The NSA (likely) is Watching You – Privacy and Data Security and the Rise of Cyber Theft

Presented to:

American Bar Association, Section of Labor and Employment Law
2014 American Bar Association Annual Meeting

Boston, Massachusetts
August 7, 2014

Adam S. Forman, Esq.*
Miller, Canfield, Paddock and Stone, P.L.C.
150 W. Jefferson, Suite 2500
Detroit, Michigan 48226
forman@millercanfield.com

* The author acknowledges the contributions of Lavon M. Ammori, David G. King, and M. Misbah Shahid, associates at Miller, Canfield, Paddock and Stone, P.L.C., to this paper.
# MILLER, CANFIELD, PADDOCK AND STONE, P.L.C.

## TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>INDEX OF AUTHORITIES</th>
<th>v</th>
</tr>
</thead>
<tbody>
<tr>
<td>I. INTRODUCTION</td>
<td>1</td>
</tr>
<tr>
<td>II. LEGAL PRINCIPLES AND IMPEDIMENTS TO EMPLOYER MONITORING OF EMPLOYEE USE OF COMMUNICATIONS TECHNOLOGY</td>
<td>1</td>
</tr>
<tr>
<td>A. Background</td>
<td>1</td>
</tr>
<tr>
<td>B. Federal Protections</td>
<td>3</td>
</tr>
<tr>
<td>1. Protections Under United States Constitution</td>
<td>3</td>
</tr>
<tr>
<td>a. First Amendment</td>
<td>4</td>
</tr>
<tr>
<td>b. Fourth Amendment</td>
<td>9</td>
</tr>
<tr>
<td>c. Fifth Amendment</td>
<td>12</td>
</tr>
<tr>
<td>d. Ninth and Fourteenth Amendment</td>
<td>13</td>
</tr>
<tr>
<td>2. Protections Under Federal Statutes</td>
<td>15</td>
</tr>
<tr>
<td>a. Electronic Communications Privacy Act</td>
<td>15</td>
</tr>
<tr>
<td>(i) Title I: Federal Wiretap Act</td>
<td>15</td>
</tr>
<tr>
<td>(ii) Title II: Stored Communications Act</td>
<td>17</td>
</tr>
<tr>
<td>(iii) Exceptions to ECPA</td>
<td>20</td>
</tr>
<tr>
<td>b. National Labor Relations Act</td>
<td>21</td>
</tr>
<tr>
<td>(i) General Overview</td>
<td>21</td>
</tr>
<tr>
<td>(ii) Email/Communication Policies</td>
<td>23</td>
</tr>
<tr>
<td>(iii) Social Media – The So-Called “New Water Cooler”</td>
<td>25</td>
</tr>
<tr>
<td>(a) Guidance from the Board</td>
<td>27</td>
</tr>
<tr>
<td>(i) Costco Wholesale Corp</td>
<td>30</td>
</tr>
<tr>
<td>(ii) Karl Knauz Motors, Inc</td>
<td>31</td>
</tr>
<tr>
<td>(iii) Hispanics United of Buffalo</td>
<td>32</td>
</tr>
<tr>
<td>(iv) Design Technology Group LLC d/b/a Bettie Page Clothing</td>
<td>33</td>
</tr>
<tr>
<td>(v) Target Corporation</td>
<td>33</td>
</tr>
<tr>
<td>(vi) New York Party Shuttle, LLC</td>
<td>34</td>
</tr>
</tbody>
</table>
(vii) World Color (USA) Corp............................................. 34
(viii) Amalgamated Transit Union................................. 35
(b) Other Guidance ....................................................... 35

c. Computer Fraud and Abuse Act ............................................ 38
d. Other Federal Statutes......................................................... 42

C. State Protections.................................................................................... 42
1. Protections Under State Constitutions .......................................... 42
2. Protections Under State Statutes................................................. 44
   a. Anti-Wiretapping and Monitoring Statutes ............................ 44
   b. Password Protection Statutes ............................................ 46
   c. Off-Duty Conduct Statutes ............................................... 50
   d. Whistleblower Protection Statutes ...................................... 52
   e. FTC Regulations Regarding Enforcements .......................... 52

D. Common Law Torts .................................................................................. 53

E. Attorney-Client Privilege for Communications via Employer Technology ........................................ 54
1. ABA Guidance on Privilege Issues................................................... 54
2. Guidance from Courts on Privilege Issues.................................... 55
   a. Cases finding communications were privileged .................... 56
      (i) Stengart v. Loving Care Agency, Inc................................. 56
      (ii) Sims v. Lakeside School.............................................. 57
   b. Cases finding communications not privileged .................... 58
      (i) Holmes v. Petrovich Development Company.................. 58
      (ii) Aventa Learning, Inc. v. K12, Inc. ............................... 59
   c. Other Considerations ......................................................... 60

3. Other Privileges for Communications via Employer Technology........ 60

III. CASE LAW REGARDING MONITORING ISSUES IN THE WORKPLACE........ 61
A. Social Media as a Tool in Hiring and Recruitment............................... 64
1. Screening Job Applicant’s Social Media Presence/Online Reputation ........................................................................ 64
   a. Applicant’s “Protected Class” Status.................................... 66
b. Employer’s Affirmative Obligation to Search All Publicly Available Information ................................................................. 67
c. Discoverability of Collected Information and Record Retention ...................................................................................... 67
   (i) Hiring Process – Federal Contractors .................................. 68
2. Internet Searches and Social Media in Recruitment ......................... 68
3. Pre-Employment Checks ......................................................................... 69
   a. Criminal Background Checks ...................................................... 69
   b. Credit Checks ............................................................................... 70
   c. Health Checks .............................................................................. 72
d. Drug Tests .................................................................................... 74
e. Lie Detectors ................................................................................ 75
B. Issues Relating to Employment ................................................................. 75
1. Privacy Concerns – Monitoring ............................................................... 75
   a. Email & Internet .......................................................................... 76
   b. Video ............................................................................................ 77
   c. Workplace and Physical Searches ............................................... 78
2. Social Media in Employment/Workplace Actions .................................. 78
   a. Adverse Action by Employer and Subsequent Discrimination Claim by Employee ............................................................... 78
   b. Harassment and Hostile Work Environment Claims ............... 80
c. Age Discrimination ...................................................................... 84
d. Retaliation .................................................................................... 84
3. Ownership of Employer-Sponsored Social Media Accounts .......... 87
4. Bring Your Own Device (“BYOD”) ............................................................ 88
   a. Control of Employer Data ............................................................ 89
      (i) Keeping Information Secure .................................................. 89
      (ii) Recordkeeping and Discovery Obligations ................. 90
   b. Compliance with Employment and Labor Laws ......................... 91
      (i) Equal Employment Opportunity Laws ............................ 91
      (ii) Labor Laws ........................................................................ 92

© 2014 Miller Canfield, Paddock and Stone, P.L.C. All Rights Reserved.
(iii) Wage and Hour Laws.............................................................. 93
(iv) Other Laws........................................................................... 95
# INDEX OF AUTHORITIES

<table>
<thead>
<tr>
<th>CASES</th>
<th>Page(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anderson v. City of Columbus, Ga., 374 F. Supp. 2d 1240 (M.D. Ga. 2005)</td>
<td>19</td>
</tr>
<tr>
<td>Bland v. Roberts, 730 F.3d 368 (4th Cir. 2013)</td>
<td>5, 6</td>
</tr>
<tr>
<td>Brewers and Malsters v. NLRB, 414 F.3d 36 (D.C. Cir. 2005)</td>
<td>76</td>
</tr>
<tr>
<td>Burlington Indus., Inc. v. Ellerth, 524 U.S. 742, 118 S. Ct. 2257 (1998)</td>
<td>80, 91</td>
</tr>
<tr>
<td>Cardinal Health 414, Inc. v. Adams, 582 F. Supp. 2d 967 (M.D. Tenn. 2008)</td>
<td>19</td>
</tr>
<tr>
<td>Carrol v. Lynch, 698 F.3d 561 (7th Cir. 2012)</td>
<td>45, 46</td>
</tr>
<tr>
<td>Carter v. County of Los Angeles, 770 F. Supp. 2d 1042 (C.D. Cal. 2011)</td>
<td>76, 77</td>
</tr>
<tr>
<td>Clarity Servs., Inc. v. Barney, 698 F. Supp. 2d 1309 (M.D. Fla. 2010)</td>
<td>38</td>
</tr>
<tr>
<td>Crowley v. Cyberstapec Corp., 166 F. Supp. 2d 1263 (N.D. Cal. 2001)</td>
<td>15</td>
</tr>
</tbody>
</table>
Cummings v. Washington Mat., 650 F.3d 1386 (11th Cir. 2011)............................................................74
Curran v. Cousins, 509 F.3d 36 (1st Cir. 2007)...........................................................................................5
Curto v. Med. World Commc’n, Inc., No. 03CV6327, 2006 WL 1318387 (E.D.N.Y. May 15, 2006)........76
Derrick v. Metro. Gov. of Nashville & Davidson Cnty., Tenn., No. 3-06-1222, 2007 WL 4468673............17
Dible v. City of Chandler, 515 F.3d 918 (9th Cir. 2008)...............................................................................7
Dorson v. City of Syracuse, No. 5:04-CV-1388, 2009 WL 2176127 (N.D.N.Y. Jul. 21, 2009).................84
EEOC v. Ford Motor Credit Co., 531 F. Supp. 2d 930 (M.D. Tenn. 2008)..................................................72
EEOC v. Mgmt. Hospitality of Racine, Inc., 780 F. Supp. 2d 802 (E.D. Wis. 2010).................................82, 83
Faragher v. City of Boca Raton, 524 U.S. 775, 118 S. Ct. 2275 (1998)..................................................80, 91
Fatland v. Quaker State Corp., 62 F.3d 1070 (8th Cir. 1995).................................................................50
Folkerson v. Circus Enters., Inc., 107 F.3d 754 (9th Cir. 1997).................................................................80
Garcia v. City of Laredo, Texas, 702 F.3d 788 (5th Cir. 2012)..............................................................17, 18
Gaskell v. Univ. of Ky., No. 09-244, 2010 WL 4867630 (E.D. Ky. Nov. 23, 2010).................................78

© 2014 Miller Canfield, Paddock and Stone, P.L.C. All Rights Reserved.
Loschen v. Trinity United Methodist Church of Lincoln, No. 4:08CV3143, 2009 WL 2902956 (D. Neb. Sept. 9, 2009) .................................................. 72
Love v. Rehuis, 946 N.E.2d 1 (Ind. 2011) .............................................................. 7


LVCR Holdings LLC v. Brekka, 581 F.3d 1127 (9th Cir. 2009) ........................................ 38


Marshall v. Mayor & Alderman of City of Savannah, Ga., 366 Fed. Appx. 91 (11th Cir. 2010) ............................................................. 78


Maypark v. Securitas Sec. Servs. USA, Inc, 775 N.W.2d 270 (Wis. Ct. App. 2009) ....... 66

McPherson v. O’Reilly Autom., Inc., 491 F.3d 726 (8th Cir. 2007) ........................................ 72


Mo. State Teachers Ass’n v. Missouri, No. 11AC-CC00553 (Mo. Cir. Co. Aug. 26, 2011) .......... 9


Myers v. Toojoy’s Corp., 640 F.3d 1278 (11th Cir. 2011) ............................................ 70

NLRB v. White Oak Manor, 452 F.App’x 374 (4th Cir. 2011) ........................................ 23


P.R. Telephone Co., Inc. v. San Juan Cable LLC, No. 11-2135, 2013 WL 5533711 (D.P.R. Oct. 7, 2013) .................................................. 90


© 2014 Miller Canfield, Paddock and Stone, P.L.C. All Rights Reserved.
18 U.S.C. § 2510(A)–(B)..........................................................................................................................16
18 U.S.C. § 2511(1).......................................................................................................................................15
18 U.S.C. § 2511(2)(c)–(d)....................................................................................................................14, 15, 19, 20, 43, 44, 74
18 U.S.C. § 2511(4)(a)–(b)....................................................................................................................15
18 U.S.C. § 2520(c)(2)(B)........................................................................................................................15
18 U.S.C. § 2701(a)....................................................................................................................................15, 16, 17, 18, 19, 20, 43, 45, 75, 94
18 U.S.C. § 2701(b)....................................................................................................................................15
29 U.S.C. § 216(b).....................................................................................................................................93
29 U.S.C. § 2002(1)....................................................................................................................................41, 74
42 U.S.C. § 1320d-9(b)(3)......................................................................................................................72
42 U.S.C. § 1983 ........................................................................................................................................9
42 U.S.C. § 2000ff ....................................................................................................................................72

**STATUTES (STATE)**

<table>
<thead>
<tr>
<th>Statute</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALA. CODE § 13A-11-30</td>
<td>44</td>
</tr>
<tr>
<td>ALASKA STAT. § 42.210.310</td>
<td>44</td>
</tr>
<tr>
<td>ARIZ. REV. STAT. Ann. § 13-3005</td>
<td>44</td>
</tr>
<tr>
<td>ARK. CODE ANN. § 5-60-120; §5-16-101</td>
<td>44</td>
</tr>
<tr>
<td>CAL. ED. CODE § 99120 (Cal. 2012)</td>
<td>46</td>
</tr>
<tr>
<td>CAL. LAB. CODE §§ 96(k), 98.6</td>
<td>49</td>
</tr>
<tr>
<td>CAL. LAB. CODE § 980 (Cal. 2012)</td>
<td>47</td>
</tr>
<tr>
<td>CAL. LABOR CODE § 432.9</td>
<td>69</td>
</tr>
<tr>
<td>CAL. PENAL CODE § 647</td>
<td>44</td>
</tr>
<tr>
<td>COLO. REV. STAT. § 18-9-303</td>
<td>44</td>
</tr>
<tr>
<td>COLO. REV. STAT. § 24-5-101</td>
<td>71</td>
</tr>
<tr>
<td>COLO. REV. STAT. § 24-34-402.5</td>
<td>49</td>
</tr>
<tr>
<td>COLO. REV. STAT. § 24-34-402.5(1)</td>
<td>49</td>
</tr>
<tr>
<td>COLO. REV. STAT. § 24-34-402.5(1)(a)–(b)</td>
<td>50</td>
</tr>
<tr>
<td>CONN. GEN. STAT. § 14-296aa(b)(1)</td>
<td>95</td>
</tr>
<tr>
<td>CONN. GEN. STAT. § 31-48d</td>
<td>44</td>
</tr>
<tr>
<td>CONN. GEN. STAT. § 31-51t</td>
<td>71</td>
</tr>
<tr>
<td>CONN. GEN. STAT. § 52-570d</td>
<td>44</td>
</tr>
<tr>
<td>D.C. CODE § 23-542</td>
<td>44</td>
</tr>
<tr>
<td>DEL. CODE ANN. tit. 11, § 2402(c)(4)</td>
<td>44</td>
</tr>
<tr>
<td>DEL. CODE ANN. tit. 14, § 94 (Del. 2012); Public Act 478</td>
<td>46, 47</td>
</tr>
<tr>
<td>DEL. CODE ANN. tit. 19, § 705</td>
<td>45</td>
</tr>
<tr>
<td>FLA. STAT. § 934.03</td>
<td>44</td>
</tr>
<tr>
<td>GA. CODE ANN. § 16-11-62.5</td>
<td>44</td>
</tr>
<tr>
<td>HAW. REV. STAT. § 378-2(8)</td>
<td>71</td>
</tr>
<tr>
<td>HAW. REV. STAT. §§ 378-2, 378-2.5</td>
<td>69</td>
</tr>
<tr>
<td>HAW. REV. STAT. § 803-42</td>
<td>44</td>
</tr>
<tr>
<td>IDAHO CODE ANN. § 18-6702</td>
<td>44</td>
</tr>
<tr>
<td>720 ILL. COMP. STAT. 5/14-1</td>
<td>44</td>
</tr>
<tr>
<td>820 ILL. COMP. STAT. 55/10 (III. 2012)</td>
<td>46, 49, 71</td>
</tr>
<tr>
<td>IND. CODE § 22-5-4-1</td>
<td>49</td>
</tr>
<tr>
<td>IOWA CODE § 727.8</td>
<td>44</td>
</tr>
<tr>
<td>LA. REV. STAT. ANN. § 23.966</td>
<td>49</td>
</tr>
<tr>
<td>LA. REV. STAT. ANN. § 15:709</td>
<td>44</td>
</tr>
<tr>
<td>KY. REV. STAT. ANN. § 344.040</td>
<td>49</td>
</tr>
<tr>
<td>MASS. GEN. LAWS. Ch. 6 §§ 151B, 168-173</td>
<td>69</td>
</tr>
</tbody>
</table>
WIS. STAT. ANN § 111.321 ..........................................................................................................................................49
WIS. STAT. § 968.31 ...............................................................................................................................................44
WYO. STAT. ANN. § 7-3-701 ................................................................................................................................44
WYO. STAT. ANN. § 27-9-105 ................................................................................................................................49

MUNICIPALITE ORDINANCES
Newark Ordinance #12-1630 (Sept. 19, 2012) ............................................................................................................69
Philadelphia Code, Title 9 ...........................................................................................................................................69

COURT RULES
Fed. R. Civ. P. 34 .........................................................................................................................................................90

OTHER AUTHORITIES
16 C.F.R. § 255.5.......................................................................................................................................................51, 52
16 C.F.R. § 682.3.........................................................................................................................................................89
29 C.F.R. § 785.11 .......................................................................................................................................................92
29 C.F.R. § 785.12 .......................................................................................................................................................92
29 C.F.R. § 785.47 .......................................................................................................................................................93
29 C.F.R. § 1635.8(b)(1)(ii)(D) .............................................................................................................................65, 90
41 C.F.R. § 60-1.3 .......................................................................................................................................................67
45 C.F.R. § 160 ......................................................................................................................................................72, 89
45 C.F.R. § 164.........................................................................................................................................................89
I. INTRODUCTION

Technology that is the norm today – blogs, cloud computing, iPhones, internet tracking software, smartphones and tablets, and Facebook for example – barely existed just a few years ago. Such advances have, among other things, raised significant privacy questions that the law is struggling to address in light of the exponential growth of technology. To this end, this paper offers a primer on how technology in the workplace has forever changed the workplace privacy landscape. The first section considers the underpinnings of some of the protections offered to employees in the workplace: the Federal Constitution; Federal statutes; State Constitutions; State statutes; Common Law; and the Attorney-Client Privilege. The second section discusses the various issues implicated by monitoring employees, including employee hiring and recruitment, privacy concerns, and the rapidly developing area of how social media has changed the workplace.

