reasonable expectation of privacy in her work laptop regarding attorney-client communications and attorney work product).

[39] *Id.*

[40] *Compare* U.S. v. Slanina, 283 F.3d 670, 676-77 (5th Cir. 2002) (reasonable expectation of privacy in employee's computer and files where he took precautions to limit access and the employer did not disseminate any policy preventing the storage of personal information and did not inform its employees that their computer use might be monitored), *vacated on other grounds*, 537 U.S. 802 (2002); Haynes v. Office of the Attorney Gen., 298 F.Supp.2d 1154, 1161-62 (D. Kan. 2003) (reasonable expectation of privacy in private computer files, despite computer screen warning of no expectation of privacy where employer's practice permitted personal use and no evidence was offered to show that the employer ever monitored private files or employee e-mails) *with* U.S. v. Simons, 206 F.3d 392, 398 & n. 8 (4th Cir. 2000) (no reasonable expectation of privacy in office computer and downloaded Internet files where employer had a policy of auditing employee's use of the Internet, and the employee did not assert that he was unaware of or had not consented to the policy); Muick v. Glenayre Elec., 280 F.3d 741, 743 (7th Cir. 2002) (no reasonable expectation of privacy in workplace computer files where employer had announced that he could inspect the computer); Thygeson v. U.S. Bancorp, No. CV-03-467-ST, 2004 WL 2066746, at *20 (D. Or. Sept. 15, 2004) (no reasonable expectation of privacy in computer files and e-mail where employee handbook explicitly warned of 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) (no reasonable expectation of privacy in workplace e-mail where employer's guidelines "explicitly informed employees that there was no such expectation of privacy"); Garrity v. John Hancock Mutual Life Ins. Co., No. Civ. A. 00-12143-RWZ, 2002 WL 974676, at *1-2 (D. Mass. May 7, 2002) (no reasonable expectation of privacy where, despite the employee created password to limit access, the company periodically reminded employees that its e-mail policy prohibited certain uses and the e-mail system belonged to the company).

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

Amendment,[42] its discussion of employee expectations of privacy in the workplace is instructive for lower courts considering expectations of privacy in the private sector.

As the Court explained, written policies and context matter when analyzing privacy issues. Addressing the issue of Quon's reasonable expectation of privacy in his text message communications, the Court stated that "employer policies concerning [monitoring of electronic] communications will . . . shape the reasonable expectations of their employees, especially to the extent that such policies are clearly communicated."[43] From this statement we may discern that as part of an analysis into whether policies are "clearly communicated," a court should consider the operational realities of the workplace. Looking at Quon's circumstances, the Court stressed that "it would be necessary to ask whether [Quon's supervisor's] statements" contradicting the policy "could be taken as announcing a change in [the employer's] policy, and if so, whether [the supervisor] had, in fact or appearance, the authority to make such a change . . . ."[44] Applying this analysis to the private sector, courts looking at privacy policies will likely assess whether the policy is written and communicated clearly, with appropriate notice to employees.

In addition to the clarity of the privacy policy and operational realities of a workplace, courts should also consider the scope of privacy policies, the type of electronic media use covered by the policy, the substance of communications covered by the policy, whether the employer actually enforces its policy and whether the employer applies its policy consistently. Below are several circumstances in which employers' privacy policies (also referred to as technology policies) or employers' enforcement of such policies has been found to be unenforceable or in violation of existing law.

1. Overbroad Technology Policies

Overly broad technology policies may, even without enforcement, violate federal law. Where a technology policy infringes on employees' rights under the National Labor Relations Act ("NLRA"), that policy may constitute an unlawful labor practice. For example, in late 2010, the National Labor Relations Board ("NLRB") filed a complaint against an employer for firing an employee who had been accused of violating a company's technology policy. The policy barred employees from depicting the company "in any way" on Facebook or other social media sites in which they post pictures of themselves.[45] The NLRB's complaint alleged, among other things, that the employer violated the NLRA by (1) terminating the employee after she engaged

---

[42] In *Quon*, the employer maintained a policy stating that employees should expect no privacy in their communications via the City's various technology devices. Quon's supervisor permitted Quon and other employees to use cellular pagers for personal use and represented that their communications via these pagers would not be audited unless they went over the monthly user allowance and failed to pay the difference. The employer subsequently obtained copies of Quon's text messages even though Quon had paid the overage fees for each time he had exceeded his monthly user allowance. *Id*. at 2625-27.

[43] *Id.* at 2630.

[44] *Id*. at 2629. In *Quon*, the Court refrained from applying the operational realities standard to the facts of the case. *Id*. at 2629-30. The Court justified its decision to refrain from doing so by citing the ever-changing nature of what society perceives to be a reasonable expectation of privacy and explaining that the Court did not want to issue a "broad holding concerning employees' privacy expectations vis-à-vis employer-provided technological equipment [because it] might have implications for future cases that cannot be predicted." *Id*. Instead, the Court assumed Quon had a reasonable expectation of privacy so that the Court could proceed to the next step in its analysis. *See id*.

[45] NLRB v. Am. Med. Response of Connecticut, Case No. 34-CA-12576, *complaint filed* Oct. 27, 2010, *available at* http://www.scribd.com/doc/41010696/American-Medical-Response-of-CT-NLRB-Nov-2010.

in concerted activities with her coworkers by criticizing her supervisor on Facebook and (2) instituting an overly broad Internet policy that interfered with employees' rights to discuss the terms and conditions of their employment.[46]

The case settled in February 2011. Although the employer made several concessions (the entire scope of the settlement is unknown), there is no formal NLRB decision on this matter. According to a formal statement by the NLRB, the company agreed to narrow its Internet policies "to ensure that they do not improperly restrict employees from discussing their wages, hours and working conditions with co-workers and others while not at work" and promised that it "would not discipline or discharge employees for engaging in such discussions."[47] This outcome confirms two important points: (1) overreaching technology policies may, on their face, violate existing law; and (2) employees may retain expectations of privacy in their SNS postings. It is also worth noting that because non-union workplaces must comply with the NLRA's rules concerning protected concerted activity, *all* employees, regardless of union status, should retain these protections.[48]

2. Selective Enforcement of Technology Policies

Employees may retain their reasonable expectation of privacy where their employers selectively enforce privacy policies. If an employer's policy provides for monitoring of employees' computer files and Internet usage, and the employer fails to enforce the policy regularly, its employees may retain a reasonable expectation of privacy. For example, in *Brown-Criscuolo v. Wolfe*, a school superintendant accessed a school principal's personal emails while the principal was out on medical leave,[49] ostensibly to gather information regarding the principal's medical condition.[50] After learning of the superintendant's conduct and finding that a personal email had been forwarded to the superintendant's email account,[51] the principal filed a claim alleging violation of her privacy rights.[52] On a motion for summary judgment, the superintendant argued that since the principal was aware of the school district's monitoring policy, which permitted "routine maintenance and monitoring" of its computer system, she could

---

[46] *Id*. at 3, ¶¶ 8-17. Under the National Labor Relations Act, employers are prohibited from interfering with, restraining or coercing employees in their rights under Section 7. *See* NLRA Section 8(a), 29 U.S.C. §§ 151-169. These rights include freedom of association, mutual aid or protection, self-organization, to form, join, or assist labor organizations, to bargain collectively for wages and working conditions through representatives of their own choosing, and to engage in other protected concerted activities with or without a union. *Id*. at Section 7.

[47] NLRB, *Settlement Reached in Case Involving Discharge for Facebook Comments*, NLRB News Releases (February 08, 2011),http://www.nlrb.gov/news/settlement-reached-case-involving-discharge-facebook-comments (last visited Mar. 11, 2011).

[48] Section 7 of the NLRA protects employees in non-unionized workplaces. *See* NLRB v. Washington Aluminum Co., 370 U.S. 9, 14 (1962) (seven unorganized employees who engaged in walk-out were protected by Section 7 of NLRA).

[49] The emails were created and sent from her employer-provided email account (which she password protected). Brown-Criscuolo v. Wolfe, 601 F. Supp. 2d 441, 449 (D. Conn. 2009).

[50] *Id*. at 450.

[51] The email forwarded to the supervisor was between the employee and her attorney, and described issues she was having with her supervisor. A fact issue remained regarding who actually forwarded the email, since the supervisor denied doing so. *Id*. at 451.

[52] In her initial complaint, the employee alleged violations of the SCA, the Wiretap Act, the Rehabilitation Act, the Equal Protection Clause of the Fourteenth Amendment, the Fourth Amendment and the First Amendment. However, she later withdrew all claims other than the Fourth and First Amendment violations. *Id*. at 448.

not have had a reasonable expectation of privacy in her work email account.[53] The court found that the superintendant failed to establish that the school district had a practice of routinely monitoring work email accounts or that it was the superintendant's duty to conduct such monitoring. The superintendant also failed to prove that the principal's email account was accessed pursuant to the superintendant's own routine computer system monitoring.[54] For these and other reasons, the court concluded that the principal had a reasonable expectation of privacy in her work email account and denied the defendant summary judgment on this issue.[55]

Although *Brown-Criscuolo* involves public sector employment, the decision reaffirms how inconsistent enforcement of technology policies may validate, rather than negate, an employee's reasonable expectation of privacy. Similarly, inconsistent *enforcement* can preserve privacy expectations even where an employer consistently *reminds* its employees of the policy.[56]

3. Discriminatory Enforcement of Technology Policies

Employees may be protected from employer enforcement of privacy policies where the employer applies its policy in a discriminatory manner. An employer is not free to enforce a legitimate technology policy selectively against an employee for exercising her statutorily protected rights, such as engaging in union organizing activities or because of her protected status.[57] Enforcement of a privacy policy in a discriminatory manner may constitute an unlawful discriminatory action.

4. Retaliatory Technology Monitoring

Employees may also be protected where employers monitor their employees' technology use in retaliation for the employees' engagement in protected activity. For example, if an employer monitors an employee's telephone calls in response to her complaint of discrimination, the employer may have engaged in unlawful retaliation. In *Dotson v. City of Syracuse*,[58] the plaintiff alleged that after she made her initial complaint of sexual harassment her employer began eavesdropping on her telephone conversations. The court found that a reasonable fact

---

53 *Id*. The policy stated that "[s]ystem users have a limited privacy expectation in the contents of their personal files on the District system."

54 *Id*.

55 *Id*. The court denied the defendant's motion for summary judgment with regard to the Fourth Amendment claim; a reasonable jury could conclude the defendant's conduct was "excessively intrusive." *Id*. at 451.

56 *See* Haynes v. Office of the Attorney Gen., 298 F.Supp.2d 1154, 1161-62 (D. Kan. 2003) (reasonable expectation of privacy in private computer files, despite computer screen warning of no expectation of privacy where employees were allowed to use computers for private communications and password protect access, were advised that unauthorized access to user's e-mail was prohibited, and no evidence was offered to show that the employer ever monitored private files or employee e-mails).

57 *See* Guard Publ'g Co. v. NLRB, 571 F.3d 53, 60 (D.C. Cir. July 7, 2009) (employer discriminated against employee in violation of the National Labor Relations Act where "in practice the only employee emails that had ever led to discipline were the union-related emails at issue here"); Gorzynski v. JetBlue Airways Corp., 596 F.3d 93, 2010 U.S. App. LEXIS 3424 (2d Cir. Feb. 19, 2010) (alleging discriminatory enforcement of technology policy based on age); *cf.* Hirschberg v. Bank of Am., N.A., No. 08 Civ. 1611, 2010 WL 4872992 (E.D.N.Y. Dec. 1, 2010) (noting that an employer's adverse employment action based on an alleged violation of a vague or non-existent policy might be relevant to prove pretext in an age discrimination case).

58 No. 5:04-CV-1388, 2009 U.S. Dist. LEXIS 62174 (N.D.N.Y. July 21, 2009).

finder could conclude that "the requisition and monitoring of plaintiff's telephone conversations was intrusive and could have dissuaded plaintiff from filing a claim."[59] Since the eavesdropping occurred in temporal proximity to the complaints, among other reasons, the court denied the employer's motion for summary judgment and dismissal of the plaintiff's Title VII retaliation claim.