II. LEGAL PRINCIPLES AND IMPEDIMENTS TO EMPLOYER MONITORING OF EMPLOYEE USE OF COMMUNICATIONS TECHNOLOGY

“U.S. law gives employees few protections against employer surveillance of their workplace communications. Even without express employee consent, U.S. employers generally may listen to workplace telephone conversations, read messages sent to and from corporate email accounts, and record and disclose the contents of employee communications. Employees that bring legal challenges to these practices rarely succeed in U.S. courts.”¹

A. Background

Given the foregoing, it should come as no surprise that employer-monitoring of employee electronic communications has become the norm. Monitoring methods take many forms, such as direct surveillance, which records periodic “snapshots” of employees’ computer screens, keystroke logging, which allows reconstruction of every computer action and keyword flagging, which alerts the company to use of specific words in email or Internet searches. It is also not just limited to the accepted practice of monitoring employee internet or email usage; employers are also increasingly monitoring employee use of social media.² As technology becomes more

² PROSKAUER ROSE, SOCIAL MEDIA IN THE WORKPLACE AROUND THE WORLD 2.0, 20 (2012) (noting an increase in employer monitoring of employee social media from 27.4% in 2011 to 35.8% in 2012).
mobile through smartphones, tablets, and the like, employers must adapt to the fact that most employees use these devices during work for personal purposes.\(^3\)

According to a recent survey by Neilsen, smartphones account for around 64% of all mobile phones in the United States and 80% of Americans who bought a new phone recently bought a smartphone.\(^4\) A similar study by Pew showed that 56% of all adult Americans are using smartphones.\(^5\) The information flow generated by the explosion of social media has dramatically changed how humans interact with each other, including within the workplace. In the employment context, a 2011 study by the Society for Human Resource Management (“SHRM”) shows that, of those surveyed, close to 70% of companies operating in the United States utilize social media in some form,\(^6\) including screening potential job candidates.\(^7\) And, according to SHRM’s 2012 report, nearly 39% of employers surveyed monitor employee social media usage on company-owned computers and/or hand-held devices and nearly 33% have disciplined employees for improper social media use.\(^8\) The same report also found that nearly sixty percent of employers do not have a formal social media policy.\(^9\) According to one survey, one in ten young Americans between the age of 16-24 are losing potential job offers because of comments or pictures on their online and social media profiles.\(^10\) A 2013 study by CareerBuilder revealed that 39% of surveyed employers screen potential hires using social media, and nearly the same amount -- 43% -- found information that caused them not to hire a particular

\(^3\) SILKROAD, SOCIAL MEDIA AND WORKPLACE COLLABORATION 9 (2012) (“60% of workers . . . check personal social media more than once a day on their mobile devices; three out of four workers check once a day or more.”)


\(^7\) SOC’Y FOR HUMAN RES. MGMT., SHRM SURVEY FINDINGS: THE USE OF SOCIAL NETWORKING WEBSITES AND ONLINE SEARCH ENGINES IN SCREENING JOB CANDIDATES (Aug. 25, 2011).

\(^8\) SOCIETY OF HUMAN RESOURCE MANAGEMENT, SHRM SURVEY FINDINGS: AN EXAMINATION OF HOW SOCIAL MEDIA IS EMBEDDED IN BUSINESS STRATEGY AND OPERATIONS (Jan. 2012).

\(^9\) Id.

As for use of social media by employees, yes, employees access social media at work and post information about work on social media, and have been disciplined for both.\(^\text{12}\)

Regardless of whether monitoring email and Internet usage, social media, cell phones and pagers, or utilizing GPS satellite tracking, employers are using policy and technology to manage productivity and protect resources. Employers addressing issues associated with technology in the workplace should, however, be aware of certain privacy rights of their employees. Both public and private sector employees have certain expectations of privacy in their persons and effects. These expectations are protected to some degree by various legal provisions, including the U.S. Constitution, state constitutions or statutes where applicable, and common law.

**B. Federal Protections**

1. **Protections Under United States Constitution**

   Typically, constitutional rules are not applicable to employees in the private sector absent state action. Accordingly, for example, searches of private-sector employees’ offices, lockers, purses, briefcases, and electronic messages are generally permissible. Nevertheless, principles developed in the public sector cases sometimes provide limited guidance to the private sector.\(^\text{13}\)

   The expanded protections afforded to public-sector employees by federal and state constitutions, however, means public-sector employers have additional considerations when dealing with employees’ social media use.\(^\text{14}\) Such considerations include free speech and association, unreasonable searches and seizures, and substantive and procedural due process

---


\(^{12}\) In fact, a 2011 survey indicates that over 40% of organizations have disciplined employees for activity on Facebook, Twitter, and/or LinkedIn, SOCIAL MEDIA AND COMPLIANCE, HEALTH CARE COMPLIANCE ASSOCIATION & THE SOCIETY OF CORPORATE COMPLIANCE AND ETHICS 6 (Feb/March 2011). This is nearly double the response rate from 2009.

\(^{13}\) See, e.g., Muwonge v. Eisenberg, No. 07-C-0733, 2008 WL 753898, at *11 n.6 (E.D. Wis. Mar. 19, 2008) (employee could make a state statutory-based claim for invasion of privacy where employer entered his office, opened his mail, and removed personal items, and noting that constitutional law in the public sector was informative in interpreting plaintiff’s reasonable expectation of privacy); K-Mart Corp. Store No. 7441 v. Trotti, 677 S.W.2d 632, 636–37 (Tex. Ct. App. 1984) (award of $100,000 in exemplary damages for common law invasion of privacy upheld where store management gained access to employee’s locker, locked by employee’s own padlock, and searched her purse and personal effects).

\(^{14}\) Although generally outside the scope of this article, it should be noted that public schools may be liable for statutory and constitutional claims from students stemming from the use of social media by other students or administrators. See, e.g., Wolfe v. Fayetteville, Ark. Sch. Dist., 600 F. Supp. 2d 1011 (W.D. Ark. 2009) (refusing to dismiss several claims against a school district in part because of a Facebook page created by school that contained “harassing and threatening posts”).
a. First Amendment

Public employers are prohibited from retaliating against an employee’s constitutionally protected speech. Spanierman v. Hughes, in which the federal court addressed this issue in the context of speech on a social networking site, provides a good overview of how courts approach First Amendment issues related to social media postings. There the teacher’s Myspace page contained inappropriate pictures as well as facilitated communication between the teacher and his students about non-school-related items including “what [students] did over the weekend at a party, or about their personal problems.” The school district eventually decided to not renew plaintiff’s contract, and the plaintiff sued alleging several claims, including First Amendment retaliation.

The first issue relating to plaintiff’s First Amendment claim was “whether the Plaintiff expressed his views as a citizen, or as a public employee pursuant to his official duties.” Under Garcetti v. Ceballos, public employees who make statements pursuant to their official duties are not speaking as citizens for the purposes of the First Amendment and thus are not entitled to its protection. In Spanierman, the court found that the plaintiff’s Myspace page was not made pursuant to his official duties -- “[t]here [was] no indication in the record that the [p]laintiff, as a teacher, was under any obligation to make the statements he made on MySpace” -- and thus Garcetti did not apply.

In order for a public employee to make out a prima facie case of retaliation based on the First Amendment, the employee must show that: (1) his speech was of a public concern; (2) he suffered an adverse employment action; and (3) there was a causal connection between the speech and the adverse employment action. The court concluded that most of the plaintiff’s Myspace posts and communications were not of a public concern, but found that a poem

15 See, e.g., Sutton v. Bailey, 702 F.3d 444 (8th Cir. 2012) (university that terminated employee for statements on Facebook did not deny employee of pre-termination due process); Byrnes v. Johnson Cnty. Cmty. Coll., No. 10-2690, 2011 WL 166715, at *3 (D. Kan. Jan. 19, 2011) (reinstating dismissed nursing student who had posted pictures of a placenta on her Facebook page because, among other things, she was given permission to take the pictures and because “[t]he appeal process provided to [p]laintiff was in no way a fair and unbiased opportunity for the students to fully present their case before a neutral and unbiased arbitrator”).
17 Id. at 298.
18 Id. at 299.
19 Id. at 309.
21 Id. at 424.
22 576 F. Supp. 2d at 309.
23 Id. at 308
showing his opposition for the Iraq War “could constitute a political statement.”

In the end however, the court found that there was no causation between plaintiff’s posting of his Iraq war poem and his adverse action. The plaintiff also brought a “freedom of association” claim as well, which the court rejected by finding that plaintiff’s Myspace page was not an “organization” for the purposes of advocating a public concern, and even if it were, he could not establish causation.

In Bland v. Roberts, the trial court held that merely “liking” a Facebook post “is insufficient speech to merit constitutional protection.” There, a deputy sheriff “liked” the Facebook page of a person running against the current sheriff. After the election, the sheriff decided not to retain several employees, and many sued alleging that the sheriff had retaliated against them for their support of his opponent. Rejecting the deputy sheriff’s claim that clicking Facebook’s “like” button triggered First Amendment protection, the court found that “[i]n cases where courts have found that constitutional speech protections extended to Facebook posts, actual statements existed within the record.”

The court continued:

No such statements exist in this case. Simply liking a Facebook page is insufficient. It is not the kind of substantive statement that has previously warranted constitutional protection. The Court will not attempt to infer the actual content of [the deputy sheriff’s] posts from one click of a button on [the opponent’s] Facebook page. For the Court to assume that the Plaintiffs made some specific statement without evidence of such statements is improper. Facebook posts can be considered matters of public concern; however, the Court does not believe Plaintiff[ ] Carter . . . ha[s] alleged sufficient speech to garner First Amendment protection.

On appeal, however, the Fourth Circuit reversed the lower court’s decision. Accepting the deputy sheriff’s claim that clicking Facebook’s “like” button triggered First Amendment protection, the Fourth Circuit found that liking the page qualified as speech and expressing support for something through the like button was “itself a substantive statement.”

According to the Fourth Circuit:

---

24 Id. at 310–11.
25 Id. at 313. See also Curran v. Cousins, 509 F.3d 36 (1st Cir. 2007) (correction officer’s posts on a website were of public concern, but no violation of First Amendment); Beyer v. Duncannon Borough, No. 1:09-CV-1398, 2012 WL 4506044 (M.D. Pa. Oct. 1, 2012) (police officer spoke as a private citizen about a public concern when he posted online commentary discussing the negative impact of the public body’s decision to remove certain rifles from service).
26 Id. at 310-11
28 Id. at 603.
29 Id. at 604.
30 Bland v. Roberts, 730 F.3d 368, 386 (4th Cir. 2013).
In sum, liking a political candidate’s campaign page communicates the user’s approval of the candidate and supports the campaign by associating the user with it. In this way, it is the Internet equivalent of displaying a political sign in one’s front yard, which the Supreme Court has held is substantive speech.  

The Court also noted that it was irrelevant to the First Amendment analysis that the sheriff’s actions were performed through a single mouse click rather than by typing a message. Several other courts have examined employee free speech rights under the First Amendment
with similar results.\textsuperscript{33} Therefore, although the First Amendment’s free speech protection applies to public employees, not all speech by public employees related to the workplace is constitutionally protected speech. Speech that is of a personal concern and outside the individual’s official job duties is not protected.

\textsuperscript{33} See, e.g., Dible v. City of Chandler, 515 F.3d 918, 927 (9th Cir. 2008) (police officer who was terminated for operating a sexually explicit website featuring pictures and videos of his wife did not have a viable First Amendment claim because his “activities . . . did not contribute speech on a matter of public concern”); Velazquez v. Autonomous Municipality of Carolina, No. 11-1586, 2012 WL 6552789 (D.P.R. Dec. 14, 2012) (plaintiff stated First Amendment retaliation claim for Facebook comments criticizing her employer, including the commissioner and department were “making decisions that jeopardized the smooth and efficient operations of the Municipal Police . . . putting in harm’s way the life of fellow officers” and posting pictures of a fellow employee sleeping on the job); Idaho State Univ. Faculty Ass’n for Preservation of First Amendment v. Idaho State Univ., No. 4:12-cv-00068, 2012 WL 1313304 (D. Idaho Apr. 17, 2012) (no violation of First Amendment where public employer prevented employees from “utilizing university-university and university-controlled listserv to distribute email communications which are at odds with positions taken by the university administration”); Yoder v. Univ. of Louisville, No. 3:09-CV-00205, 2012 WL 1078819 at *8 (W.D. Ky. Mar. 30, 2012), aff’d 526 F.App’x 537, (6th Cir. 2013) (student who posted patient information on her Myspace page in violation of confidentiality agreement not entitled to bring First Amendment claim based on her right to publish information on the Internet); Gresham v. City of Atlanta, No. 1:10-CV-1301, 2011 WL 4601020, at *2, *5 (N.D. Ga. Sept. 30, 2011) (plaintiff’s Facebook post criticizing an Atlanta police investigator for visiting a relative that he had arrested and “obstructing” his investigation was a matter of public concern because it raised issues concerning “the integrity of the law enforcement services,” but under Pickering v. Bd. of Educ., 391 U.S. 563, 88 S. Ct. 1731 (1968), was outweighed by the police department’s “interest in investigating workplace misconduct internally, in maintaining unity and discipline within the police force, and in preserving public confidence in its abilities” and thus defendants were entitled to summary judgment on plaintiff’s First Amendment retaliation claim), adhered to on reconsideration, 2012 WL 1600439 (N.D. Ga. May 7, 2012), affirmed on appeal, No. 12-12968, --- Fed.App’x ---, 2013 WL 5645316 (11th Cir. 2013); Snyder v. Millersville Univ., No. 07-1660, 2008 WL 5093140 (E.D. Pa. Dec. 3, 2008) (denying injunction sought by student teacher whose Myspace page contained pictures of her as a “drunken pirate,” leading to her not completing a student teaching practicum because, in part, she admitted that her postings related only to “personal matters” not matters of public concern); Mattingly v. Milligan, 4:11CV00215, 2011 WL 5184283 (E.D. Ark. Nov. 1, 2011) (denying defendant’s motion for summary judgment in First Amendment retaliation case where plaintiff was terminated after posting to Facebook about her concerns over the loss of her co-workers’ jobs because the posts were of a public concern and not subject to the Pickering balancing test, and finding that plaintiff’s supervisor was not entitled to qualified immunity); Richerson v. Beckon, No. C07-5590, 2008 WL 833076, at *4 (W.D. Wash. Mar. 27, 2008) (school district’s involuntary reassignment of a teacher due to comments made on her blog did not violate First Amendment because comments were not of a public concern). But see Greer v. City of Warren, No. 1:10-cv-01065, 2012 WL 1014658 (W.D. Ark. Mar. 23, 2012) (display of confederate flag on police officer’s Myspace page is protected speech); Love v. Rehfeld, 946 N.E.2d 1 (Ind. 2011) (email sent by firefighter supporting political candidate was protected public-employee speech); Navab-Safavi v. Broad. Bd. of Governors, 650 F. Supp. 2d 40 (D.D.C. 2009) (employee who was terminated because of a YouTube video protesting the Iraq War sufficiently pled proper First and Fifth Amendment claims to survive defendant’s motion to dismiss), aff’d, 637 F.3d 311 (D.C. Cir. 2011).
As with other constitutional rights, in some situations, an employer’s interests may outweigh an employee’s right to free speech. In *Shepherd v. McGee*, the plaintiff worked as a case worker for child-protective services investigating reports of child abuse and neglect. If she determined that a home was unsafe, she would assist the district attorney’s office petition for protective custody, by testifying in court. The plaintiff had a private Facebook page, on which she identified her job and employer, but no disclaimer indicating that posts were her own opinions. Her Facebook friends included a judge, deputy district attorneys, defense attorneys and law-enforcement officials. She was discharged for posting several negative comments on her private Facebook page about clients who drove luxury vehicles or had expensive home-entertainment systems and for her proposed “rules for society,” which included:

1. If you are on public assistance, you may not have additional children and must be on reliable birth control . . .
2. If you’ve had your parental rights terminated by DHS, you may not have more children . . .
3. If you are on public assistance, you may not own a big flat screen television; . . .
4. If you physically abuse your child, someone should physically abuse you.

Dismissing the plaintiff’s First Amendment claims, the court explained that even if the plaintiff’s speech was constitutionally protected as a matter of public concern, her employer’s interests outweighed hers. There were legitimate concerns that the plaintiff’s Facebook posts would be subject to discovery and that they would have to be disclosed in physical abuse cases. In addition, the posts could be used against her when testifying, harming the credibility and neutrality required of a case worker, and rendering her useless as a witness.

---

35 Id. at *6.
36 Id. at *3.
37 Id. at *3. See also *Gresham v. City of Atlanta*, No. 12-12968, ---Fed.App’x---, 2013 WL 5645316 (11th Cir. 2013) (affirming dismissal of police officer’s First Amendment claim, where evidence demonstrated that officer’s Facebook posts accusing fellow officers of unethical conduct would have a “natural tendency to endanger the spirit de corps and good working relationships amongst officers” and disrupt the legitimate interests of the department”); *Duke v. Hamil*, No. 1:13-cv-1663, 2014 WL 414222 (N.D. Ga. Feb. 4, 2014) (dismissing First Amendment claim of deputy police chief who posted on his private Facebook page that “It’s time for the second revolution,” shortly after the November 2012 presidential election, because of potential and/or actual disruption caused by plaintiff’s posts); *Graziosi v. City of Greenville*, ---F. Supp. 2d---, No. 4:12-cv-68, 2013 WL 6334011 (N.D. Miss. Dec. 3, 2013) (dismissing First Amendment claim of officer who complained on Facebook page of then-mayor that chief of police did not send police officer representatives to the funeral of an officer killed in the line of duty, because the comments were not about a matter of public concern and, even if they were, the chief’s interest in maintaining his authority and preserving close working relationships outweighed any constitution protection).
Another First Amendment consideration is whether an enacted law or public employer’s policy effectively chills a public employee’s right to free speech. For example, in 2011, Missouri passed a law requiring each school district to “develop a written policy concerning teacher-student communication and employee-student communications.”38 The law prohibited teachers from having “a nonwork-related website that allows exclusive access with a current or former student.”39 A Missouri teacher filed a putative class action alleging that this law was unconstitutional because it was a prior restraint on speech and was overbroad and vague.40 In August of that same year, a Missouri state court entered a preliminary injunction blocking the law’s implementation, finding that the law “would have a chilling effect on speech.”41 The Missouri legislature subsequently repealed this portion of the law.42

b. Fourth Amendment

The Fourth Amendment to the U.S. Constitution protects privacy, in part, by prohibiting those acting under government authority from conducting unreasonable searches and seizures. Generally, a search is “unreasonable” where an employee’s reasonable expectation of privacy in the object searched outweighs the government-employer’s need to conduct the search and obtain information. For public employers, therefore, the Fourth Amendment is a real concern. Damages for those found liable for violating an employee’s Fourth Amendment rights include punitive damages under 42 U.S.C. § 1983 and the Fourth Amendment itself.43 When determining whether a public employee’s right of privacy has been violated, courts will use the “reasonable expectation of privacy” standard derived from Fourth Amendment cases such as O’Connor v. Ortega.44 In O’Connor, the Supreme Court held that privacy protections will be determined by “balancing the invasion of the employee’s legitimate expectation of privacy against the government’s need for supervision, control, and the efficient operation of the workplace.”45 Although the Court in O’Connor failed to produce a majority opinion providing clear guidance, several propositions were set forth providing an analytical framework for lower federal courts to follow when trying to determine whether a public employer’s justification for and method of carrying out a search outweighs an employee’s privacy interest in his offices and files. These propositions are as follows:

38 S.B. 54, 2011 Leg. (Mo. 2011).
39 Id.
42 MO. REV. STAT. § 162.069. See also Gattuso v. Cnty. Of Gloucester, No. 1:13-cv-00092 (D.N.J. 2013) (complaint alleging county’s Social Networking/Media Policy is so overbroad that it chills constitutionally protected speech).
45 Id. at 718.
A public employee can have a reasonable expectation of privacy in his or her workplace. One’s expectation of privacy, however, may be reduced by “actual office practices and procedures, or by legitimate regulation.”

Balancing “employees’ legitimate expectations of privacy against the government’s need for supervision, control, and the efficient operation of the workplace.”

Considering the burdens that a warrant requirement would place on a public employer, employer intrusions on public employees’ protected privacy interests “should be judged by the standard of reasonableness under all the circumstances.”

When balancing an employer’s interests in efficiency and regulating employee conduct against employee’s expectation of privacy: (a) consider whether search was initially justified by reasonable suspicion that search would turn up evidence of what searchers were seeking; and (b) the scope of the search must not go beyond that justified by the initial reason for searching.

In short, there are three primary considerations that must be kept in mind when determining whether a search of a public employee’s workplace is permissible under the Fourth Amendment:

1. whether the employee has a reasonable expectation of privacy in the thing to be searched;
2. the employer must have a reasonable, work-related need or suspicion to search; and
3. the scope of the search must not exceed what is necessary to investigate the employer’s need or suspicion.

In City of Ontario v. Quon, the Supreme Court applied the O’Connor principles to examine the extent of a public employee’s right to privacy as it relates to electronic communications and modern technology in the workplace. Quon, an officer and member of the City of Ontario Police Department’s (“OPD”) SWAT team, was provided a two-way pager by the City of Ontario (“City”). Under OPD’s policies, pagers were not to be used for personal communications, the City reserved the right to monitor all electronic activity, and employees

---

46 Id. at 717.
47 Id. at 719–20.
48 Id. at 725–26.
49 Id. at 726.
51 Id. at 2624–25.
were informed that they should not have any expectation of privacy when using electronic resources.\textsuperscript{52}

Even though the OPD had a policy that all text messages were subject to monitoring, Quon’s supervisor assured Quon and some additional officers that he would not enforce the policy of inspection, and Quon paid overage fees for texts beyond the limit allotted by the City’s contract.\textsuperscript{53} After several months, Quon’s supervisors decided to audit the pager messages to determine whether officers were paying extra for work-related texts or personal texts. The audit included a review of the text messages, which showed that many of Quon’s messages were personal, and he was disciplined for violating OPD policy.\textsuperscript{54} He and three other officers sued under the Fourth Amendment.

Overturning the Ninth Circuit, the Supreme Court held that the search of the text messages was reasonable and did not violate the Fourth Amendment. In so ruling, the Court first expressed concern over broadly defining privacy expectations as they relate to electronic equipment in the workplace, stating that “[the] judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear.”\textsuperscript{55} Therefore, rather than issuing a broad holding as to the extent of employee privacy rights in the workplace with respect to employer-provided electronic devices, the Court instead rested its holding on more narrow grounds.

In so doing, the Court made three assumptions before arriving at its holding: (1) that Quon had a reasonable expectation of privacy in the text messages sent on the employer-provided pager; (2) that the police department’s viewing of the transcript constituted a search under the Fourth Amendment; and (3) that the standards applicable to a search of a government employee’s office apply equally to the search of a government employee’s employer-provided electronic device.\textsuperscript{56} The majority found that police department’s search was justified because there were “reasonable grounds for suspecting that the search [was] necessary for a noninvestigatory work-related purpose.”\textsuperscript{57} Next, the Court determined that the scope of the search was reasonable because reading the transcript of his messages was an efficient way to determine if Quon had been using his electronic device for personal use and the search was restricted to a two-month period of time.\textsuperscript{58} The Court also noted that it was unreasonable for Quon to believe that his personal communications on an employer-provided device would be immune from an audit, regardless of whether his supervisor assured him of privacy.

\textsuperscript{52} Id. at 2625.
\textsuperscript{53} Id. at 2625–26.
\textsuperscript{54} Id. at 2626.
\textsuperscript{55} Id. at 2629.
\textsuperscript{56} Id. at 2630.
\textsuperscript{57} Id. at 2631 (quoting O’Connor, 480 U.S. at 726).
\textsuperscript{58} Id. at 2631.
Therefore, the Court found that even assuming Quon had a reasonable expectation of privacy in his text messages, and that City’s review of the text messages constitute a search under Fourth Amendment, the search was reasonable under principles in O’Connor because it was motivated by a legitimate work-related purpose and was not excessive in scope.\(^{59}\)

It is likely only a matter of time before the Supreme Court provides guidance regarding the Constitution’s privacy expectations in this digital age.\(^{60}\)

c. Fifth Amendment

The Fifth Amendment privilege against self-incrimination protects an individual from being compelled to give information that may be used against him later in a criminal

\(^{59}\) Id. at 2633. See also, Cunningham v. New York State Dep’t of Labor, 997 N.E.2d 468, (N.Y. Ct. App. 2013) (attaching a GPS device to a Department of Labor employee’s personal car was a search within meaning of the state and federal constitutions that was within the “workplace” exception to search warrant requirement, however, the GPS tracking was unreasonable in scope because it included non-work and vacation time).

\(^{60}\) Cf. United States v. Jones, 132 S.Ct. 945, 957 (2012) (Sotomayor, J., concurring) (“[I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. . . . I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year.”) (internal citations omitted); United States v. Young, No. 2:12-cr-00502, 2013 WL 6665378 (D. Utah Dec. 17, 2013) (rejecting argument that instantaneous nature of email conversation made it more like a face-to-face meeting or phone call, court held that person lost reasonable expectation of privacy in sent email once it reached intended recipient); Chaney v. Fayette Cnty. Pub. Sch. Dist, No. 3:13-cv-00089, --- F. Supp. 2d ---, 2013 WL 5486829 (N.D. Ga. Sept. 30, 2013) (minor student who shared bikini photo with Facebook friends and their friends lacked reasonable expectation of privacy needed to support Fourth Amendment claim against school district that publicly shared the photo); Murphy v. Spring, No. 13-CV-96, 2013 WL 5172951 (N.D. Okla. Sept. 12, 2013) (public school supervisory personnel’s access and use of an employee's private email account to find evidence to use against her in an administrative proceeding gave to claim under Fourth Amendment because her reasonable expectation of privacy was violated). In re Applications for Search Warrants for Information Associated with Target Email Address, Nos. 12-MJ-8119, 12-MJ-8191, 2012 WL 4383917, at *5 (D. Kan. Sept. 21, 2012) (“an individual has a reasonable expectation of privacy in emails or faxes stored with, sent to, or received through an electronic communications service provider”) (citing U.S. v. Warshak, 631 F.3d 266 (6th Cir. 2010)); State of New York v. Harris, 949 N.Y.S.2d 590. (N.Y. Crim. Ct. 2012) (no violation of Fourth Amendment where court enforced subpoena to Twitter, stating “[t]here is no reasonable expectation of privacy for tweets that the user has made public”); Hardy et al v. Shuren, No. 1:11-cv-01739 (D.D.C. Jan. 25, 2012) (complaint filed by several Food and Drug Administration scientists alleging, inter alia, violation of the Fourth Amendment when court ordered the FDA to install spyware to monitor the employees’ private email accounts like Gmail and Yahoo!); cf State v Roden, 279 P.3d 461 (Wash. Sup. Ct. 2012) (by sending text messages, an individual gives implicit consent to the interception of those messages under Washington law).
It is well settled that government employers cannot use threat of termination of employment to compel employees to incriminate themselves.

d. Ninth and Fourteenth Amendment

Public employees have implied constitutional rights to privacy that have been interpreted by the U.S. Supreme Court as falling within the “penumbra” of several constitutional amendments. Two types of privacy interests have been interpreted as falling within the “zone of privacy” protected by the Ninth or Fourteenth Amendment: (1) the individual interest in avoiding disclosure of personal matters, and (2) the interest in making important, personal decisions.

Employees have asserted the former interest in challenging employers’ inquiries for types of information, such as financial or medical. The latter interest typically involves challenging an employer’s policies that interfere with employee’s personal life outside of work.

In NASA v. Nelson, the Supreme Court in 2011 considered the former constitutional right to informational privacy, which was mentioned over thirty years ago in Whalen v. Roe and

See U.S. Const. amend. V.

See Garrity v. New Jersey, 385 U.S. 493, 87 S. Ct. 616 (1967) (Fifth Amendment privilege of police officers was violated when they were interrogated about an alleged conspiracy to fix traffic tickets, were warned that their answers could be used against them in a criminal proceeding, and were told they had the right to remain silent but, if they used the right, would be subject to termination); see also Uniformed Sanitation Men Ass’n, Inc. v. City of New York, 392 U.S. 280, 88 S. Ct. 1917 (1968) (discharge of city employees for refusal to sign waivers of immunity before grand jury or for invoking their constitutional privilege against self-incrimination before investigation commissioner was violative of constitutional privilege).


See Amadio v. Skovira, 191 F. Supp. 2d 898 (N.D. Ohio 2002) (information regarding hours city employee worked at part-time job for private employer did not implicate fundamental or traditional right to privacy, and, thus, supervisor did not violate employee’s due process right to privacy under Fourteenth Amendment by obtaining such records without employee’s permission, where supervisor did not seek or obtain any information regarding employee’s financial information, credit history, or other financial records); see also Thomas v. Carrasco, No. 1:04-cv-05793, 2010 WL 4024930, at *3 n.5 (E.D. Cal. Oct. 13, 2010) (discussing disagreement among the circuits as to whether there is a constitutional right to privacy in medical records).

See, e.g., Sylvester v. Fogley, 465 F.3d 851 (8th Cir. 2006) (even assuming a police officer had a substantive right of privacy for engaging in off-duty sexual activity with a crime victim, the police department did not infringe this right because the conduct was job-related and it had compelling reasons to prohibit such conduct). See also section on Off-Duty Conduct, below.
Nixon v. Administrator of General Services. In Nixon, employees of companies working under contracts with NASA alleged that NASA’s background checks -- which inquired into, among other things, drug use or treatment for drug use, and solicited information from references on the subject’s honesty and integrity, as well as other general conduct, use of intoxicants, finances, and mental health -- violated their constitutional right to informational privacy.

Finding that these inquiries did not violate any informational privacy employees may have, the Court stated: We assume, without deciding, that the Constitution protects a privacy right of the sort mentioned in Whalen and Nixon. We hold, however, that the challenged portions of the Government’s background check do not violate this right in the present case. The Government’s interests as employer and proprietor in managing its internal operations, combined with the protections against public dissemination provided by the Privacy Act of 1974, 5 U.S.C. § 552a, satisfy any “interest in avoiding disclosure” that may “arguably ha[ve] its roots in the Constitution.”

In rejecting the argument that the government had a constitutional burden to use the least restrictive method possible to elicit the information, the Court reasoned that the open-ended nature of the questions was reasonably aimed at identifying who would faithfully conduct the government’s business. Further, questions related to drug use and counseling for drug use were reasonable follow-ups to one another and were related to the government’s purpose.

In all three cases where the U.S. Supreme Court discusses the constitutional right to informational privacy, the Court has found that the requests for information did not violate such a right because of sufficient statutory safeguards to protect the individual’s privacy interest.

66 NASA v. Nelson, 131 S. Ct. 746 (2011). In Whalen, the Court upheld a New York law permitting the collection of names and addresses of persons prescribed dangerous drugs, finding that the statute’s “security provisions,” which protected against “public disclosure” of patient information, 462 U.S. at 600–01, were sufficient to protect a privacy interest “arguably . . . root[ed] in the Constitution.” Id. at 605. In Nixon, the Court upheld a law requiring former President Nixon to turn over his presidential papers and tape recordings for archival review and screening, concluding that the federal act at issue, like the statute in Whalen, had protections against “undue dissemination of private materials.” 433 U.S. at 458.


68 131 S. Ct. at 752–54.

69 Id. at 751.

70 The Court also held that there was no risk of public disclosure due to statutes such as the Privacy Act, 5 U.S.C. § 552a.

71 131 S. Ct. at 759–60.

72 Although not an employment case, in People v. Holmes, No. 12-cr-1522, 2013 WL 6059218 (Colo. Dist. Ct. Nov. 7, 2013), the court denied Aurora Colorado shooting suspect James Holmes’ motion to suppress dating site records and profile information from AdultFriendFinder.com and Match.com because Holmes failed to demonstrate a subjective or reasonable expectation of privacy in the content of his profiles. Applying the Holmes decision to the employment context, it is quite possible that courts will similarly be reluctant to find an expectation of privacy in information employees willingly and voluntarily place online, even if the information is as non-public as subscription records.
2. Protections Under Federal Statutes

a. Electronic Communications Privacy Act

Congress’s first attempted to regulate the interception and access of employee email when it passed the Electronic Communications Privacy Act of 1986.\(^\text{73}\) This legislation was enacted to make the already existing Federal Wiretap Act\(^\text{74}\) applicable to newly emerging communication devices. The ECPA carries criminal penalties and provides a civil cause of action against persons who violate it.\(^\text{75}\) Among the provisions of the ECPA, Title I is commonly known as the “Federal Wiretap Act,” and Title II is commonly known as the “Stored Communications Act.”

(i) Title I: Federal Wiretap Act

The Federal Wiretap Act prohibits the interception of electronic mail without the authorization of one of the parties to the communication.\(^\text{76}\) It defines unlawful “interception” as “the acquisition of the contents of any wire, electronic or oral communication through the use of any electronic, mechanical or other device.”\(^\text{77}\) Under the definition of “electronic, mechanical or


\(^{74}\) 47 U.S.C. § 605.

\(^{75}\) Criminal penalties for violations of the ECPA include a fine of up to $500 and up to five years’ imprisonment for Title I violations, and a fine of up to $250,000 and up to one year imprisonment for Title II violations. 18 U.S.C. §§ 2511(4)(a)–(b), 2701(b). The double-jeopardy clause prevents conviction for both Titles. See United States v. Moriarty, 962 F.Supp. 217 (D. Mass. 1997). Civil penalties for Title I violations are $100 per day for each interception, or $10,000. 18 U.S.C. § 2520(c)(2)(B). There is a $1,000 civil penalty floor for Title II violations. Id. § 2707. Punitive damages are permitted under both Titles for willful violations. Id. § 2520.

\(^{76}\) See 18 U.S.C. § 2511(1).

other device,” unless an employer has set up some “device” (for example, software) to access messages in transit, the Federal Wiretap Act is likely inapplicable.

Viewing Internet postings or webpages such as Facebook and Myspace pages would likely not constitute “interception.” For example, in Konop v. Hawaiian Airlines, Inc., an airline pilot sued his employer under the federal Wiretap Act and Stored Communications Act after a company vice president used other employees’ names to log into the pilot’s private website, which contained bulletins critical of upper management. The Ninth Circuit held that even where an employer had accessed the employee’s password-protected website without authorization, the viewing of the website was not an “interception.” In so holding, the court explained that an interception must occur during transmission of information from website to the user and, therefore, viewing the information on a website after the information is transmitted is not interception.