An employer that monitors an employee's Internet usage in response to a complaint of discrimination may invite liability, regardless of whether the employee knows at the time that he or she is being monitored. In *Zakrzewska v. The New School*,[60] an employee sought leave to amend her discrimination complaint to add a claim of retaliation where her employer monitored her Internet usage after she complained of discrimination. The employer argued that the monitoring could not constitute an adverse employment action because the employee was unaware of the monitoring at the time it occurred. The court, however, disagreed. Refusing to "foreclose the possibility that a trier of fact reasonably could find that defendants' alleged covert monitoring…'well might have dissuaded a reasonable worker from making or supporting a charge of discrimination,'" the court granted the employee's motion.[61]

C. Accessing Employees' Personal Data and Communications without Permission

Even a clear, consistently enforced and equally applied technology policy does not give an employer unfettered access to all of its employees' personal electronic communications, such as text messages, personal online email accounts, restricted-access SNS content or password-protected blogs. Employers, like the rest of us, are subject to federal statutes providing both criminal and civil penalties for unauthorized access to electronic communications and data, such as the Electronic Communications Privacy Act[62] and two of its subsections: the Stored Communications Act ("SCA"),[63] and the Wiretap Act.[64] To summarize each, the SCA prohibits individuals from accessing, without authorization, stored electronic communications, and the Wiretap Act prohibits individuals from accessing, without authorization, electronic communications while they are in transit. Employers may pay heavily for assuming that their technology policies shield them from these laws.[65]

---

59 *Id*. at *57.

60 543 F. Supp. 2d 185 (S.D.N.Y. 2008).

61 *Id*. at 187 (quoting Burlington N. & Santa Fe Ry. v. White, 548 U.S. 53, 68 (2006)).

62 18 U.S.C. § 2510, *et seq*.

63 18 U.S.C. § 2701, *et seq*. The SCA provides criminal and civil penalties for intentional unauthorized access of stored electronic communications.

64 18 U.S.C. § 2510, *et seq*.

65 For violations of the SCA, employees may obtain an award of actual damages and, even without proof of actual damages, statutory damages, attorneys' fees and costs, and punitive damages where the violation was intentional. *See* Pure Power Boot Camp, Inc. v. Warrior Fitness Boot Camp, LLC, No. 08 Civ. 4810 (THK), 2010 WL 5222128, at *8-9 (S.D.N.Y. Dec. 22, 2010) (defendant-employees were estopped from claiming actual damages after claiming only statutory damages, but were entitled to statutory damages of $1,000 per SCA violation whether or not they suffered actual damages; the court refused to award costs and attorney's fees and punitive damages at the summary judgment stage); Pietrylo v. Hillstone Rest. Group, No. 06-5754 (FSH), 2009 WL 3128420 (D.N.J. Sept. 25, 2009) (district court upheld jury's award of back pay and punitive damages based on the jury's finding that defendants' SCA violations were malicious). *But see* Van Alstyne v. Elec. Scriptorium Ltd., 560 F.3d 199 (4th Cir. 2009) (awarding punitive damages and attorney's fees absent proof of actual damages, but stating that statutory damages under the SCA are only recoverable where a plaintiff has also suffered actual damages).

1. Personal Online Email Accounts

Employers who intentionally access employees' personal email accounts without their permission risk liability under the SCA even if the employer's technology policy aims to elicit blanket authorization. In *Pure Power Boot Camp, Inc. v. Warrior Fitness Boot Camp, LLC*,[66] an employer's computer use policy aimed to do just that. The policy stated that employees had no right of personal privacy in any matter stored in or created on the company's system, including "the use of personal e-mail accounts on Company equipment."[67] It also stated that computer usage was subject to monitoring without additional notice.[68] Following an employee's separation from employment, the employer accessed the employee's personal online Hotmail account and other personal email accounts by using the username and password saved on the employer's computer. On the employee's motion to preclude the use or disclosure of the emails and seeking their immediate return and payment of attorneys' fees and costs, the employer argued that the employee had waived all privacy in his online Hotmail account because he had received the employer's technology policy. The court rejected this argument; the employer's request for enforcement of its computer use policy, the court explained, was not supported by the actual policy, which applied solely to the company's equipment and not to emails on systems maintained by outside entities.[69]

An employee's subjective belief may be the most important consideration for whether authorization has occurred, not whether the employer's policy was clear. In *Pure Power*, the court seemed to follow this line of reasoning and concluded that the employee's "subjective belief that his personal e-mail accounts, stored on third-party computer systems, protected (albeit ineffectively) by passwords, would be private" was reasonable.[70] The court explained: "If [an employee] had left a key to his house on the front desk at [his workplace], one could not reasonably argue that he was giving consent to whoever found the key, to use it to enter his house and rummage through his belongings . . ."[71] As such, the court held that the employer's access was unauthorized and clearly violated the SCA. In a later decision, the court granted the employee's summary judgment motion in part, maintaining that the employee's rights under the SCA were violated and awarding statutory damages (even without proof of actual damages). However, the court held that a dispute of fact remained as to whether the employer and/or others who accessed the employee's emails were personally liable for the violations.[72]

---

66 587 F. Supp.2d 548 (S.D.N.Y. 2008).

67 *Id*. at 552.

68 *Id*. at 552-3.

69 The court found that the employer's e-mail policy was "by its own terms, limited to 'Company equipment.'" *Id*. at 559. The policy stated, in relevant part: "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* … [including] the use of personal e-mail accounts *on Company equipment. The Company*, in its discretion *as owner of the E-Mail system*, reserves the right to review, monitor…and delete any matter stored in, created on, received from, or sent through *the system* …, without the permission of any system user, and without notice." *Id*. at 552-3 (emphasis added).

70 *Id*. at 561.

71 *Id*.

72 Pure Power Boot Camp, Inc. v. Warrior Fitness Boot Camp, LLC, No. 08 Civ. 4810 (THK), 2010 WL 5222128, at *5 (S.D.N.Y. Dec. 22, 2010).

2. Password-Protected or Invitation-Only Websites

Similarly, employers risk violating the SCA if they access otherwise restricted websites, such as social networking sites and password-protected chat groups. In *Pietrylo v. Hillstone Restaurant Group*,[73] a district court upheld a jury verdict and punitive damages against an employer that violated the SCA where it accessed a group of employees' password-protected and invite-only online forum maintained by a group of employees without permission. The restricted-access discussion forum, located on MySpace, was created so the plaintiff employees and other invited employees could air grievances concerning their employment. A participant in the discussion provided her password to a manager,[74] who subsequently accessed the forum, reviewed the content and fired the employees who had created it. The district court concluded that a reasonable jury could find that the managers knew their access was unauthorized, and that the employee who provided access to the MySpace forum was coerced into doing so.[75]

Employers seeking to search through employees' password-protected SNS content also risk violating the SCA where they subpoena third-party SNS sites, regardless of whether this is done within or outside the context of pending litigation. Individuals generally have standing to challenge subpoenas for their SNS content.[76] As explained in *Crispin v. Christian Audigier Inc.*,[77] "an individual has a personal right in information in his or her profile and inbox on a social networking site and his or her webmail inbox" sufficient to confer standing to move to quash subpoenas of social networking sites."[78] Even within the context of ongoing discovery, courts will generally quash employers' subpoenas to employees' social networking site providers because compliance with such an order would violate the SCA. In *Crispin*, for example, the court found that an employee's private messages sent through MySpace and Facebook were "inherently private" and protected under the SCA.[79] The court also determined that wall postings and comments on these social networks fell under the SCA, to the extent these

---

[73] No. 06-5754 (FSH), 2009 WL 3128420 (D. N.J. 2009). *See* discussion *supra* Part II.B.2..

[74] The parties disputed whether this employee was coerced into turning over her password to her managers.

[75] The employee that provided her password and log-in information to the managers testified that she felt she had to comply with her managers' request for the information or risk adversely affecting her job.

[76] A litigant seeking to obtain another party's private online communications may be able to avoid application of the SCA altogether by simply serving a Rule 34 document request directly on the party whose communications are sought. Mark S. Sidoti, Philip J. Duffy & Paul E. Asfendis, *How Private is Facebook Under the SCA? Courts Struggle with Social Networking Access Questions Under the Stored Communications Act*, 8 NO. 11 INTERNET L. & STRATEGY 1 (November 2010).

[77] 717 F. Supp. 2d 965 (C.D. Cal. 2010).

[78] *Id.*; *see also* Mancuso v. Florida Metro. Univ., Inc., No. 09 Civ. 61984-CIV, 2011 WL 310726 (S.D. Fla. Jan. 28, 2011) (quoting *Crispin*, holding an employee has standing to move to quash a subpoena seeking information from social networking sites).

[79] *Id.* at 991. *See also* In re Subpoena Duces Tecum to AOL, LLC, 550 F. Supp. 2d 606 (E.D. Va. 2008) (affirming ruling quashing subpoena to America Online seeking e-mails and other information relating to the accounts of non-party witnesses, stating "the statutory language of the [SCA] does not include an exception for the disclosure of electronic communications pursuant to civil discovery subpoenas"); *compare* Janice Chasten v. Franklin, No. C10-80205 MISC JW (HRL) 2010 WL 4065606 (N.D. Cal. Oct. 14, 2010) (in the criminal law context, holding subpoena to produce all of defendant's Yahoo emails would be "an invasion . . . of the specific interests that the [SCA] seeks to protect").

communications were not publicly available (meaning that the employee's SNS privacy settings prevented the general public from accessing the communications).[80]

While employees may be under the impression that SNS content is personal and private, employers may be able to obtain this information in the course of litigation directly from their employees. Employees' SNS content is generally protected from surreptitious collection by employers outside of the litigation context, but once litigation commences, the discovery process allows employers to obtain relevant personal information, such as diaries, calendars, and SNS content.[81] Where an employer makes a discovery request seeking production of relevant SNS content from an employee, the employee generally must comply, unless the requested information is not reasonably accessible.[82] Where employees do not produce requested relevant SNS content in response to discovery requests, employers may seek compliance through a court order.

For the most part, courts apply general discovery principles to requests seeking disclosure of employees' SNS content. Where there is evidence indicating that SNS content would be relevant to existing claims or defenses and the employee failed to produce the relevant content, a court is likely to order production of the SNS content. Most courts will not simply grant an employer's request to explore an employee's SNS content without some indication that such content exists, is relevant and has been withheld. For example, where an employer requests SNS content related to an employee's emotions, feelings or mental state; such content is actually relevant to the claims or defenses at issue; no such content has been produced, and there is evidence that such content exists; a court is likely to order the employee to turn over her SNS content.[83] Likewise, an employee's private messages exchanged with third parties regarding her sexual harassment allegations may be discoverable, while sexually explicit emails that do not

---

[80] *Id.* The court remanded its ruling for a determination of whether the wall posting and comments were publicly available as a result of the employee's privacy settings.

[81] *See* EEOC v. Simply Storage Mgmt., 270 F.R.D. 430, at 434 (S.D. Ind. 2010) (discovery of social networking sites "requires the application of basic discovery principles in a novel context," and the challenge is to "define appropriately broad limits . . . on the discoverability of social communications.").

[82] *See* Fed. R. Civ. P. 26 (b)(2)(B) ("A party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost.").

[83] *See* Simply Storage Mgmt., 270 F.R.D. at 435 (in a sexual harassment suit where plaintiff's emotional condition was at issue, the court ordered production of the SNS material defendants requested to the extent that it regarded any emotion, feeling or mental state). Some courts have eschewed relevancy considerations and authorized blanket production of entire SNS accounts where there was a clear indication that relevant and responsive evidence had been improperly withheld. See Bass v. Miss Porter's School, No. 3:08-cv-1807, 2009 WL 3724968 (D. Conn. Oct. 27, 2009) (ordering production of plaintiff's entire Facebook profile after an *in camera* review of withheld Facebook printouts which were "clearly relevant" communications, and finding that plaintiff's initial court-ordered production offered "no guidance as to the grounds or basis" used to determine which documents to produce); Ledbetter v. Wal-Mart Stores, Inc., No. 06-cv-01958-WYD-MJW, 2009 WL 1067018 (D. Colo. Apr. 21, 2009) (denying personal injury plaintiffs' motion for protective order against subpoena of their SNS content where plaintiffs' waived privilege to communications contained therein and where the information sought was reasonably calculated to lead to the discovery of admissible evidence); *but see* Romano v. Steelcase, Inc., 907 N.Y.S.2d 650 (N.Y. Sup. Ct. 2010) (ordering authorization for all SNS content after plaintiff resisted questions regarding private SNS content in her deposition and where plaintiff's public SNS profile page contained relevant information such that it was likely the rest of her SNS site would contain additional relevant evidence).

relate to her employment likely will not be discoverable.[84] Because general rules of discovery still apply, an employer should not be granted blanket access to *all* SNS content, as most SNS content will not be relevant to the pending claims and defenses. The better approach allows discovery of relevant SNS content and rejects requests for unjustified fishing expeditions into employees' SNS content.[85]