---

79 See, e.g., Wesley Coll. v. Pitts, 974 F.Supp. 375 (D. Del. 1997) (inadvertent glimpse of computer screen not “interception”; screen was medium for information rather than electronic device capable of being used to intercept email within meaning of the act). Compare Crowley v. Cyberstapex Corp., 166 F. Supp. 2d 1263, 1269 (N.D. Cal. 2001) (defendant did not “intercept” electronic communication since the defendant received email on a drive/server and not a “device”), with United States v. Szymuszkiewicz, 622 F.3d 701 (7th Cir. 2010) (defendant who set up a rule to forward emails used three devices: his own computer, supervisor’s computer, and city server). See also Rene v. G.F.Fishers, Inc., 817 F. Supp. 2d 1090 (S.D. Ind. 2011) (employer’s use of keylogger software to record all keystrokes made on employee’s computer did not violate Federal Wiretap Act because “[i]n order to violate the FWA, contemporaneous interception must occur while the transmission is traveling through a system that affects interstate or foreign commerce”) (citing United States v. Barrington, 648 F.3d 1178 (11th Cir. 2011)).
80 Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 873, 874 (9th Cir. 2002). The court found the employer violated the Stored Communications Act when it used log-in information from two employees to gain access to the website. The violation occurred because neither of the employees used the website and under the Stored Communications Act only “users” can authorize third-party access.
81 Id. at 879.
82 Id. at 876–79.
Other cases are in line with Konop's reasoning.\footnote{See, e.g., Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107 (3d Cir. 2003) (employer did not "intercept" email within meaning of act where employer searched its email server and found email that showed employee was engaged in acts of disloyalty against employer; Wyatt v. City of Barre, 885 F. Supp. 2d 682 (D. Vt. 2012) (no interception for "replaying a legally recorded message"); Larson v. Liberty Mut. Fire Ins. Co., No. 11-00272, 2012 WL 93181 (D. Haw. Jan. 10, 2012) (employee’s email stored on an Internet service provider was not intercepted in “transmission” when messages were downloaded from the account); cf. Ehling v. Monmouth-Ocean Hosp. Serv., 872 F. Supp. 2d 369 (D.N.J. 2012) (employer did not violate the analogous state Wiretap Act where the employer accessed post-transmission stored information on employee’s private Facebook page containing disparaging remarks about patients through another employee’s Facebook account). But see United States v. Szymuszkiewicz, 622 F.3d 701 (7th Cir. 2010) (finding “interception” where an employee created a rule on his supervisor’s Microsoft Outlook email account to forward a copy of her emails to his account because the server intercepted the emails in transmission).}

(ii) Title II: Stored Communications Act

The Stored Communications Act\footnote{Pub. L. No. 99-508, tit. II, 100 Stat. 1848 (1986) [hereinafter SCA].} prohibits unlawful access to stored email.\footnote{18 U.S.C. § 2701(a).} It defines electronic storage to include “any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof and any storage of such communication by an electronic communication service for purposes of backup protection of such communication.”\footnote{18 U.S.C. § 2510(A)–(B).}

Generally, the SCA prohibits individuals from intentionally accessing stored electronic information without authorization.\footnote{18 U.S.C. § 270(a)(1). See, e.g., Borchers v. Franciscan Tertiary Province of Sacred Heart, 962 N.E.2d 29 (Ill. App. Ct. 2012) (an employer who accesses an employee’s personal electronic communication may be liable under the SCA if the requisite “intent” is present).} Courts have found that accessing information in a personal
restricted communications area can violate the SCA.\textsuperscript{88} For example, in \textit{Pietrylo v. Hillstone Restaurant Group},\textsuperscript{89} an employee set up a Myspace group that was accessible only to certain individuals and specifically not to the restaurant’s management. Upon pressure from a manager, one of the group members gave up her password to the manager, and the employee was eventually terminated because of information on the Myspace page.\textsuperscript{90} A jury found that the employer had violated the SCA for accessing the site without permission and that the act of pressuring one of the employees to give up her password was malicious, exposing the employer to punitive damages.\textsuperscript{91} It should be noted that in this case, the jury found that the employer did not violate the employee’s common law right to privacy.\textsuperscript{92} Such claims are usually state and fact specific, but query whether using improper means to obtain access to a restricted website constitutes an unlawful invasion of privacy or for public employers, a violation of the Fourth Amendment.

Contrasting \textit{Pietrylo} is the Fifth Circuit decision in \textit{Garcia v. City of Laredo, Texas}.\textsuperscript{93} In \textit{Garcia}, the employer terminated the employee for violating police department rules and regulations based upon images and text messages retrieved from her personal cell phone.\textsuperscript{94} The employer obtained these images and text messages when a police officer’s wife removed the employee’s cell phone from an unlocked locker at work, reviewed the cell phone’s contents, and then turned over the cell phone to the employer believing that she had discovered evidence of violations of police department police.\textsuperscript{95} Arguing that her cell phone was a “‘facility’ in which electronic communication is kept in electronic storage in the form of text messages and pictures

\textsuperscript{88} See \textit{Joseph v. Carnes}, No. 1:13-cv-02279, 2013 WL 2112217 (search of companies,’ owners’ and employees’ emails by another one of the owners by simply following the steps required to access the email server may nonetheless have violated the SCA) (N.D. Ill. May 14, 2013); \textit{Doe v. City & Cnty. of San Francisco}, 835 F. Supp. 2d 762 (N.D. Cal. Dec. 13, 2011) (searching through an employee’s personal electronic mailbox when left open on a company-owned computer may constitute “access” in violation of SCA); \textit{Maremont v. Susan Fredman Design Grp.}, No. 10 C 7811, 2011 WL 6101949, at *5–*6 (N.D. Ill. Dec. 7, 2011) (employee may bring an SCA claim against her employer for exceeding authority by accessing personal Facebook and Twitter accounts without permission); see also \textit{Shefts v. Petrakis}, No. 10-cv-1104, 2011 WL 5930469, at *5–*6 (C.D. Ill Nov. 29, 2011) (hiring a third party to access and copy stored electronic communications from an Internet server does not release liability for “access” under the SCA regardless of whether the copied files are opened or read). But cf. \textit{Genworth Fin. Wealth Mgmt. v. McMullan}, No. 3:09-CV-1521, 2012 WL 1078011, at *13–*14 (D. Conn. Mar. 30, 2012) (summary judgment inappropriate in SCA claim by employer against former employee who, after termination, accessed company-owned websites with passwords granted during employment).


\textsuperscript{90} \textit{Id.} at *3.

\textsuperscript{91} \textit{Id.} at *3–*6.

\textsuperscript{92} \textit{Id.} at *1. See also \textit{Rene v. G.F. Fishers, Inc.}, 817 F. Supp. 2d 1090 (S.D. Ind. 2011) (plaintiff sufficiently pled violation of SCA where employer utilized keystroke software to obtain access to plaintiff’s email and personal checking account).

\textsuperscript{93} 702 F.3d 788 (5th Cir. 2012).

\textsuperscript{94} \textit{Id.} at 790.

\textsuperscript{95} \textit{Id.}
stored on the cell phone,” the employee sued her employer for violating the SCA.\textsuperscript{96} In rejecting this argument, the Fifth Circuit noted that the “the relevant ‘facilities’ that the SCA is designed to protect are not computers that enable the use of an electronic communication service, but instead are facilities that are operated by electronic communication service providers and used to store and maintain electronic storage.”\textsuperscript{97} In other words, a “home computer of an end user is not protected by the SCA.”\textsuperscript{98} Even if a cell phone was a facility, continued the court, the text messages and images contained on her cell phone were not in “electronic storage” as this includes “only the information that has been stored by an electronic communication service provider.”\textsuperscript{99} In contrast, reasoned the Fifth Circuit, “[a]n individual’s personal cell phone does not provide an electronic communication service just because the device enables use of electronic communication services.”\textsuperscript{100}

If the foregoing was not confusing enough, there also remains a split of authority regarding the meaning of the second prong of the SCA’s definition of “electronic storage.” Under the second prong, “electronic storage” includes “any storage of such communication by an electronic communication service for purposes of backup protection of such communication.” The issue primarily revolves around whether emails retained on a web-based email service provider’s server are stored in “backup storage” for purposes of the SCA. Recently, in Cheng v. Romo, the court held that emails viewed in a browser distinct from the browser on which the emails were originally viewed are stored in “backup storage” by the web-based server for purposes of the SCA.\textsuperscript{101} In Cheng, the defendant accessed several of plaintiff’s emails that were stored on his Yahoo! Email account, by logging onto his account using his password, viewing the emails on her own web browser and printing the emails.\textsuperscript{102} The defendant argued that at the time she read the emails, they had already been opened by the plaintiff and were not in “electronic storage.”\textsuperscript{103} Disagreeing with the defendant’s argument, the court found that the emails were covered at least by the second prong of the SCA’s definition of “electronic storage” because they were “backup storage.”\textsuperscript{104} According to the court, regardless of the number of

\begin{itemize}
  \item \textsuperscript{96} Id. at 792.
  \item \textsuperscript{97} Id. (citation omitted).
  \item \textsuperscript{98} Id. (citation omitted).
  \item \textsuperscript{99} Id. at 793
  \item \textsuperscript{100} Id. at 793; see also Castle Megastore Group, Inc., v. Wilson, No. CV-12-02101, 2013 WL 672895 (D. Ariz. Feb. 25, 2013) (employee bound by confidentiality agreement did not violate SCA by posting video of confidential company managers meeting on his Vimeo.com account, which shared with others by giving them his login information).
  \item \textsuperscript{102} Id. at *3
  \item \textsuperscript{103} Id. at *1.
  \item \textsuperscript{104} Id. at *2
\end{itemize}
times either party viewed the plaintiff’s email, the Yahoo! Server continued to store copies of those same emails that previously had been transmitted to the parties’ respective browsers.105

The SCA does not, however, protect information that is readily available to the general public. Also, as a cautionary note, some courts have found that while the SCA prohibits unauthorized access of electronic communication service, it does not prohibit the disclosure of any information gleaned from the access, authorized or not.106

(iii) Exceptions to ECPA

There are three exceptions to ECPA that allow an employer to legally intercept an employee’s telecommunication:

(1) the “consent” exception;
(2) the “business” exception; and
(3) the “service provider” exception.

Under the “consent” exception, an employer may monitor any wire, oral, or electronic communication if at least one individual consents to the interception.107 Arguably, “consent” may be obtained by giving employees advance notice of the employer’s monitoring policy.108

The “business” exception permits an employer to intercept communication if done in the ordinary course of business using a qualifying device.109 Under this exception, therefore, an employer may monitor telephone calls, email, and Internet activity as long as such activity is in the ordinary course of business and done either for the purpose of providing the service or protecting its rights or property.110

105 Id. at *3. See also Jennings v. Broome, 133 S.Ct. 1806 (2013) (letting stand decision from South Carolina Supreme Court, which held that opened emails stored on Yahoo’s internet-based email system are not “stored” for purposes of “backup protection.”).
108 See, e.g., Murphy v. Spring, No. 13-CV-96, 2013 WL 5172951(N.D. Okla. Sept. 12, 2013) (public school supervisory personnel’s access and use of an employee’s private email account to find evidence to use against her in an administrative proceeding gave rise to justiciable claim under the ECPA because defendant bears the burden of proving the exception); United States v. Faulkner, 323 F. Supp. 2d 1111 (D. Kan. 2004) (implied consent where individual is on notice of monitoring of all telephone calls); see also Griggs-Ryan v. Smith, 904 F.2d 112 (1st Cir. 1990) (an employee can impliedly consent based on employee’s behavior that manifests acquiescence to monitoring).
110 See, e.g., Anderson v. City of Columbus, Ga., 374 F. Supp. 2d 1240 (M.D. Ga. 2005) (holding that there was a question of fact as to whether it was in the ordinary course of employer’s business to monitor everything employee said while wearing her headset at work).
Importantly for employers, the “service provider” exception permits an entity providing the wire or electronic communications service (for example, email or voicemail) to retrieve information maintained on an entity’s system to protect the employer’s property rights. This exception does not apply, however, where the employer tries to access such a system owned by a third party. Stated differently, an employer can intercept electronic communications from its own email system, but cannot intercept electronic communication from Google or Yahoo!

b. National Labor Relations Act

(i) General Overview

Employers seeking to monitor the electronic activities of its workforce should also be mindful of the National Labor Relations Act. The NLRA provides rights to employees engaged in “concerted activity for the purposes of collective bargaining or other mutual aid or protection. . . .” Section 7 of the NLRA specifically provides:

Employees shall have the right to self-organization, to form, join, or assist labor organizations, to bargain collectively through representatives of their own choosing, and to engage in other concerted activities for the purpose of collective bargaining or other mutual aid or protection, and shall also have the right to refrain from any or all such activities except to the extent that such right may be affected by an agreement requiring membership in a labor organization as a condition of employment as authorized in section 8(a)(3).

Examples of such activity includes communications among employees about wages, hours, and work conditions, regardless of whether the communication occurs within the employer’s facilities. Importantly, the NLRA applies to both unionized and non-unionized settings. The National Labor Relations Board (“NLRB” or “Board”) has stated that “concerted activity” includes individual activity where “individual employees seek to initiate or to induce or to
prepare for group action, as well as individual employees bringing truly group complaints to the
attention of management.Individual activity engaged in solely by and on behalf of an
employee himself or herself -- for example, an “individual gripe” -- is not protected under the
NLRA.

Once concerted activity is found, the analysis turns to whether the activity is protected
under the NLRA. To determine whether employee misconduct during otherwise protected
activity falls outside the protection of the NLRA, the Board’s Atlantic Steel decision requires a
consideration of four factors: (1) the place of the discussion; (2) the discussion’s subject matter;
(3) the nature of the outburst on the part of the employee; and (4) whether the outburst was
provoked by the employer’s unfair labor practice. These factors are intended to permit “some
latitude for impulsive conduct by employees” during protected activity while acknowledging the
employer’s “legitimate need to maintain order.” Statements do not lose the NLRA’s
protection unless they are “so violent or of such serious character as to render the employee unfit
for further service.” For example, in Atlantic Steel, an employee’s comments about a
supervisor asserting that the supervisor was a “lying son of a bitch” or a “mother fucking liar”
were deemed unprotected where they were found to be unprovoked and in a work setting where
the language was not normally tolerated. Other cases, however, have held that employing
satire and irony to mock an employer does not deprive the communication of protection under
the NLRA and that “[u]npleasantries uttered in the course of otherwise protected concerted
activities does not strip away the Act’s protection.”

In addition to precluding employers from taking action against employees for engaging in
protected concerted activity, the NLRA also prevents employers from adopting and
implementing a work rule -- such as a social media rule -- that would “reasonably tend to chill

118 Id.
120 Atl. Steel, 245 N.L.R.B. at 817.
122 Timekeeping Sys., Inc., 323 N.L.R.B. 244 (1997). See also U.S. Postal Serv., 241 N.L.R.B. 389 (1979) (referring to supervisors as assholes); Groves Truck & Trailer, 281 N.L.R.B. 1194 (1986) (employee called the company’s CEO a “cheap son of a bitch”).
123 See Hills & Dales Gen. Hosp. & Danielle Corlis, Case No. 7-CA-53556 (Feb. 17, 2011). In Hills and Dales, an ALJ concluded that several of the employer’s general work rules were overbroad, including that employees “will not make negative comments about our fellow team members and we will take every opportunity to speak well of each other,” and that employees “will not engage in or listen to negativity or gossip [and] . . . that listening without acting to stop it is the same as participating.” Id. at 6-9. Note too that the employer’s discipline of an employee for a Facebook post was used as evidence that the employer enforced these work rules, even though “there [was] no evidence . . . that the remarks that [the employee] made on Facebook were protected by the Act.” Id. at 6 n.5.
employees in the exercise of their Section 7 rights."\textsuperscript{124} For example, in 1998, the NLRB General Counsel issued an opinion indicating that an employer cannot adopt a policy prohibiting all non-business use of email among its employees, because such restrictions would be overly broad and unlawful.\textsuperscript{125} The Board has adopted a two-step test to determine whether a work rule has such an effect.\textsuperscript{126} First, a rule is unlawful if it explicitly restricts section 7 activities.\textsuperscript{127} If the rule does not explicitly restrict section 7 activities, it is unlawful only on a showing that: (1) employees would reasonably construe the language to prohibit section 7 activities; (2) the rule was promulgated in response to union activity; or (3) the rule has been applied to restrict the exercise of section 7 rights.\textsuperscript{128}

Finally, note that the NLRA may also preempt state privacy laws that otherwise provide workers with certain privacy rights.\textsuperscript{129}

(ii) Email/Communication Policies\textsuperscript{130}

Employers wishing to take charge of their electronic communication devices, however, are not without remedy. According to the General Counsel’s Office, a policy that blocks external email for legitimate business reasons or that has reasonable use limitations does not run


\textsuperscript{125} \textit{Pratt & Whitney}, Cases 12-CA-18446, 18722, 18745, 18863, (Feb. 23, 1998).

\textsuperscript{126} \textit{Lutheran Heritage Vill.-Livonia}, 343 N.L.R.B. 646, 647 (2004).

\textsuperscript{127} Id. at 646.

\textsuperscript{128} Id. As another example, in \textit{Allied Aviation Serv. Co. of N.J.}, 248 N.L.R.B. 299 (1980), the Board found that two letters sent to customers by a union member were protected as concerted activity. The Board cited previous case law holding that an employee may properly engage in communication with a third party in an effort to obtain the third party’s assistance in circumstances where the communication was related to a legitimate, ongoing labor dispute between the employees and their employer, and where the communication did not constitute a disparagement or vilification of the employer’s product or its reputation.