3. Text Message Content

Employers that own their employees' cell phones, pay the bills and are parties to the cellular service contracts may still violate the SCA where they access employees' personal text messages via the wireless provider. Wireless providers also risk violating the SCA where they disclose employees' text message content to employers.[86] Employers who nevertheless demand production of such text messages from wireless providers may also be liable under the SCA.[87]

4. Electronic Communications

The federal Wiretap Act prohibits unauthorized interception of transmitted electronic communications.[88] Employers that monitor employees' telephone calls may incur liability under the federal Wiretap Act.[89] Similarly, employers who use spyware on their employees' computers

---

[84] *See* Mackelprang v. Fidelity Nat'l Title Agency of Nev., Inc., No. 2:06-cv-0078-JCM-GWF, 2007 WL 119149, at *3 (D. Nev. Jan. 9, 2007) (in a sexual harassment suit, the court denied defendant's motion to compel all information on plaintiff's MySpace account, but invited a more tailored request for MySpace "private messages that contain information regarding [employee's] sexual harassment allegations… or which discuss her alleged emotional distress…").

[85] *See* McCann v. Harleysville Ins. Co. of N.Y., 910 N.Y.S.2d 614 (4th Dep't 2010) (in personal injury case, affirming denial of defendant's motion to compel SNS account authorization, where defendant "failed to establish a factual predicate with respect to the relevancy of the evidence" and essentially sought permission to conduct "a fishing expedition into plaintiff's Facebook account[,]" but leaving open the possibility that defendant could renew its request later).

[86] *See* Quon v. Arch Wireless Operating Co., 529 F.3d 892 (9th Cir. 2008), *petition for reh'g en banc denied,* 554 F.3d 769 (9th Cir. 2009), *cert. denied sub nom. USA Mobility Wireless, Inc. v. Quon*, 130 S. Ct. 1011 (2009) (wireless provider violated SCA by disclosing to employer transcripts of employee's text messages sent to and from employer-issued pager).

[87] In *Quon*, the plaintiff did not allege that the City violated the SCA by demanding production of the employee's text message communications. Arguably, the employee could have made this claim and succeeded.

[88] *See* 18 U.S.C. § 2511(1)(a)-(b) (prohibiting intentional interception of any wire, oral, or electronic communication, or intentional use of an electronic device to intercept an oral communication).

[89] *See* Garza v. Bexar Metro. Water Dist., 639 F. Supp. 2d 770, 775 (W.D. Tex. 2009) (The court rejected the contention that employer's employee handbook policy established the plaintiff-employee's consent to the alleged real-time interception of his telephone calls, reasoning that "[d]efendants did not simply listen to [the employee's] stored voice mail messages; instead, they intercepted and listened to entire telephone conversations."); Hay v. Burns Cascade Co., No. 5:06-CV-0137 (NAM/DEP), 2009 WL 414117 (N.D.N.Y 2009) (denying summary judgment of employee's Wiretap Act claims where employer maintained policy stating that it could monitor any transmission but employee presented evidence that she did not receive the policy and was never alerted that her calls were monitored); *but see* Arias v. Mut. Cent. Alarm Serv., Inc., 202 F.3d 553 (2d Cir. 2000) (recording employees' telephone conversations was within ordinary course of business for company which regularly monitored incoming and outgoing calls).

may face liability under the Act. Arguably, an employer might also face liability where it auto-forwards an employee's email to an account reviewed by the employer.[90]

D. Employees' Privileged Communications with Counsel

In addition to the protections described above, employees may also be protected against interception of their communications with counsel. The issue in this context, again, focuses on whether the employee has a reasonable expectation of privacy in her electronic communications such that her attorney-client communication privilege remains intact. If not, the employee may inadvertently waive her attorney-client privilege. The circuits appear to be split over whether employees may waive the attorney-client privilege by storing privileged files on a company computer where the employer maintains a privacy policy aimed at reducing their expectations of privacy.[91] Unfortunately, not all of the rulings in this area include a detailed and reasoned analysis of the waiver issue. However, most courts follow a multi-part test to determine whether a waiver of privilege occurred.

Two recent decisions provide detailed and well-reasoned analyses on the issue of privilege and employer-owned technology, *U.S. v. Hatfield* and *Stengart v. Loving Care*. In *U.S. v. Hatfield*,[92] the court addressed whether an employee's otherwise privileged electronic communications and documents, which were maintained on his work computer, could remain confidential for privilege purposes. The court applied a four-factor test, well established within the district courts,[93] and added its own fifth factor: (1) whether the employer maintained a policy banning personal use; (2) whether the employer monitored employees' use of company computers or emails; (3) whether third parties had a right to access the employees' computer or emails; (4) whether the employee was on notice of the use and monitoring policies; and (5) whether disclosure of the privileged information would be consistent with the employer's interpretation of its own policy.[94]

---

90 *Cf.* U.S. v. Szymuszkiewicz, 622 F.3d 701, 703 (7th Cir. 2010) (jury's conviction of defendant-employee for intentionally intercepting electronic communication through use of an electronic device in violation of Wiretap Act was upheld; there was sufficient evidence to find defendant set up auto-forwarding on his supervisor's computer directing all supervisor's messages to be forwarded to defendant).

91 *Compare* U.S. v. Ziegler, 474 F.3d 1184, 1190 (9th Cir. 2007) (reasonable expectation of privacy in the contents of work computer) *with* Muick v. Glenayre Elec., 280 F.3d 741, 743 (7th Cir. 2002) (no expectation of privacy in contents of work computer); U.S. v. Simons, 206 F.3d 392, 398 (4th Cir. 2000) (computer usage policy defeated public-sector employee's reasonable expectation of privacy).

92 No. 06-CR-0550, 2009 WL 3806300 (E.D.N.Y. 2009).

93 *See* Curto v. Med. World Comm'n., Inc., 03-CV-6327, 2006 WL 1318387, at *2-3 (E.D.N.Y. May 15, 2006) (applying four-factor test and finding that employee did not waive privilege by maintaining documents on employer's computer); Geer v. Gilman Corp., 06-CV-0889, 2007 U.S. Dist. LEXIS 38852, at *3-4 (D. Conn. Feb. 12, 2007); *In re* Asia Global Crossing, Ltd., 322 B.R. 247, 259-61 (Bankr. S.D.N.Y. 2005). These factors have also been applied to employers' access of personal computer data and emails outside of the Second Circuit. *See e.g.* Gates v. Wheeler, No. A09-2355, 2010 WL 4721331, at *6-7 (Minn. Ct. App. Nov. 23, 2010) (applying the four-factor test, the court found no technology policy, and determined that plaintiff-partner's expectation of privacy in his work email account, accessed by defendant partner and site administrator, was reasonable and the attorney client privilege had not been waived); Haynes v. Attorney Gen. of Kan., No. 08-4209-RDR, 2005 WL 2704956, at *3-4 (D. Kan. Aug. 26, 2005) (applying the four-factor test, court found public employee had no reasonable expectation of privacy in personal data saved on his work computer).

94 U.S. v. Hatfield, 2009 Westlaw 3806300, at *8.

The court found several problems with the employer's broad computer use policy, including that the employer understood its policy to protect other employees' "privileges," *i.e.*, expectations of privacy.[95] The court concluded that it would be "fundamentally unfair to subject [the employee] to the consequences of waiving privilege based on a strict, theoretical interpretation of [the employer's] Computer Usage Policy that was never imagined by [the employer] itself and [was], in fact, contradicted by [the employer's] own actions. . . ."[96] Thus, employees may be able to retain their privileged communications even if they are created or stored on their work computers and their employers maintain a broad technology policy.[97]

In *Stengart v. Loving Care Agency, Inc.*,[98] the New Jersey Supreme Court upheld a lower court's ruling that an employer interfered with its former employee's reasonable expectation of privacy when it retrieved emails sent and received on a company computer between the former employee and her attorney. The court observed that "the electronic age-and the speed and ease with which many communications may now be made, has created numerous difficulties in segregating personal business from company business."[99] In this context, the court balanced the company's right to create and enforce reasonable rules for workplace conduct against the public policies underlying the attorney-client privilege, and found that while an employer has a right to establish policies governing computer use and to discipline employees who violate them, a policy that states that an employer could read an employee's attorney-client communication would be unenforceable.[100]

In contrast, where employees are communicating with their counsel via their employers' email account (*i.e.*, not via a personal password-protected web-based email account such as Gmail, Yahoo! or Hotmail), courts are less willing to protect the privilege.[101] For example, in *Holmes v. Petrovich Dev. Co., LLC*,[102] a California state court recently held that an employee who used her employer's computer and email system to communicate with her attorney had waived the attorney-client privilege.[103] The court distinguished *Stengart* based on the fact that

---

95 The court also found that that the policy did not expressly prohibit usage for personal legal matters, it did not state that the employer *will* monitor computer usage (it merely reserved the employer's *right* to do so) and there was no evidence that the employer actually monitored computer usage. The court was less concerned about the factors weighing in favor of waiver, *i.e.*, that the employee had knowledge of the monitoring policy because he was the CEO and the policy was implemented under his watch.

96 U.S. v. Hatfield, 2009 WL 3806300, at *10.

97 *See also* Stengart v. Loving Care Agency, Inc., 973 A.2d 390, 399-401 (N.J. Super. Ct. App. Div. 2009), *aff'd in part and modified in part*, 990 A.2d 650 (N.J. Super. Ct. App. Div. 2010); Nat'l Econ. Research Assocs. v. Evans, No. 04 Civ. 2618, 2006 WL 2440008, at *4 (Mass. Super. Aug. 3, 2006) (employee did not waive the attorney-client privilege by communicating with his attorney using a password-protected Yahoo e-mail account on a company-provided laptop computer, employee had a reasonable expectation of privacy and the company's technology use policy did nothing to temper that expectation).

98 973 A.2d at 399-401.

99 *Id*. at 400.

100 *Id.* at 397.

101 *See* Long v. Marubeni Am. Corp., No. 05 Civ. 639, 2006 U.S. Dist. LEXIS 76594 (S.D.N.Y. Oct. 19, 2006) (finding privilege to be waived); Beth Israel Med. Ctr. Inc., 847 N.Y.S.2d 436, 444 (N.Y. Sup. Ct. 2007) (same).

102 191 Cal. App. 4th 1047 (Cal. App. 2011).

103 *See also* Alamar Ranch, LLC v. Cnty. of Boise, No. CV-09-004-S-BLW, 2009 WL 3669741, at *4 (D. Idaho Nov. 2, 2009) (despite client's claim that she was unaware of the employer's policy, client received the warning that her work e-mails would be stored by employer and it was unreasonable for her to believe that e-mails sent directly from her work e-mail address would not be available for retrieval by her employer).

the employee in *Holmes* used her work email account, not a password-protected web-based account, and the company policy concerning monitoring specifically addressed communications on its email system.[104] Consequently, employees and their attorneys should be careful not to use employer email systems for confidential communications since in this context they are least likely to be protected.

E. Potential Privacy Claims Under State Law

Employees may find additional privacy-related protections under state law.[105] Although some states have common-law invasion of privacy doctrines,[106] others, like New York, do not.[107] However, some of these states may have recreational activities laws that provide additional protections to employees. Such laws may include protections for technology use outside the workplace, such as blogging or Tweeting.[108]

For example, New York Labor Law § 201-d prohibits termination of employees based on recreational activities performed outside the workplace. In late 2010, a former employee filed a complaint against an employer alleging that the employer terminated her in violation of § 201-d due to her blogging activities. In that case, *Tagocon v. J.P. Morgan Chase*,[109] the employee

---

104 Holmes v. Petrovich Dev. Co., 191 Cal. App. 4th 1047, 1068 (Cal. Ct. App. Jan. 13, 2011).

105 Several states have enacted legislation limiting employers' ability to monitor employees' use of workplace technologies. Connecticut and Delaware have requirements that obligate employers to notify employees that their e-mail is being monitored. *See* CONN. GEN. STAT. ANN. § 31-48d (1999); DEL. L. CODE, tit. 19, § 705(b) (Supp. 2002). Michigan and Illinois have integrated prohibitions on collecting information, by technological monitoring or otherwise, about certain employee behavior into statutes which govern the use of personnel records. *See* MICH. COMP. L. § 423.508 (2008); 820 ILL. COMP. STAT. 40/9 (2008).