\textsuperscript{129} For example, in \textit{Haggins v. Verizon New England, Inc.}, 648 F.3d 50 (1st Cir. 2011), the First Circuit held that the NLRA preempted employee claims brought under the Massachusetts law challenging the employer’s policy of requiring employees to carry cell phones with global position system capability and tracking software.

\textsuperscript{130} Employers should also note that other technology policies may implicate the NLRA. For example, in \textit{Stephens Media, LLC v. N.L.R.B.}, 677 F.3d 1241 (D.C. Cir. 2012), the Court of Appeals for the District of Columbia recently enforced the Board’s decision that employees engaged in protected, concerted activity when they secretly recorded a conversation with a member of management, noting that there is no \textit{per se} rule against the making of secret audio recordings and that determining whether doing so violates the NLRA must be done on a case-by-case approach. Additionally, in \textit{N.L.R.B. v. White Oak Manor}, 452 F.App’x 374 (4th Cir. 2011), the Fourth Circuit enforced the Board’s decision that the employer violated the NLRA by disciplining an employee under its policy that prohibited the taking of pictures inside the facility without prior written authorization because her taking pictures – which purportedly showed the employer was not enforcing the dress code fairly – was protected, concerted activity.
afoul of the law.\textsuperscript{131} In Ocean Spray, the employer maintained a common email distribution address for one of its facilities that enabled it to quickly send emails to all employees working there. Pursuant to the employer’s written policy, employees were prohibited from forwarding external emails to the address because of concerns about Internet viruses. In the policy, the employer stated that its Internet and voicemail were company property and it reserved the right to monitor and audit them without notice. During a subsequent union organizing campaign, a non-employee union organizer sent external emails to the employer’s common email address. One day later, the employer deactivated the address, without warning. The union responded by filing an NLRB charge alleging that the employer’s conduct violated the NLRA. Rejecting this argument, the General Counsel issued an advice memorandum stating that the employer’s concern about computer viruses was a legitimate, nondiscriminatory business reason for deactivating the common email address. Moreover, because the policy pre-dated the union’s organizing campaign, it found that the policy was not a pretext. The General Counsel also pointed out that the union did not have a protected right of access to the employer’s email system.

In Associated Press, the issue was whether the employer’s communications policy violated the NLRA. The policy stated that the employer’s email and the Internet systems were company property that, generally, could be used only for business purposes. An exception, however, was included for “reasonable use” of the electronic systems for non-business purposes, including reasons such as confirming a doctor’s appointment by email or making a quick purchase over the Internet. The employer’s policy was based on efficiency and system capacity considerations. Like in Ocean Spray, the union in Associated Press challenged the legality of the employer’s policy by filing an NLRB charge. Concluding that the charge should be dismissed, the General Counsel advised that the policy did not unlawfully chill legally protected communications because the “reasonable use” exception evidenced the employer’s acceptance of non-business use of its email and Internet systems. The General Counsel also based its decision on the employers legitimate business reasons underpinning the policy.\textsuperscript{132}

The decision in Benson v. Cuevas, 737 N.E.2d 952 (N.Y. Ct. App. 2000) although not an NLRB decision, is also instructive.\textsuperscript{133} In that case, the court affirmed the Public Employee Relations Board’s decision to revoke a union official’s email privileges because the union employee used the email for unauthorized union activities. According to the court, the fact that the employer had an email policy prohibiting unofficial use and had issued the employee warnings supported the employer’s decision to deny him email access. On the other hand, in E.I. du Pont de Nemours & Company, the NLRB concluded that an employer could not enforce its


\textsuperscript{132} But see, Weyerhaeuser Co., 359 N.L.R.B. 138 (2013) (finding that a corporate policy restricting employee’s use of electronic media was lawful but that the company violated the NLRA when it warned union stewards and committee members that they had exchanged an “unacceptable volume” of email during work time.”)

\textsuperscript{133} 293 A.D.2d 927 (N.Y. App. Div. 2002).
no-solicitation rule to deny the union access to its email system because the employer had allowed employees to send riddles and other information that established an inconsistent pattern with restrictions on email imposed to prevent union access.\(^{134}\)

Employees using employer-provided electronic resources to discuss their employers’ vacation policies will almost certainly be found to be engaged in protected “concerted activity.” In *Timekeeping Systems, Inc.*, 323 N.L.R.B. 244 (1997) the NLRB found that email messages between employees discussing terms and conditions of employment are protected “concerted activities” under the NLRA.\(^{135}\) The employee in this case emailed his coworker, criticized a new vacation policy and attempted to get the coworker and others to tell their boss that they did not approve of the new policy.

(iii) Social Media – The So-Called “New Water Cooler”

Over the past few years, the NLRB has placed increased emphasis on the application of labor law to social media.\(^{136}\) The first well publicized complaint filed regarding this issue was filed by the NLRB’s Hartford office on October 27, 2010, against American Medical Response of Connecticut for its decision to terminate an employee who had posted negative remarks about her supervisor on her Facebook page.\(^{137}\) Such comments included referring to her boss as a psychopath, “dick,” and “scumbag.” Other employees then added further comments, including “I am sorry, hon! Chin up!” The company terminated the employee pursuant to its Internet usage policy. Specifically, the company’s employee handbook prohibited employees “from making disparaging, discriminatory or defamatory comments when discussing the Company or the employee’s superiors, coworkers and/or competitors.” American Medical Response’s standards of conduct also prohibited “[r]ude or discourteous behavior to a client or coworker” and the “[u]se of language or action that is inappropriate in the workplace whether racial, sexual or of a general offensive nature.” The employee filed an unfair labor practice charge, claiming that her posting was protected concerted activity under the NLRA and that the company’s Internet usage policy overly broad. Unfortunately for those hoping that a decision in this case would provide some guidance on the issue, the case settled before an administrative law judge could hear it. According to the NLRB’s press release, the terms of the settlement called for the company to “revise its overly-broad rules to ensure that they do not improperly restrict employees from discussing wages, hours and working conditions with coworkers and others

\(^{134}\) 311 N.L.R.B. 893 (1993).

\(^{135}\) 323 N.L.R.B. 244 (1997).

\(^{136}\) According to an August 5, 2011 report issued by the U.S. Chamber of Commerce, the NLRB had reviewed 117 charges, issued 7 complaints and presided over 5 settlement agreements involving social media issues. **Michael J. Eastman, U.S. Chamber of Commerce, A Survey of Social Media Issues Before the NLRB** 2 (Aug. 5, 2011). The U.S. Chamber of Commerce submitted a Freedom of Information Act request to the Board seeking copies of all charges, complaints, and completed settlements related to social media to which the NLRB responded on May 5, 2011. *Id.* at 2 & n.5.

while not at work and that they would not discipline or discharge employees for engaging in such discussions.”

Social media has also been addressed by the NLRB’s Acting General Counsel’s Office. In April 2011, the Acting General Counsel’s Office required Regional Directors to submit all “[c]ases involving employer rules prohibiting, or discipline of employees for engaging in, protected concerted activity using social media, such as Facebook or Twitter” to the General Counsel’s Division of Advice because “of the absence of precedent or because they involve identified policy priorities.” The Acting General Counsel’s office has also published three separate “Report[s] of the Acting General Counsel Concerning Social Media Cases” (“Reports”) in response to “[r]ecent developments in the Office of the General Counsel [that] have presented emerging issues concerning the protected and/or concerted nature of employees’ Facebook and Twitter postings, the coercive impact of a union’s Facebook and YouTube postings, and the lawfulness of employers’ social media policies and rules.”

Published in April 2011, January 2012, and May 2012, the Reports broadly cover whether an employee’s social media use was protected/concerted activity, whether the employer’s social media policy was too broad and thus chilled protected/concerted activity, and whether a union engaged in unlawful conduct by posting interviews with non-union workers about their immigration status on Facebook and YouTube. The following are the key takeaways from the Reports:

1. Employer policies should not be so broad that they prohibit activity protected by the NLRA, such as the discussion of wages or working conditions. Accordingly, employers should coordinate with key stakeholders regarding the legal and business rational for protecting information and regulating conduct on social media so they can properly

---

139 LAFE E. SOLOMON, OFFICE OF GEN. COUNSEL, NLRB, MANDATORY SUBMISSIONS OF ADVICE 1-2 (Apr. 12, 2011).
141 Id. (summarizing fourteen different investigations conducted by the Acting General Counsel’s Office).
144 Cf. Amalgamated Transit Union and Charles Weigand, Case No. 28-CB-78377 (Nov. 28, 2012) (union did not violate NLRA by failing to disavow statements made by members on the union’s Facebook page threatening employees who refused to strike).
define and clarify specific types of information covered and conduct regulated.

2. For employees’ social media activity to fall under the protection of Section 7, there must be evidence of concerted activity related to the terms and conditions of employment;

3. Employees’ comments on social media sites will generally not be protected if they are simply complaints unrelated to working conditions or wages that impact a group of employees;

4. A “savings clause” or “disclaimer” will not cure an otherwise unlawfully overbroad policy; and

5. Employers should review the model policy identified by the Acting General Counsel as lawful.

Practitioners seeking further guidance are encouraged to review these three Reports as they provide several fact specific examples of what the General Counsel’s Office believes to be proper and improper employer conduct. The Reports also provide significant discussion as to how specific language in employer policies – confidentiality provisions, for example – may chill Section 7 rights.\(^ {145} \) Notably the May 2012 report contains an entire social media policy that the Acting General Counsel considers to be lawful under the NLRA.

(a) Guidance from the Board

The Board has issued six decisions -- detailed below -- that provide guidance to employers seeking to regulate employee conduct on social media. Though the decisions are the first time the Board has weighed in on the issue, the decisions should come as no surprise given the Acting General Counsel’s activity as well as the fact that several Administrative Law Judges have also examined the extent to which: (1) employees may engage in protected, concerted

---

activity using social media;\textsuperscript{146} and (2) employer policies may be so overly broad so as to chill

\textsuperscript{146} ALJ Orders Examining Employee/Employer Conduct: In re Richmond District Neighborhood Center, 20-CA-091748 (Nov. 5, 2013) (dismissing complaint filed by employees that posted on Facebook that he would have “crazy events” at work without permission, play loud music and get artists to place graffiti on walls, do “cool shit” and let the employer figure it out, and have parties all year and field trips all the time, because employer received grants and funding from government and private donors and reasonably believed that the Facebook comments jeopardized its program’s funding and the safety of the youth it serves); Pier Sixty, LLC and Hernan Perez and Evelyn Gonzalez, Case Nos. 2-CA-068612, 2-CA-070797 (April 18, 2013) (employer violated Section 8(a)(1) for firing employee who posted on Facebook “‘Bob is such a NASTY M***** F*****R don’t know how to talk to people!!!!! F**k his mother and his entire f*****g family!!!! What a LOSER!!!! Vote YES for the UNION.”); Miklin Enters., Inc. d/b/a Jimmy John’s and Indus. Workers of the World, at 1, Case Nos. 18-CA-19707, 18-CA-19727, 18-CA-19760 (Apr. 20, 2012) (employer violated NLRA when (1) co-owner encouraged union members on a “Anti-Union Facebook page” to take down posters complaining about the employer’s sick leave policy and (2) assistant manager encouraged employees to contact one of the union employees and “let him know how they feel” because “[b]y encouraging other employees and managers to harass [the union member] for activities that were protected, as well as some that were arguably unprotected. [The] posts on Facebook condoned such harassment.”); Three D, LLC and Jillian Sanzone and Three D, LLC v. Vincent Spinella, Case Nos. 34-CA-12915, 34-CA-12926 (Jan. 3, 2012) (employer violated NLRA (1) by discharging two employees who had participated in Facebook conversations with customers, current employees and a current employee – including one who just “liked” posts – concerning the employer’s tax withholding and accounting practices and (2) by threatening to bring a defamation lawsuit against the employees).
Section 7 rights.\textsuperscript{147}

\textsuperscript{147} ALJ Orders Examining Policies: Boch Imports, d/b/a Boch Honda, 1-CA-83551 (Jan. 13, 2014) (finding employer’s social media policies prohibiting discourteous behavior, disclosing information about other employees, engaging in activities that would have a negative impact on the business, using company logos for any reason, violated Act an required a remedy, even where employer had already revised its policies and distributed a new handbook correcting the offending provisions); UPMC and SEIU Healthcare Pennsylvania, CTW, CLC, Case No. 06-CA-081896 (April 19, 2013) (employer’s policy was unlawfully overboard by (1) requiring written consent to use websites or social media that “describe any affiliation with [the employer] . . . disparage or misrepresent [the employer] or make false or misleading statements regarding [the employer] or to use [the employer]’s logos or other copyrighted or trademarked materials” and (2) prohibiting employees from transferring “sensitive, confidential, and highly confidential information” without written approval); Dish Network Corp. and Comm’n Workers of America and Eric Sutton, Case Nos. 16-CA-62433, 16-CA-66142, 16-CA-68261 (Nov. 14, 2012) (employer’s social media policy violated the NLRA because it: (1) prohibited employees from making “disparaging or defamatory comments about [the employer];” and (2) prohibited employees from engaging in “negative electronic discussion during ‘Company time’”); Echostar Tech., LLC and Gina M. Leigh, Case No. 27-CA-066726 (Sept. 20, 2012) (reviewing several employer policies – including the employer’s social media policy – and concluding that, among other things, (1) the employer’s policy prohibiting “disparaging comments about EchoStar, its employees, officers, directors, vendors, customers, partners, affiliates, or our or their, products/services” was overly broad; (2) the employer’s statement that “[s]hould a conflict arise between a EchoStar policy and the law, the appropriate law shall be applied and interpreted so as to make the policy lawful” did not “save” otherwise unlawful policies; and (3) the employer’s policy that prevented employees from using social media with Company resources or on company time was unlawful); General Motors, LLC and Michael Anthony Henson, Case No. 07-CA-53570 (May 30, 2012) (reviewing employer’s social media policy and finding that the following policies violated the NLRA: (1) requiring employees to not reveal “non-public” company information including “any topic related to the financial performance of the company,” “information that has not been disclosed by the authorized person in public form,” and personal information regarding any employee; (2) requiring an employee to not post any information “when in doubt about whether the information you are considering sharing falls into one of the above categories”; (3) requiring that employees obtain permission when quoting someone else; and (4) requiring employees to get permission before posting any photos, video, quotes, or personal information of anyone other than the employee); G4S Secure Solutions (USA) Inc. and International Union, Security, Police and Fire Professionals of America, Case No. 28-CA-23380, at 1 (March 29, 2012) (employer’s policy regulating use of “Photographs, images and videos of . . . employees in uniform” was not unlawfully overbroad where it “only apply[ed] to posting photographs of the worksite or uniformed employees on social networking sites” and employer “ha[d] legitimate reasons for not having pictures of uniformed employees or employees who are at work posted on Facebook and similar sites;” whereas the employer’s policy prohibiting employees from commenting on “work-related legal matters without express permission of the Legal Department” to be overly broad because it “would reasonably be read to prohibit two employees . . . from sending messages to each other about their issues at work and their EEOC and hotline complaints via a social networking site” and would also “prohibit a discussion group among concerned employees on a social networking site.’’): Three D, LLC and Jillian Sanzone and Three D, LLC v. Vincent Spinella, Case Nos. 34-CA-12915, 34-CA-12926 (Jan. 3, 2012) (employer’s Internet/Blogging Policy was lawful as it provided that employees could be disciplined for disclosing “confidential and propriety information” or “engaging in inappropriate discussions about the
On September 7, 2012, the NLRB finally weighed in on the social media discussion and issued its first decision in Costco Wholesale Corp. In Costco, the Board reviewed several policies implicating employee social media use and found that Costco violated the NLRA because these policies were unlawfully overbroad. For example, the Board concluded that several of Costco’s policies governing the disclosure of “confidential” information – including “payroll,” employee contact information, and “all information relating to Costco and its employees” – unlawfully chilled discussions regarding wages, hours, and other terms and conditions of employment.

One of the key policies at issue directly governed electronically posted statements by employees:

Employees should be aware that statements posted electronically (such as online message boards or discussion groups) that damage the Company, defame any individual or damage any person’s reputation . . . may be subject to discipline, up to and including termination of employment.

Finding that this policy violated the NLRA because it was unlawfully overbroad, the NLRB reasoned that “the broad prohibition against making statements that ‘damage the Company, defame any individual or damage any person’s reputation’ clearly encompasses concerted communications protesting the [Company]’s treatment of its employees.” “[N]othing in this rule,” continued the NLRB, “even arguably suggests that protected communications are excluded from the broad parameters of the rule.” The policy did not, for example, “present accompanying language that would tend to restrict its application” to non-protected statements or conduct “that is malicious, abusive, or unlawful.” Accordingly, the NLRB concluded, “employees would reasonably conclude that the rule requires them to refrain from engaging in certain protected communications (i.e., those that are crucial of the [Company] or its agents).”

Whereas most of the Board’s decision in Costco seemed to track the reasoning identified in prior reports from the Acting General Counsel and decisions from Administrative Law Judges, the Board included language that may signal a willingness to consider the argument that a savings clause or disclaimer would be sufficient to cure an otherwise unlawfully overbroad provision:

Indeed, there is nothing in the [electronic post] rule that even arguably suggests that protected communications are excluded from the broad parameters of the

---

rule. In these circumstances, employees would reasonably conclude that the rule requires them to refrain from engaging in certain protected communications (i.e., those that are critical of the [Company] or its agents).

(ii) **Karl Knauz Motors, Inc.**

A few weeks after issuing its decision in Costco, the NLRB issued its second decision regarding social media. On September 28, 2012, the Board issued its decision in Karl Knauz Motors, Inc. d/b/a Knauz BMW, a case that reviewed whether an employee was discharged in violation of the NLRA and whether the employer’s policies were unlawfully overbroad. Specifically at issue in Karl Knauz Motors were two posts on Facebook by a salesperson at a BMW dealership. The first complained about how he thought food provided at a sales event – hot dogs and chips – was inappropriate given the company’s high end clientele and thus affected his potential commission and the second was a post mocking an accident that had occurred at an adjacent but related dealership.

During the administrative hearing, the ALJ found that while the first post regarding the food was protected concerted activity despite the fact that no other employees commented on his post, the employer took no action against the employee because of this post. Rather, the ALJ concluded that employer discharged the employee because of his second Facebook post regarding the accident. Since the post regarding the accident was not related to any employees’ terms and conditions of employment, the ALJ concluded the employer did not violate the NLRA when it discharged him.

Agreeing with the ALJ, the Board adopted the ALJ’s finding that the employer lawfully discharged the employee solely because of his unprotected Facebook postings about the auto accident. Based on this decision, the Board found it unnecessary to pass on whether the employee’s post regarding the food at the sales event was protected. The Board also affirmed the ALJ’s finding that the employer’s “courtesy” rule in its employee handbook was unlawfully overbroad. Among other things, the “courtesy” rule stated that:

> Courtesy is the responsibility of every employee. Everyone is expected to be courteous, polite and friendly to our customers, vendors, and suppliers, as well as to their fellow employees. No one should be disrespectful or use profanity or any other language which injures the image or reputation of the Dealership.

In so holding, the Board reasoned that “employees would reasonably construe the rule’s broad prohibitions against ‘disrespectful’ conduct and ‘language which injures the image or reputation of the Dealership’ as encompassing Section 7 activity, such as employees’ protected statements – whether to coworkers, supervisors, managers, or third parties who deal with the [employer] – that object to their working conditions and seek the support of others in improving them.” Notably, however, citing Costco, the NLRB once again seemed to leave the door open for a

---

149 358 N.L.R.B. 164 (2012).

© 2014 Miller Canfield, Paddock and Stone, P.L.C. All Rights Reserved.
savings clause/disclaimer argument: “there is nothing in the rule, or anywhere else in the employee handbook, that would reasonably suggest to employees that employee communications protected by Section 7 of the Act are excluded from the rule’s broad reach.” Whether the Board ultimately will conclude that a saving’s clause or disclaimer will save an otherwise unlawfully overbroad policy or rule remains unsettled, however.

(iii)  Hispanics United of Buffalo

On December 14, 2012, the NLRB issued its third decision regarding social media and provided specific guidance as to how the NLRB defines protected concerted activity in this social media era. In Hispanics United of Buffalo, the NLRB expressly stated that it will treat employee activity on social media using the same “analytical framework” that has been in place for nearly thirty years. Put another way, the NLRB will not treat social media any differently than other ways in which employees may engage in protected concerted activity.

The employer in Hispanics United of Buffalo, a non-union employer, discharged five employees after the employees made negative comments on Facebook – while off-duty and via their personal computers – about one of their coworkers. The dispute arose after an employee posted a comment on her Facebook page stating that one of her coworkers was complaining that fellow employees were not doing enough and soliciting opinions from her other coworkers. Four coworkers responded, albeit with profanity and sarcasm, defending their job performance and commenting on working conditions. The employer discharged all five employees pursuant to its “zero tolerance” harassment policy.

In adopting the recommendations of an ALJ, the NLRB found that by firing the employees, the employer violated the employees’ right to engage in protected concerted activity. The NLRB held that the posts were protected by the NLRA because the employees were discussing their job performance. In reaching this conclusion, the NLRB reasoned that when the employee stated her concerns and solicited her coworkers views, which were subsequently provided, the employees were “taking the first step towards taking group action to defend themselves against the [coworker’s] accusation [that they were not doing enough].” Whether the original employee intended to voice her complaints was irrelevant, found the NLRB, because the Facebook posts had the clear “mutual aid” objective of preparing coworkers to defend against the complaints. Finally, the NLRB rejected the employer’s argument that its “zero tolerance” anti-harassment policy applied, noting that the comments could “not reasonably be construed as a form of harassment or bullying” under the policy, and even if it did, it could not apply the policy “without reference to Board law.” Accordingly, by discharging the five employees for their Facebook posts, the employer violated the NLRA.

151 Id (citing Meyers I).
152 DirectTV U.S. DirectTV Holdings, LLC, 359 N.L.R.B. 54 (2013) (concluding several policies – including non-social media related policies – chilled employee rights under the NLRA).
Soon after its decision in *Hispanics United of Buffalo*, the NLRB issued another opinion in April 2013 on concerted protected activity and social media. In *Design Technology Group LLC d/b/a Bettie Page Clothing*,153 the NRLB held that an employer violated Section 8(a)(1) by discharging employees who engaged in protected concerted activity on Facebook.

In *Bettie Page Clothing*, employees asked their manager if the store could close an hour earlier because other stores in the area were closing at that time and street people were harassing them from outside the store, which had no security system. The manager said she would discuss the request with corporate, but the issue remained unresolved. Accordingly, on a day the manager was off work, two employees contacted the store’s owner and HR to complain, angering the manager. Subsequently, the two complaining employees, plus a third, posted several messages on Facebook criticizing the manager. One of the employees posted, “Tomorrow I’m bringing a California workers [sic] rights book to work. My mom works for a law firm that specializes in labor law and BOY will you be surprised by all the crap that’s going on that’s in violation.”

Another employee, who was friends with the manager, showed the manager the posts. The manager contacted HR and six days later, discharged the two complaining employees. The third employee was fired later, allegedly because of attendance issues.

Among other things, the employer claimed that the posts were not intended for the employees’ mutual aid and protection, but rather were a scheme to make comments on Facebook in order to set up their firing. In support, the employer testified that the employees started laughing when they were told they were fired and posted on Facebook “Muhahahaha! ‘So they’ve fallen into my crutches [sic].’” In adopting the ALJ’s opinion, the NRLB rejected the employer’s claim that the workers “schemed to entrap” the company into firing them and the defense lacked any evidence or legal support. The ALJ also noted that the company shifted explanations as to why the employees were fired. The ALJ concluded – and the Board agreed – that the firing violated the employees’ Section 8(a)(1) rights. The NLRB also noted that while the communications were continuations of protected activity that began offline – the postings would have been protected by Section 7 “in and of themselves.”

Just one week later, the NLRB issued its opinion in *Target Corporation* providing additional guidance on social media policies and protected concerted activity.154 Target had a “Use Technology Appropriately” policy that said, “If you enjoy blogging or using online social networking sites such as Facebook and YouTube, ... please note there are guidelines to follow if

---

you plan to mention Target or your employment with Target in these online vehicles[.]” The policy said employees who blogged or used social media should not release “confidential guest, team member or company information,” must “[c]learly distinguish yourself from Target” so as to avoid appearing as a spokesperson, and cannot harass or make threats to guests or team members.

In adopting the ALJ’s recommendations, the NLRB ruled that the policy restricted the employees’ right to share information with other workers regarding their wages, hours and other conditions of employment. The NLRB did not elaborate on its decision.

(vi) New York Party Shuttle, LLC

A week later, the NLRB issued its opinion in New York Party Shuttle LLC.155 The NLRB upheld the ALJ’s decision finding that New York Party Shuttle unlawfully discharged an employee when it failed to give him any tour assignments after he publicized his union organization activities and criticized the company’s employment practices in emails and Facebook postings to third parties. The NLRB ruled that the communications constituted union activity, even if they were directed to tour guides of other New York City companies because they were “obvious continuation of [his] prior organizational activity, activity which was known to [the employer].” Before the activity leading to his discharge, the employee had sent out previous emails to the employer’s guides and other guides in New York City detailing concerns about existing terms and conditions of employment, listing the benefits of unionization and talking about approaching the NLRB. Interestingly, the employee sent the emails in question to employees of a competitor from which he had resigned; not New York Party Shuttle’s employees. His Facebook postings, however, were made to a page accessible to all New York city tour guides. The ALJ and NLRB rejected the company’s contention that the communications were not protected activity because they were libelous because they were largely true. Consequently, the Board ordered the employer to reinstate the employee and awarded him back pay.

(vii) World Color (USA) Corp.

Whether an employer’s suggestion that it knew about an employee’s Facebook posts permits an inference of protected activity of unlawful retaliation was squarely at issue in World Color (USA) Corp.156 In that case, the employee at a commercial printing and publishing company claimed that his shift was reassigned in retaliation for comments he posted on his Facebook page. Specifically, he claimed that he criticized the company and discussed the union in response to another individual’s post. When he asked his supervisor why he was being reassigned, the supervisor allegedly responded that reassignments were not always about production and asked the employee if he thought that management was unaware of his Facebook posts. Based on that evidence, the ALJ found that since the employee could reasonably believe

156 360 N.L.R.B. slip op. 37 (Feb. 12, 2014).
that his reassignment was retaliation for his Facebook posts, which the ALJ concluded were protected activity, the supervisor’s statements unlawfully interfered with his Section 7 rights.

Reversing the ALJ, the NLRB first found that the record failed to demonstrate what the employee posted on Facebook, whether the posts were protected and that the supervisor’s comments could reasonably be understood to be in response to the alleged protected concerted activity. According to the Board, the contents of the Facebook posts were undocumented and were merely based on the employee’s unspecific recollections. And, whereas the supervisor’s alleged statement may have implied the company did not like the employee’s posts, the Board could not infer a causal connection. In short, the Board would not allow an employer’s ambiguous statement to bridge the various evidentiary gaps.

(viii) Amalgamated Transit Union

Recently, the Board had the opportunity to review the obligation to disavow threats or other statements that arguably violate the NLRA on a proprietary social media page by persons who are not agents of the social media pages’ owner. In Amalgamated Transit Union, the NLRB agreed with the ALJ that the union did not violate the NLRA by failing to remove certain threatening comments related to protected concerted activities from its Facebook page, because the individuals who posted the comments were not union agents. The charging party was an employee who filed an unfair labor practice charge against the union in response to certain threatening comments that appeared on the union’s Facebook page. Employees who refused to participate in the union’s strike against the employer were threatened with less favorable representation, physical harm and violence. Affirming the ALJ’s conclusions, the Board held that the union did not violate the NLRA by failing to remove or disavow the Facebook comments because they were posted by individuals who were not agents of the union. Two members further found that the comments would not have been unlawful threats, even if union agents made them.

(b) Other Guidance

In addition to those materials referenced above, additional guidance may also be gleaned from recent Advice Memorandums that have been published by the NLRB’s Division of

157 360 N.L.R.B. slip op. 44 (Feb. 12, 2014).
Advice. In one case, *Hoodview Vending Co.*, the NLRB held that social media discussions between coworkers over things like wages, work schedules and job security involved subjects of such mutual workplace concern that they inherently constituted concerted activity, whether or not they contemplated group action. This expansive holding has been limited by at least one advice memorandum. In *Tasker Healthcare Group*, the NLRB issued an advise memorandum distinguishing *Hoodview Vending*’s concept of “inherent concerted activity” by concluding that an employee’s profanity-laced comments about the company and her supervisor in a private group message on Facebook in which she allegedly told her supervisor to “back the freak off” and suggested that the employer could “FIRE ME … Make my day” constituted unprotected “boasting and griping.” At the same time, in *Butler Medical Transport, LLC and William Norvell*, the Division of Judges ruled that a hospital violated the NLRA when it fired an employee who contacted another former employee on Facebook and commented that she should contact an attorney because the post was protected activity.

Another important area of interest is whether taking and posting photographs or video taken on company premises can be banned through a social media policy. These cases are particularly important in light of recent cases at fast food chains such as Taco Bell and Subway where pictures were posted online of employees licking taco shells or rubbing genitals on a foot long bread. In one advice memo, a policy prohibiting “photographs or video of the Company’s premises, processes, operations, or products, which includes confidential information owned by the Company, unless you have received the Company’s prior written approval” is overly restrictive on an employees’ right to engage in protected concerted activity. The memo continued:

We further find that the portion of the rule prohibiting employees from photographing or videotaping the Employer’s premises is unlawful as such a prohibition would reasonably be interpreted to prevent employees from using social media to communicate and share information regarding their Section 7

---


159 359 N.L.R.B. 36 (2013)


161 *Butler Medical Transport, LLC and William Norvell*, 5-CA-94981, 97854, 2013 WL 4761153 (Sept. 4, 2013)

activities through pictures or videos, such as of employees engaged in picketing or other concerted activities.\textsuperscript{163}

On the other hand, more recently, in \textit{Whole Food Market, Inc.}, an NLRB ALJ concluded that a policy prohibiting recording conversations with a tape record or other recording device (including a cell phone or any electronic device), without prior approval, did not violate the rights of employees to engage in protected concerted activity.\textsuperscript{164} The ALJ found that the only activity forbidden by rule was recording conversations or activities, not employees freely speaking to each other and engaging in Section 7 conversations.\textsuperscript{165} More rulings are expected from the NLRB on workplace photography and recording, as cases such as \textit{Giant Foods} and \textit{Whole Food Market, Inc.} work their way through the agency.

Finally, the Board has yet to address whether an employer’s social media policy is a mandatory subject of bargaining. That said, “[i]t is well established that work rules that can be grounds for discipline are mandatory subjects of bargaining”\textsuperscript{166} and therefore social media policies are likely “other terms and conditions of employment” that must be bargained.\textsuperscript{167} The NLRB has, however, found on procedural grounds that an employer violated the NLRA for discharging an employee for posts made on the employee’s Facebook page.\textsuperscript{168} Further it should be noted that just because an employee’s social media postings reference union activity does not

\textsuperscript{163} \textit{Id.} at *8

\textsuperscript{164} \textit{Whole Foods Market, Inc.}, 01-CA-096965 (Oct. 3, 2013)

\textsuperscript{165} \textit{Id.}

\textsuperscript{166} \textit{In re King Soopers, Inc.}, 340 N.L.R.B. 628, 628 (2003).

\textsuperscript{167} \textit{In Children’s Hospital of Pittsburgh of UPMC}, the employer settled a charge where the union alleged that the employer implemented a social networking policy without prior notice to the union and without bargaining over the conduct covered by the policy or the conduct’s effects. No. 06-CA-37047 (settlement agreement approved Jan. 21, 2011). On March 27, 2012, attorneys for the United Food and Commercial Workers Local 1500 filed a charge against Stop & Shop Supermarkets alleging, among other things, that the employer violated the NLRA by “unilaterally promulgating, implementing and maintaining a new ‘social media policy’ without first bargaining with the Union.”

\textsuperscript{168} \textit{In Bay Sys Tech., LLC}, 357 N.L.R.B. 28 (2011), an employee posted a comment on his Facebook page complaining about the employer not issuing employee paychecks on time. (entering default judgment after employer failed to answer complaint). A week later a local newspaper published the Facebook comment and the employer allegedly retaliated by sending an email to its employees: (a) “express[ing] disappointment” that the employees chose to complain on Facebook and to the local paper; (b) noting that the employees breached their nondisclosure agreements; (c) threatening legal action; (d) implying that the employees would be discharged unless they explained their actions and their intentions for their further with the employer; and (e) suggesting that this conduct would be used in their performance evaluations. Note that because the employer failed to answer this complaint, the NLRB assumed the facts to be undisputed.
necessarily mean the employer may then use such a reference to remove a state court action to federal court under the preemption doctrine.  

Employers should take extreme care when taking an adverse action against an employee for his/her usage of social media, especially where that usage relates in any way to work.

c.  Computer Fraud and Abuse Act

The Computer Fraud and Abuse Act “CFAA” prohibits “knowingly and with intent to defraud, access[ing] a protected computer without authorization, or exceed[ing] authorized access, and . . . obtain[ing] anything of value.”  

It provides both civil and criminal penalties for accessing or obtaining information from a protected computer without authorization and provides a private cause of action against anyone who, knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access and by means of such conduct furthers the intended fraud.

Some employers have brought claims under this statute against employees or former employees who used company computers to misappropriate (download or send) confidential property or information.  

At the same time, however, a growing number of federal courts have limited the use of the CFAA by employers to pursue employees who depart with sensitive

---

169 See Moore v. Highlands Hosp. Corp., No. 11-131, 2011 WL 5598907 (E.D. Ky. Nov. 17, 2011) (remanding removed case back to state court involving the termination of an employee who started a Facebook page titled “Nurses for lower patient-to-nurse ratios” and encouraged other nurses to join the largest union of registered nurses because the employee only brought state law claims, was not a union member, did not work under the terms of a collective bargaining agreement, and did not base her claims on an alleged violation of any labor agreement and stating that the state court should determine whether plaintiff should have brought her claims to the NLRB under Garmon preemption).


171 Employers should note that the Cloud Computing Act of 2012 is currently pending in the U.S. Senate and would extend the CFAA to cover cloud computing. S.B. 3569 112th Cong. (2012).

172 See Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage Inc., 119 F. Supp. 2d 1121 (W.D. Wash. 2000) (employer could sue former employee and employee’s new employer for CFAA violations where employee sent emails containing employer’s confidential information and trade secrets to the new employer, a competitor, while still working for the employer); see also Int’l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418 (7th Cir. 2006) (employer had a cause of action under CFAA where former employee deleted files on his company computer before resigning and starting his own competing company). But see Lee v. PMSI, Inc., No. 8:10-cv-2904, 2011 WL 1742028 (M.D. Fla. May 6, 2011) (dismissing employer’s CFAA counterclaim where employer only alleged that former employee accessed personal websites – Facebook, personal email, and news websites – from employer’s computer and not internal employer information that she was not entitled to obtain or alter).
Employers can face challenges in proving: (1) lack of authorization; and (2) damage or loss.