106 *See* Sanchez-Scott v. Alza Pharm., 86 Cal. App. 4th 365, 372 (Cal. Ct. App. 2001) (recognizing common law invasion of privacy claim); Brown-Criscuolo, 601 F. Supp. 2d 441 (D. Conn. 2009) (employee's invasion of privacy claims survived summary judgment, even where employer maintained computer use policy warning of computer monitoring, because employer accessed employee's password-protected work email account); Walston v. UPS, No. 2:07-CV-525, 2009 U.S. Dist. LEXIS 10307 (D. Utah Feb. 11, 2009) (finding invasion of privacy where co-worker recorded employee without permission and employee suffered severe anxiety); Gates v. Wheeler, A09-2355, 2010 WL 4721331 (Minn. Ct. App. Nov. 23, 2010) (temporary injunction restraining defendant-partner's access of plaintiff's work and private emails was upheld based on an invasion of privacy claim); Hill v. Nat'l Collegiate Athletic Ass'n., 7 Cal. 4th 1, at 36 (Cal. 1994) (California's constitutional right to privacy applies to conduct by private persons); Norman-Bloodsaw v. Lawrence Berkeley Lab., 135 F.3d 1260, 1271 (9th Cir. 1998) (private employer violated employee's constitutional right to privacy when it tested for medical conditions without employee's knowledge or consent).

107 *See* Mack v. U.S., 814 F.2d 120, 123 (2d Cir. 1987) (New York law does not recognize invasion of privacy as a common-law tort); Andrews v. Bruk, 160 Misc. 2d 618, 620 (N.Y. Misc. 1994), *rev'd on other grounds*, 220 A.D.2d 376 (N.Y. App. Div. 1995) ("[u]nfortunately, to date, unlike most jurisdictions, New York has not adopted a common-law right to privacy"). *But see* Randi A.J. v. Long Island Surgi-Center, 842 N.Y.S.2d 558, 565 (N.Y. App. Div. 2007) (recognizing public policy right to keep medical treatment private and personal and medical records confidential).

108 *See* N.Y. LAB. L. § 201-d; 2 CAL. CODE REGS. § 7286.7(b) (prohibiting employers from inquiring into any issues which otherwise serve no "business purpose"); COLO. REV. STAT. § 24-34-402.5 (prohibiting discharge for engaging in lawful off-duty activity unless the restriction is rationally related to the employee's duties, a bona fide occupation requirement, or is necessary to avoid a conflict); N.D. CENT. CODE § 14-02.4-08 (same).

109 No. 10116415, *complaint filed* (N.Y. Sup. Ct. Dec. 20, 2010). *See Ex-JPMorgan Employee Says She Was Fired for Blogging:* Tagocon v. JPMorgan Chase, Westlaw Journal Employment, 25 No. 13 Westlaw Journal Employment 3, 2011 WL 231646 (WJEMP) (Jan. 25, 2011). Tagocon is seeking a declaratory judgment that JPMorgan's actions violated New York law. She also seeks actual damages, including back and front pay,

asserted that prior to and during her employment she maintained a blog, the subject matter being personal and aimed at publicizing her novels. According to her complaint, the blog did not contain any reference to her work or employment. However, upon discovering that her employer maintained a policy prohibiting employee Internet postings, even when done on personal time, the employee approached her employer to confirm whether her blog violated the policy.[110] Her employer told her to remove the blog or face termination. She refused and was subsequently terminated. Although there has been no decision on the merits of the case as of the date this paper was written, a future ruling may have far-reaching implications on the scope of recreational activities statutes and whether such laws may protect employees engaging in lawful recreational activities like blogging or social networking.

Some states also provide protections similar to the Wiretap Act and prohibit "tampering with private communications."[111] Employees may also have claims of false light invasion of privacy (*e.g.*, for online misrepresentations about employees, such as statements made by managers on social networking sites like LinkedIn),[112] intrusion of seclusion,[113] or tort claims arising out of workplace cyberstalking.[114] It may also be possible to bring a tortious interference with contract claim against an employer who requires an employee to authorize employer access

---

compensatory damages for pain and suffering, and punitive damages, Robert Ottinger, *Social Networking and Your Job*, New York Employment Lawyer Blog (Feb. 8, 2011), http://www.newyorkemploymentlawyerblog.com/employment_law/ (last visited Mar. 6, 2011); Kathianne Boniello, *Banker's Blogger Booted*, N.Y. POST, Jan. 2, 2011, *available at* http://www.nypost.com/p/news/local/bank_bloggerbooted_PPrpezgTbdtDuVGLzbdX3K#ixzz1EloQdmlz.

[110] J.P. Morgan's Code of Conduct 2010 states, in relevant part, "Employees' postings on internet sites, including social and business networking websites… should not include any information related to the firm's business," which " is broadly defined and generally includes anything related to the financial services industry; the firm itself and its businesses; such matters as the firm's security, technology support, procurement practices, legal/regulatory /compliance issues, etc.; and the firm's customers, employees, or vendors." *See* J.P. Morgan Chase & Co. Code of Conduct, 3.4, Publications, speeches, Internet postings, and other communications relating to JPMorgan Chase's busine**ss,** available online http://www.jpmorganchase.com/corporate/About-JPMC/code-of-conduct.htm (last visited Mar. 15, 2011). The policy also includes provisions limiting political speech and cites the policy on *Communication on Matters Relating to the Company's Business* as a source for "[a]dditional information on employees' communications, and … pre-clearance of certain types of communications..." *Id.*

[111] *See* N.Y. PENAL L. § 250.25 (prohibiting obtaining or revealing "telephonic or telegraphic communication," as well as accessing, without a sender or receiver's consent, "a sealed letter or other sealed private communication"); CAL. PENAL CODE § 632 (prohibiting eavesdropping or recording a confidential communication); CAL. PENAL CODE § 502 (prohibiting unauthorized access to computers and computer data); *see also* Patrolmen's Benevolent Ass'n v. City of New York, No. 97 CV 7138(SJ), 2000 WL 307377, at *3 (E.D.N.Y. Mar. 26, 2000) (reasonable minds could differ as to whether police officers had reasonable expectation of privacy that was violated by installation of surveillance camera in multipurpose room).

[112] *See* Meyerkord v. Zipatoni Co., 276 S.W.3d 319, 325 (Mo. Ct. App. 2008) (false light invasion of privacy where employer falsely listed employee as registrant on controversial and highly publicized website hosted by third party and kept employee's name on website after his employment terminated.).

[113] *See* Doe v. Kohn Nast & Graf, P.C., 866 F. Supp. 190, 196 (E.D. Pa. 1994) (jury may decide whether opening personal mail sent to workplace is highly offensive to a reasonable person).