There is a split among courts as to the issue of “without authorization.” For example, in *LVCR Holdings LLC v. Brekka*, where an employee copied files and emailed them to a personal email account and the employer did not maintain guidelines prohibiting employees from emailing work documents to non-work computers, the Ninth Circuit found that the CFAA claim failed. It reasoned that the employee was authorized access to the proprietary material at issue because he was given access to computer systems while employed, and the employer did not have a policy that rescinded this authorization. The Ninth Circuit revisited *Brekka* in *United States v. Nosal*, clarifying “that ‘exceeds authorized access’ in the CFAA is limited to violations of restrictions on access to information, and not restrictions on its use.” In so holding, the Ninth Circuit reasoned that the legislative intent and plain meaning of the CFAA was “to punish

---

173 See *LVCR Holdings LLC v. Brekka*, 581 F.3d 1127 (9th Cir. 2009); see also *Lockheed Martin Corp. v. Speed*, No. 6:05-CV-1580-ORL-31, 2006 WL 2683058 (M.D. Fla. Aug. 1, 2006) (rejecting employer’s claim against former employees who downloaded and copied the plaintiff’s confidential information before resigning and going to work for a competitor because employee did not access the computers “without authorization” and did not exceed “authorized access”).

174 581 F.3d 1127 (9th Cir. 2009). See also *Clarity Servs., Inc. v. Barney*, 698 F. Supp. 2d 1309 (M.D. Fla. 2010) (similar).

175 676 F.3d 854, 864-65 (9th Cir. 2012) (affirming dismissal of CFAA count against former employee who conspired with co-workers who were still employed by the employer to obtain contact lists and other confidential information to start a competing business because the former employee’s accomplices “had permission to access the company database and obtain the information contained within”).
hacking—the circumvention of technological barriers—not misappropriate of trade secrets—a subject Congress has dealt with elsewhere.”

On the other hand other courts including the Seventh Circuit, in International Airport Centers L.L.C. v. Citrin, came to a different conclusion as to the application of “without authorization.” In Citrin, an employee accessed his company laptop and deleted the data in it by using a secure-erasure program, which rendered the deleted material irretrievable. The court concluded that employee’s access was “without authorization” at the point “he resolved to destroy files that incriminated himself and other files that were also the property of his employer, in violation of the duty of loyalty that agency law imposes on an employee.” Similarly, the...
Eleventh Circuit, in *United States v. Rodriguez*, held that an employee working for the Social Security Administration who knowingly and repeatedly accessed personal records of several individuals for nonbusiness reasons contrary to organizational policy had “exceeded his authorized access” by violating the employer’s “use” policy, despite being authorized to view and access the information as part of his job duties.\(^{179}\)

Another challenge in bringing a CFAA action is proving that a current or former employee caused loss or damage as contemplated by the Act.\(^{180}\) Many courts have held that trade secret misappropriation or lost revenue alone does not meet the statutory definition of damage, particularly when data is simply accessed and copied but not impaired in any way.\(^{181}\) Employers have been able to use the CFAA to get back laptops from departing employees because the requisite “loss” and “damage” elements of CFAA can be shown.\(^{182}\)

\(^{179}\) 628 F.3d 1258, 1263 (11th Cir. 2010); see also Musket Corp. v. Star Fuel of Okla., No. CIV-11-444-M, 2012 WL 3595048, at *11 (W.D. Okla. Aug. 21, 2012) (no summary judgment on CFAA claim where employee downloaded software onto his company laptop to upload information from the laptop to an online backup drive because employee did not receive permission to download the software and had signed a non-disclosure agreement that prohibited the use or disclosure of any of the employer’s confidential or proprietary information). For more on this circuit split, see Stephanie Green and Christine Neylon O’Brien, *Exceeding Authorized Access in the Workplace: Prosecuting Disloyal Conduct Under the Computer Fraud and Abuse Act*, 50 AM. BUS. L. J. 281.

\(^{180}\) Section 1030(g) of the CFAA provides that a civil action may be brought only if the conduct involves one of the following factors: (I) loss during any 1-year period aggregating at least $5,000 in value; (II) actual or potential modification or impairment of medical examination, diagnosis, treatment, or care; (III) physical injury to any person; (IV) a threat to public health or safety; or (V) damage affecting a computer used by or for an entity of the U.S. Government in furtherance of the administration of justice, national defense, or national security.

\(^{181}\) See Telquest Intern. Corp. v. Dedicated Bus. Sys., Inc., No. 06-5359, 2009 WL 3234226 (D.N.J. Sept. 30, 2009), (holding that “[the plaintiff] does not allege that it suffered a loss of revenue because [its] computer functions were inoperative, but because [it] lost customers as a result of defendants’ business activities. This does not constitute loss under the CFAA.”).

\(^{182}\) See Lasco Foods, Inc. v. Hall and Shaw Sales, Mktg & Consulting LLC, 600 F. Supp. 2d 1045 (E.D. Mo. 2009) (“loss” and “damage” elements shown where employee refused to return computer, deleted company files, and company had to perform forensic investigation to determine what information was deleted); see also Executive Sec. Mgmt. Inc., v. Dahl, 830 F. Supp. 2d 883 (C.D. Cal. 2011) (employer raised a triable issue of fact under the CFAA where employees used “erasure programs” to delete employer’s data off employer’s computers without permission).
d. Other Federal Statutes

Discussion of other federal statutes as related to privacy issues in the workplace regarding specific types of pre-employment screening and employment monitoring are found in section on Pre-Employment Checks below. These statutes include Fair Credit Reporting Act, Employee Polygraph Protection Act, and statutes related to medical information such as American Disability Act of 1990, Health Insurance Portability and Accountability Act of 1996, Family Medical Leave Act, and the Genetic Information Nondiscrimination Act of 2008.

Other statutes implicated by employee use of technology include the Hatch Act and the Fair Labor Standards Act. For example, the U.S. Office of Special Counsel published a “Frequently Asked Questions Regarding Social Media and the Hatch Act” answering several questions concerning federal employee use of social media. As to the Fair Labor Standards Act, non-exempt employees might need to be compensated for accessing company email on a mobile device outside of regularly scheduled working hours. This would include devices owned by the employer, as well as those owned by employees, but used to access the employer’s email system.

C. State Protections

1. Protections Under State Constitutions

Ten state constitutions include an explicit guarantee of privacy: Alaska, Arizona, California, Florida, Hawaii, Illinois, Louisiana, Montana, South Carolina, and

---

184 See, e.g., Allen v. City of Chicago, No. 10 C 3183, 2013 WL 146389 (N.D. Ill. Jan. 14, 2013) (conditionally certifying FLSA claim where plaintiffs alleged that they were “required to use” work issued mobile devices outside of normal working hours without receiving compensation).
185 Alaska Const. art. 1, § 22: “The right of the people to privacy is recognized and shall not be infringed. The legislature shall implement this section.”
186 Ariz. Const. art. II, § 8: “No person shall be disturbed in his private affairs, or his home invaded, without authority of law.”
187 Cal. Const. art. I, § 1: “All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy.”
188 Fla. Const. art I, § 23: “Every natural person has the right to be let alone and free from governmental intrusion into the person’s private life except as otherwise provided herein. This section shall not be construed to limit the public’s right of access to public records and meetings as provided by law.”
189 Haw. Const. art. I, §§ 6 & 7: “The right of the people to privacy is recognized and shall not be infringed without the showing of a compelling state interest. The legislature shall take affirmative steps to implement this right.”
Washington. A select number of states allow employees of private employers to bring privacy claims. For example, California grants constitutional privacy rights to private-sector employees. The California Supreme Court found that California’s constitutional right to privacy applies to private, as well as public, entities. Some states, including Alaska and New

© 2014 Miller Canfield, Paddock and Stone, P.L.C. All Rights Reserved.
Jersey, have deemed their state constitutions to provide a sufficient public policy basis for privacy claims by a private employee.\textsuperscript{197}

Employers should also consult local counsel with respect to the application of additional state constitutional provisions, even those that generally track the U.S. Constitution.\textsuperscript{198}

2. \textit{Protections Under State Statutes}\textsuperscript{199}

a. \textit{Anti-Wiretapping and Monitoring Statutes}

Most states have passed anti-wiretapping laws similar to ECPA that regulate the interception and recording of electronic communications, including telephone calls.\textsuperscript{200} Generally, these laws require the consent of at least one person who is a party to the conversation

\textsuperscript{197} See Hennessy \textit{v. Coastal Eagle Point Oil Co.}, 609 A.2d 11 (N.J. 1992) (privacy may serve as a source of public policy exception to at-will employment, but courts should balance the privacy interests against the interests of the employer); Luedtke \textit{v. Nabors Alaska Drilling, Inc.}, 768 P.2d 1123, 1130 (Alaska 1989) (public policy protecting an employee’s right to withhold private information from his employer exists in Alaska and that violation of that policy “may rise to the level of a breach of the implied covenant of good faith and fair dealing,” which is the basis for the public policy exception to at-will employment).

\textsuperscript{198} See, e.g., Cunningham \textit{v. N.Y. State Dep’t of Labor}, 89 A.D.3d 1347 (N.Y. App. Div. 2011) (public employer that utilized GPS to track plaintiff’s personal car as part of an investigation that the employee was reporting false information as to hours worked and had submitted false vouchers for travel reimbursements did not violate New York’s constitutional guarantee against illegal searches and seizures); Eisenstein \textit{v. Bd. of Trs. of Purdue Univ.}, A5D101205PL00049 (Ind. Cir. Ct. May 7, 2012) (complaint by Purdue professor alleging violation of civil and privacy rights after the university investigated comments he made on Facebook that were critical of Muslims).

\textsuperscript{199} Though outside the scope of this paper, employers should generally be aware of state specific criminal laws that might apply to employees who take or gain access to confidential information. See, e.g., Willoughby \textit{v. State}, 84 So.3d 1210 (Fla. Dist. Ct. App. 2012) (employee violated state statute prohibiting taking trade secret/confidential information from a computer network when she transferred data from employer’s computer system to her laptop for the purposes of working from home even though she acted without a malicious purpose).

\textsuperscript{200} For a recent example of the application of an analogous state law, see Marcus \textit{v. Rogers}, No. L-4477-08, 2012 WL 2428046 (N.J. Super. Ct. App. Div. Jun. 28, 2012) (no violation of New Jersey’s Wiretapping and Electronic Surveillance Control Act – modeled after the SCA – where individual opened, read, and printed out emails from a coworker’s personal email account that was left open on a public computer because the “index” to the coworker’s inbox was left open and no jury could find that the employee “did not know he was exceeding the authorization that was implied by the fact that the index was displayed and the contents of the various emails accessible without use of a password or code.”).
to consent to recording the conversation. Some states provide broader coverage than the ECPA and require the consent of all parties involved.

Monitoring employees by recording telephone conversations or electronic communications, and even participating in social media, is perhaps covered by these statutes, and employers should check their specific state laws.

Some states require employers to notify employees when they conduct electronic monitoring. For example, in Connecticut, each employer who engages in any type of electronic monitoring shall give prior written notice to all employees who may be affected, informing them of the types of monitoring that may occur. Each employer shall post, in a conspicuous place which is readily available for viewing by its employees, a notice concerning the types of electronic monitoring which the employer may engage in. Such posting shall constitute such prior written notice. This law, however, provides several exceptions for the notice requirement, including when the employer “has reasonable grounds to believe the employee is

---

201 Jurisdictions that require consent by one party are Alabama (ALA. CODE § 13A-11-30); Alaska (ALASKA STAT. § 42.210.310); Arizona (ARIZ. REV. STAT. Ann. § 13-3005); Arkansas (ARK. CODE ANN. § 5-60-120; §5-16-101); Colorado (COLO. REV. STAT. § 18-9-303); Delaware (DEL. CODE ANN. tit. 11, § 2402(c)(4)); District of Columbia (D.C. CODE § 23-542); Georgia (GA. CODE ANN. § 16-11-62); Hawaii (HAW. REV. STAT § 803-42); Idaho (IDAHO CODE ANN. § 18-6702); Iowa (IOWA CODE § 727.8); Louisiana (LA. REV. STAT. ANN. § 15:709); Maine (ME. REV. STAT ANN. Tit. 15, § 709); Michigan (MICH. COMP. LAWS § 750.539c); Minnesota (MINN. STAT. § 626A.02); Missouri (MO. REV. STAT. § 542.402); Nebraska (NEB. REV. STAT. § 86-290); New York (N.Y. PENAL LAW §§ 250.001, 250.05); North Carolina (N.C. GEN. STAT. §§ 15A-287; 14-155); Ohio (OHIO REV. CODE ANN. § 2933.52); Oregon (OR. REV. STAT. §§ 165.540, 165.543; 133.005); Rhode Island (R.I. GEN. LAWS §§ 11-35-21; 12-5-1); South Carolina (S.C. CODE ANN. § 17-30-20); South Dakota (S.D. CODIFIED LAWS § 23A-35A-20); Tennessee (TENN. CODE ANN. § 39-13-601); Utah (UTAH CODE ANN. § 77-23a-4); Virginia (VA. CODE ANN. § 19.2-62); West Virginia (W. VA CODE § 62-10-3); Wisconsin (WIS. STAT. § 968.31); Wyoming (WYO. STAT. ANN. § 7-3-701).

202 Consent by all parties is required in California (CAL. PENAL CODE § 647); Connecticut (CONN. GEN. STAT. § 52-570d); Florida (FLA. STAT. § 934.03); Illinois (720 ILL. COMP. STAT. 5/14-1); Maryland (MD. CODE ANN § 10-402); Massachusetts (MASS. GEN. LAWS ch. 272, § 99); Montana (MONT. CODE ANN. § 45-8-213); New Hampshire (N.H. REV. STAT. ANN. § 570-A:2); Pennsylvania (18 PA. CONS. STAT. § 5703); Washington (WASH. REV. CODE § 9.73.030).

203 See, e.g., Sitton v. Print Direction, 718 S.E.2d 532 (Ga. Ct. App. 2011). The employer fired the employee after discovering that the employee was working on the side for a competitor. Upon discovering this, the employer went into the employee’s office and moved the employee’s mouse that was connected to his personal -- not work -- computer. This allowed the employer to view emails showing that the employee was working for a competitor and the employer printed out the emails. Claiming a violation of Georgia’s computer theft, trespass, and privacy laws, the employee sued the employer. Reasoning that the employer had authority to inspect the employee’s personal computer due to the employer’s broad computer usage policy and that the inspection was reasonable in light of the situation, the court affirmed the dismissal of the employee’s state law claims.

204 CONN. GEN. STAT. § 31-48d.
engaged in violating a law.” Additionally, the Connecticut Supreme Court found that the statute
did not create a private right of action.205

Delaware law requires employers who monitor employees’ Internet access, telephone
calls, or email to provide notice to the employees at hiring or before beginning monitoring.206
Employers may provide notice either by posting it electronically so an employee sees it at least
once each day, or by providing a one-time notice in writing, in an electronic record or in another
electronic form, and having it acknowledged by the employee either in writing or electronically.
Unlike the Connecticut law, the Delaware law does not exempt employers from giving notice to
employees when the monitoring of email communications is for purposes of investigating an
illegal activity. As in Connecticut, violation of the statute may result in monetary penalties.

Workplace postings or polices should suffice as notice, but employers should consult
counsel in their state to determine whether they need to comply with state electronic monitoring
statutes.207

b. Password Protection Statutes

Some employers have taken the controversial step of requiring applicants to provide log-
in and password information during the application process. Such practices may also apply to a
company’s employees as well as job applicants.

In 2011, the Maryland Department of Public Safety and Correctional Services suspended
its practice of requiring social media log-in and passwords after receiving a letter from the
American Civil Liberties Union (ACLU).208 The ACLU complained that the requirement
violated an employee’s privacy and was illegal under the Stored Communications Act (SCA) and
Maryland law.209 The ACLU claimed that by requiring log-in and password information for
employment purposes, the department was accessing protected communications without proper

205 In Gerardi v. City of Bridgeport, 985 A.2d 328 (Conn. 2010), the city of Bridgeport monitored the
whereabouts of city fire inspectors with GPS devices in city vehicles without the inspectors’ knowledge.
Some of the fire inspectors became subject to disciplinary actions for improper job performance, first
detected through the use of the GPS. The employees sued under Connecticut’s electronic monitoring act,
but the court held for the city employer since it did not find an express or implicit private right of action
in the statute.

206 DEL. CODE ANN. tit. 19, § 705.

207 A recent Seventh Circuit decision illustrates the intricacies of state electronic monitoring statutes. In
Carrol v. Lynch, 698 F.3d 561 (7th Cir. 2012), the court found that the “fear of crime” exemption to the
Illinois eavesdropping statute applied and thus the employer was not liable for using a recording made by
a coworker’s wife to terminate the employee.

208 Letter from Gary D. Maynard, Secretary, Md. Dep’t of Pub. Safety & Corr. Servs., to Sara N. Love,
President, ACLU of Md. (Feb. 22, 2011).

209 Letter from Deborah A. Jeon, Legal Dir., ACLU of Maryland, to Gary D. Maynard, Secretary, Md.
Dep’t of Pub. Safety & Corr. Servs. (Jan. 25, 2011). The letter also notes that the City of Bozeman,
Montana rescinded a similar policy after public outcry.
authorization. The department subsequently modified its practice to require applicants to “log into their accounts and let an interviewer watch while the potential employee clicks through wall posts, friends, photos and anything else that might be found behind the privacy wall.”