[114] Most states have criminal cyberstalking laws. *E.g.*, Arizona (ARIZ. CRIM. CODE (1995): 13-2921); Alaska (ALASKA CRIM. L. § 11.41.270); Connecticut (CONN. PENAL CODE § 53a-183); New Jersey (N.J. REV. STAT. §§ 2C:33-4, 2C:12-10 (2001 S.B. 1616)); New York (N.Y. PENAL CODE § 240.30); Oklahoma (OKLA. (1996): §21-1173); and Wyoming (WYO. § 6-2-506).

to her social networking site profile, by claiming that this act violates her service agreement or that doing so violates public policy concerns.[115]

F. International Trends in Workplace Privacy Protections

Unlike the U.S., many countries have had strong privacy policies in place since World War II, in both the public and private workplace. In fact, in many countries such as Chile, France or Mexico, the right to privacy in regard to emails in the workplace is an unwaivable right.[116] In most European Union ("EU") countries this was a direct reaction to the holocaust and widespread civilian collusion with the Nazi regime.[117] In certain Asian countries and in parts of South America, data privacy and other individual privacy rights in the workplace are protected by statute and in some countries they are constitutional rights.[118] However, in the global workplace, all of these countries, much like the U.S., share an increased sense of urgency in dealing with the technological revolution in the workplace and its resulting lack of employee privacy.

Specifically, in many European countries, monitoring, gaining access to employees' computers and video surveillance are void *ab initio* or circumscribed by statute.[119] In 2007, the European Court of Human Rights held, under Article 8 of the European Convention on Human Rights, that employee email messages are protected communications.[120] More recently, the EU released a plan to revise European data protection rules based on the Commission's position that an individual's ability to control his or her information, have access to the information, and modify or delete the information are "essential rights that have to be guaranteed in today's digital world."[121] Increasingly, individual EU nations are poised to enact more stringent privacy laws. For instance, Finland recently introduced a statute expanding employee privacy rights[122] and Sweden is expected to follow suit.[123] Within the last year, Germany (a country which instituted strong data privacy and anti-monitoring laws after the holocaust) also approved a draft law amending its Federal Data Protection Act, which prohibits employers from disciplining employees for their private online activities, to provide even broader protections.[124]

---

115 Facebook's privacy policy prohibits those who use the site from soliciting login information or accessing an account that belongs to someone else. Facebook Statement of Rights and Responsibilities (Dec. 21, 2009) (http://www.facebook.com/policy.php#!/terms.php) (last visited Mar. 19, 2010).

116 *Overview*, RESTRICTIVE COVENANTS AND TRADE SECRETS IN EMPLOYMENT LAW: AN INTERNATIONAL SURVEY, VOL. I (Lazar & Siniscalco, eds., 2010) at I-30.

117 *Id.* at I-30.

118 *Id*. at I-31 and 32.

119 *Id*. at I-30.

120 Copland v. U.K., 45 Eur. Ct. H.R. 37 (2007).

121 The EU Data Protection Directive 95/46/EC. *See* Boris Segalis, *European Commission Announces Strategy for Revising EU Data Protection Rules*, Information Law Group, Nov. 4, 2010, *available at* http://www.infolawgroup .com /2010/11/articles /eu-1/european-commission-announces-strategy-for-revising-eu-data-protection-rules/ (last visited Feb. 25, 2011).

122 The Act on the Protection of Privacy in Working Life 759/2004 (Fin.) (Laki yksityisyyden suojasta työelämässä 759/2004 (Fin.)).

123 Jarno J. Vanto, et al., *Employee Expectation of Privacy with Respect to Use of Employer-Owned Workplace Computers and Other Electronic Devices and Files Stored on Such Devices—Global Cases*, 2 A.L.R. Int'l 587, (Originally published in 2010).

124 On August 25, 2010, the German government approved a draft law concerning special rules for employee data protection, amending the German Federal Data Protection Act (the Bundesdatenschutzgesetz or "BDSG") by

Even outside the EU, other countries continue this trend toward protecting employee privacy rights. In the Middle East, the Israeli National Labour Court issued a decision in February 2011 that severely limits the extent to which employers can monitor their employees' emails. According to the opinion, employers must now create an understandable policy for employee use of communications systems at the workplace. This policy must be clearly communicated to all employees, and must be written into their contracts.[125]

CONCLUSION

The changing forms of technology and their vast access to information will undoubtedly continue to dictate operational realities and expectations of privacy in the workplace. The challenge for courts is that they must continuously monitor these changes and balance a businesses need to protect data and proprietary information against individual rights and freedoms. In the wake of *City of Ontario v. Quon*, and facing the risk of sacrificing overbroad constitutional rights, courts may consider the societal role of the particular electronic communication at issue and refrain from issuing rulings based solely on the language of a standardized privacy policy. In *Quon*, the Supreme Court recognized the increasing importance of technology in workers' lives, noting that "[c]ell phone and text message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self identification."[126] As the Court explained, the more pervasive and essential or necessary an electronic tool becomes for an individual's self-expression or identification, the "[stronger] the case for an expectation of privacy."[127] As new technologies become the norm of every-day life and employees' private lives intertwine with their work lives, the law will have to respond accordingly with safeguards that prevent employers from abusing and interfering with their employees' every day communications and recognize that workplace privacy is a value worth protecting.

---

adding provisions that specifically address data protection in the employment context. Currently, employee data protection is regulated by (1) general provisions in the BDSG, (2) the new Section 32 of the BDSG introduced by the most recent reform in September 2009, (3) the Works Constitution Act, (4) guidance from state data protection authorities, and (5) comprehensive case law from federal and local labor courts. The draft law covers nine key subject areas, including employer Internet searches. December 20, 1990 (BGBl.I 1990 S.2954), amended by law of Sept. 30 2009.

[125] Labour Appeal no. 90/08 Tali Isakov Inbar v. The Commissioner for women labour. *See* Boris Segalis, *Israel's National Labor Court Imposes Strict Limits on Employee Monitoring* Information Law Group, Feb. 10, 2011, *available at* http://www.infolawgroup.com /2010/11/articles /eu-1/european-commission-announces-strategy-for-revising-eu-data-protection-rules/ (last visited Feb.25, 2011).

[126] *Quon* at 2630.

[127] *Id.*