At least thirteen states have passed legislation governing such conduct – Arkansas, California, Colorado, Illinois, Maryland, Michigan, Nevada, New Jersey, New Mexico, Oregon, Utah, Vermont and Washington. Employers conducting business in each of these states should take note of these statutes especially since each takes a different approach to proscribing certain conduct. For example, Maryland’s law generally prohibits employers from either requesting or requiring that an applicant or employee disclose a user name or password to the employer and provides exceptions to employers conducting investigations regarding securities or financial law and regulations and unauthorized downloading of the employer’s proprietary information or financial data. Maryland’s law, however, does not provide for a private cause of action, contains no enforcement language, and does not vest a state agency with responsibility to investigate and enforce the new law. Illinois’ “Right to Privacy in the Workplace Act” initially did not provide any exceptions, including those for investigatory purposes, but only affirmatively stated that the act does not prevent employers from promulgating and maintaining “lawful workplace policies governing the use of the employer’s electronic equipment,” monitoring “usage of the employer’s electronic equipment and the employer’s electronic mail . . . [or] obtaining about a prospective employee or an employee information that is in the public domain . . . .” In August 2013, however, the act was amended to permit employers access to information regarding “professional” social media accounts. “Professional accounts” are those “created, maintained, used, or accessed by a current or prospective employee for business purposes of the employer.” Under the amended act, which took effect on January 1, 2014, employers may request access to a “professional account” when they have a “duty to screen

---

210 Id.
213 MD. CODE ANN., LAB. & EMP. § 3-712 (Md. 2012).
214 820 ILL. COMP. STAT. 55/10 (Ill. 2012). Note that a bill introduced on January 30, 2013 would both broaden this Act with the addition of a retaliation provision, but also provide exceptions for employer investigations and employer-owned devices or accounts. See H.B. 1047, 98th Gen. Assem. (Ill. 2013). See also, H.B. 64, 98th Gen. Assem. (Ill. 2013) (Signed by Governor Pat Quinn on August 2, 2013 limiting the ability of colleges and universities to demand social media account and password information from students).
employees or applicants prior to hiring.” New Mexico’s law only covers access to prospective employee’s social networking accounts.  

Michigan’s Internet Privacy Protection Act (“IPPA”) prohibits employers from requesting that an employee or applicant grant access to, allow observation of, or disclose information that allows access to or observation of “personal internet accounts,” such as Gmail, Facebook and Twitter. Under the IPPA, an employer may not discharge, discipline, fail to hire, or otherwise penalize an employee or applicant declining such requests. There are, however, several noted exceptions.

Utah’s Internet Employment Privacy Act generally track’s Michigan’s IPPA. California’s law expressly allows employers to “request an employee to divulge personal social media [information] reasonably believed to be relevant to an investigation of allegations of employee misconduct, or employee violation of applicable laws and regulations, provided that the social media [information] is used solely for purposes of that investigation or a related proceeding.”

Arkansas, Colorado, Nevada, New Jersey, Oregon and Washington have enacted similar statutes.

In addition, at least thirty-two other states are considering or have considered new or additional legislation governing such practices: Arizona, California, Connecticut, Delaware, Florida, Georgia, Hawaii, Illinois, Iowa, Kansas, Louisiana, Maine, Maryland, Massachusetts, Minnesota, Mississippi, Missouri, Montana, 

216 S.B. 371 (N.M. 2013).
218 H.B. 100 (Utah. 2013).
221 See Arz. S.B. 1411 (2013).
225 See Fla. S.B. 198 (pre-filed 2014).
Employers who require login and password disclosures have also attracted the attention of Congress. Two bills were introduced in 2012 – the Social Networking Online Protection Act and the Password Protection Act of 2012 – the former being reintroduced in 2013. Additionally, Senators Charles Schumer and Richard Blumenthal sent letters to the Equal Employment Opportunity Commission and the U.S. Department of Justice on March 25, 2012 requesting that they investigate whether this practice violates the Stored Communications Act, the Computer Fraud and Abuse Act, and applicable federal anti-discrimination law. To date, neither the EEOC nor the Department of Justice has issued any formal guidance on this issue.

Finally, Facebook’s official position is that requiring the log-in and password disclosure could not only “potentially expose[ ] the employer who seeks . . . access to unanticipated legal liability,” it also is “a violation of Facebook’s Statement of Rights and Responsibilities to share or solicit a Facebook password.”

---

251 See W.V. H.B. 2966 (2013).
Two important rules can be gleaned from the statutes discussed above. First, publicly available social media content is not at issue. The statutes mentioned above do not restrict employer’s ability to rely upon publicly available information. Further, acting on restricted social media content that is voluntarily provided to a coworker is not prohibited by the statutes. In such situations, it is important to document all sources of information that may lead to an adverse employment action in the event of future litigation.

c. **Off-Duty Conduct Statutes**

Employers should be aware that some states have passed “off-duty conduct” statutes. These statutes typically prevent employers from taking an adverse action against employees for otherwise legal conduct when off-duty, such as drinking alcohol, using tobacco products, or participating in a political activity. In California, for example, the off-duty conduct broadly covers all “lawful conduct occurring during nonworking hours away from the employer’s premises” but subsequent court decisions have found that this law does not confer any additional substantive rights but rather protects “recognized constitutional rights.” At the same time, however, they tend to contain broad exceptions -- like creating a material conflict of interest -- so that employers are still able to take some action. For example, Colorado law prohibits an employer from firing an employee “due to that employee’s engaging in any lawful activity off the premises of the employer during nonworking hours . . .” It exempts restrictions relating to *bona fide* occupational qualification (BFOQ) requirements or those aimed at preventing conflicts

---

258 The states that offer some of the broadest protections are California (CAL. LAB. CODE §§ 96(k), 98.6); Colorado (COLO. REV. STAT § 24-34-402.5); New York (N.Y. LAB. LAW § 201-d); North Dakota (N.D. CENT. CODE § 14-02/4-03). At least seventeen states offer protection to tobacco users: Connecticut (CONN. GEN. STAT. § 24-34-402.5); Indiana (IND. CODE § 22-5-4-1); Kentucky (KY. REV. STAT. ANN. § 344.040); Louisiana (LA. REV. STAT. ANN. § 23.966); Maine (ME. REV. STAT. ANN. Tit. 26, § 597); Mississippi (MISS. CODE ANN. § 71-7-33); New Hampshire (N.H. REV. STAT. ANN. § 275:37-a); New Jersey (N.J. STAT. ANN. § 34:6B-1); New Mexico (N.M. REV. STAT. § 41-1-85); Ohio (OH. REV. STAT. § 23-20.10-14); Oklahoma (OKLA. STAT. tit. 40, § 500); Oregon (OR. REV. STAT. § 659A.315); Rhode Island (RI. GEN. LAWS § 23-20.10-14); South Carolina (S.C. CODE. ANN. § 41-1-85); South Dakota (S.D. CODIFIED LAWS § 41-1-85); Virginia (VA. CODE. ANN. §§ 2.2-2902, 15.2-1504); West Virginia (W. VA. CODE § 21-3-19); Wyoming (WYO. STAT. ANN. § 27-9-105). Finally, at least eight states offer protection to those who use “lawful products” (tobacco, alcohol, etc.): Illinois (820 ILL. COMP. STAT. 55/5); Minnesota (MINN. STAT. § 181.938); Missouri (MO. REV. STAT. § 290.145); Montana (MONT. CODE ANN. §§ 39-2-313, 39-2-314); Nevada (NEV. REV. STAT. § 613.333); North Carolina (N.C. GEN. STAT. § 95-28.2); Tennessee (TENN. CODE ANN. § 50-1-304); Wisconsin (WIS. STAT. ANN § 111.321).


260 COLO. REV. STAT. § 24-34-402.5(1).
of interest. 

New York’s law is broader: “[I]t shall be unlawful for any employer or employment agency to refuse to hire, employ or license, or to discharge from employment” because of off-duty conduct including political activities, the legal use of consumable products, legal recreational activities outside of work, and union/civil-service membership. 

Additionally, employers should also take note that state record-keeping statutes with respect to non-employment activities might also apply to information collected on social media sites. For example, section 8 of Michigan’s Bullard-Plawecki Employee Right to Know Act states that:

An employer shall not gather or keep a record of an employee’s associations, political activities, publications, or communications of nonemployment activities, except if the information is submitted in writing by or authorized to be kept or gathered, in writing, by the employee to the employer. This prohibition on records shall not apply to the activities that occur on the employer's premises or during the employee's working hours with that employer that interfere with the performance of the employee's duties or duties of other employees.

Social media sites will likely disclose information concerning “an employee’s associations, political activities, publications, or communications of nonemployment activities.”

---

261 COLO. REV. STAT. § 24-34-402.5(1)(a)–(b). See also Marsh v. Delta Air Lines, Inc., 952 F.Supp. 1458 (D. Colo. 1997) (employer not liable under off-duty conduct law when it terminated employee for writing a letter critical of employer because within the bona fide occupational requirements is an implied duty of loyalty with regard to public communications). But see Watson v. Pub. Serv. Co. of Colo., 207 P.3d 860 (Colo. Ct. App. 2008) (rejecting the Marsh court’s broad interpretation of the exceptions to the Colorado off-duty conduct statute). North Dakota also has a similar exception for preventing conflicts of interest. See Fatland v. Quaker State Corp., 62 F.3d 1070 (8th Cir. 1995) (employer’s decision to terminate employee because employee operated an off-hours competitor fit within statute’s BFOQ and thus was not liable under North Dakota’s off-duty conduct law).

262 N.Y. LAB. LAW. § 201-d(2)(a)–(d).

263 MICH. COMP. LAWS § 423.508(1).
Thus, employers should check their specific state laws concerning off-duty conduct prior using information gleaned from an employee’s social media posting or from other monitoring to take adverse action.\(^{264}\)

d. **Whistleblower Protection Statutes**

Whether an employee’s social media postings trigger whistleblower protections under state statutes is another potential risk. Most whistleblower laws dictate that an employee must “report” violations to “public bodies” or entities. It appears that any whistleblower protection might derive from the extent that an employee posts on social media sites maintained by those to whom the employee would be required to “report.” Conversely, posts generally to the employee’s own social media page will likely not constitute a “report” given the specific “reporting” requirement to “public bodies” or entities.

Because this is a developing area with little applicable case authority, employers are advised to tread cautiously when dealing with potential whistleblowers use of social media sites.

e. **FTC Regulations Regarding Enforcements**

Employers should be on notice of the Federal Trade Commission regulations requiring the disclosure of relationships between “the endorser and the seller of the advertised product that might materially affect the weight or credibility of the endorsement. . . .”\(^{265}\) The regulations provide several hypothetical situations, including one involving social media:

Assume that instead of speaking about the clinic in a television interview, the tennis player touts the results of her surgery -- mentioning the clinic by name -- on a social networking site that allows her fans to read in real time what is happening in her life. Given the nature of the

\(^{264}\) *See also Land v. L’Anse Creuse Pub. Sch. Bd. of Educ.*, No. 288612, 2010 WL 2135356 (Mich. Ct. App. May 27, 2010) (affirming decision by the State Tenure Commission that the school district did not have reasonable and just cause to discharge the plaintiff for pictures taken without her consent at a bachelor/bachelorette party); *In re Jennifer O’Brien*, No. 108-5/11, 2013 WL 132508 (N.J. Super. Jan. 11, 2013) (upholding dismissal of teacher for conduct unbecoming a tenured teacher who posted on Facebook that, among other things, she was “not a teacher—I’m a warden for future criminals”); *Rubino v. City of New York*, 965 N.Y.S.2d (N.Y. App. 2013) (termination of tenured teacher was “shocking to . . . one’s sense of fairness” who “vented” on Facebook about her students with the following post: “After today, I am thinking the beach sounds like a wonderful idea for my 5th graders! I HATE THEIR GUTS! They are the devils (sic) spawn! One of her Facebook friends then posted, ‘oh you would let little Kwame float away!’ to which [the teacher] responded, ‘Yes, I wd (sic) not throw a life jacket in for a million!!’”); *Palleschi v. Cassano*, 102 A.D.3d 603 (N.Y. App. Div. 2013) (upholding dismissal of an EMS employee under state law who posted to Facebook the contents of a 911 caller’s gynecological emergency and her identifying information in violation of department regulations); *In re Cook, Pocatello Sch. Dist. Grievance Panel*, No. 14-03 (D. Ida. 2013) (Idaho school district grievance panel found that discharge for posting Facebook picture of coach’s fiancé touching her covered breast was “unduly harsh and unfair.”).

\(^{265}\) 16 C.F.R. § 255.5.
medium in which her endorsement is disseminated, consumers might not realize that she is a paid
endorser. Because that information might affect the weight consumers give to her endorsement,
her relationship with the clinic should be disclosed.266

D. Common Law Torts

Where an employee may not be able to prove a violation of federal or state statutory law,
an employer may be liable for common law invasion of privacy. In general, there are four
privacy torts: (1) unreasonable intrusion upon another’s seclusion; (2) appropriation of another’s
likeness; (3) unreasonable public disclosure of private facts; and (4) false-light privacy invasion.

The availability of these tort claims depends on the relevant state law and the specific
facts alleged. Of the four privacy torts, unreasonable intrusion upon seclusion is probably the
most relevant to employers. Recently, in Ehling v. Monmouth-Ocean Hosp. Serv., Civ., the
plaintiff sued her employer for invasion of privacy, alleging that her employer gained access to
her private Facebook posts by “coercing, strong-arming and/or threatening” a coworker into
accessing his own Facebook page and showing the employer her posts.267 In dismissing the
claim, the court noted that the employer did not obtain access to the plaintiff’s Facebook page by
logging into her account or asking another employee to log in.268 Rather, the employer was a
passive recipient of information that it did not seek out or request.269 The plaintiff voluntarily
gave information to her Facebook friend.270 Her Facebook friend, in turn, voluntarily gave it to

266 Id. See also Press Release, Fed. Trade Comm’n, Spokeo to Pay $800,000 to Settle FTC Charges
Company Allegedly Marketed Information to Employers and Recruiters in Violation of FCRA (June 12,
2012) (online data broker settled with FTC for, among other things, “deceptively post[ing] endorsements
of [its] services on news and technology websites and blogs, portraying the endorsements as independent
when in reality they were created by Spokeo’s own employees”); Press Release, Fed. Trade Comm’n,
Public Relations Firm to Settle FTC Charges That It Advertised Clients’ Gaming Apps Through
Misleading Online Endorsements (Aug. 26, 2010) (public relations company settled with FTC after
employees “pose[d] as ordinary consumers posting game reviews at the online iTunes store . . . [while]
not disclosing that the reviews came from paid employees working on behalf of the [game] developers”);
Surgery Franchise That Flooded Internet with False Positive Reviews (July 14, 2009) (plastic surgery
company settled with state attorney general where employees published fake, positive reviews about the
company to “trick Web-browsing consumers into believing that satisfied customers were posting their
own stories”).
2013).
268 Id. at *14
269 Id.
270 Id.
the employer. Throughout the document, it is mentioned that whereas the friend’s conduct may have been a “violation of trust,” it was not a violation of privacy.

The tort of intrusion upon seclusion is defined as the intentional intrusion upon the solitude or seclusion of another or his private affairs or concerns that would be highly offensive to a reasonable person. To determine whether an intrusion would be offensive to a reasonable person, courts have examined the degree of intrusion, the conduct and circumstances surrounding the intrusion, and the intruder’s motives and objectives. The key factor, however, is to what extent an employee would have had a “reasonable expectation of privacy” in the particular instance and to what extent intrusion on that expectation of privacy is justified.

Employees have alleged the tort of intrusion, particularly in the context of monitoring by employers and information privacy. It is a difficult claim, however, for employees to successfully assert.

E. Attorney-Client Privilege for Communications via Employer Technology

A new issue confronting counsel and litigants is whether electronic evidence from a party to his or her legal counsel that was created on (or sent from) an organization-provided computer is protected from disclosure by the attorney-client privilege. Perhaps not surprisingly, courts that addressed this issue have reached different conclusions.

1. ABA Guidance on Privilege Issues

In 2011, the American Bar Association issued formal guidance concerning whether an employer’s attorney is required by the Model Rules of Professional Conduct to notify an

---

271 Id.
272 Id. at *14
273 RESTATEMENT (SECOND) OF TORTS § 625B (Supp. 2010).
274 O'Connor, 480 U.S. at 723.
275 See, e.g., Sumien v. CareFlite, No. 02-12-00039-CV, 2012 WL 2579525 (Tex. App. July 5, 2012) (former employee could not show employer intruded on his seclusion by viewing a comment he posted on another former employee’s Facebook wall); Moore v. Univ. Hosp. Cleveland Med. Ctr., No. 1:11-CV-00508, 2011 WL 5554272 (N.D. Ohio Nov. 15, 2011) (employee fired for showing co-workers pornography contained on his personal email had no expectation of privacy to access his personal email account “on a hospital-owned computer sitting in the middle of a hospital floor within the easy view of both patients and other staff-members”). But see Ehling v. Monmouth-Ocean Hosp. Serv., 872 F. Supp. 2d 369 (D.N.J. May 30, 2012) (employee adequately pled invasion of privacy claim where the employer gained access to the employee’s Facebook posts by “coerce[ing], strong-arm[ing], and/or threaten[ing]” a co-worker into accessing his own Facebook page to show the employer’s posts to the employee) (alterations in original); Coughlin v. Town of Arlington, No. 10-10203, 2011 WL 6370932, at *11–*12 (D. Mass. Dec. 19, 2011) (plaintiffs adequately pled claims for invasion of privacy where employer obtained access to one of the plaintiff’s personal email accounts by monitoring the plaintiff’s work email).
employee’s attorney when he/she receives copies of emails the employee sent to his/her attorney via the employer’s email system. Concluding that an employer’s attorney is not required to do so under the Model Rules, the ABA Formal Opinion focused on Rule 4.4(b), which provides that “[a] lawyer who receives a document relating to the representation of the lawyer’s client and knows or reasonably should know that the document was inadvertently sent shall promptly notify the sender.” According to the ABA:

[E]-mails between an employee and his or her counsel are not “inadvertently sent” by either of them. A “document [is] inadvertently sent” to someone when it is accidentally transmitted to an unintended recipient, as occurs when an e-mail or letter is misaddressed or when a document is accidentally attached to an e-mail or accidentally included among other documents produced in discovery. But a document is not “inadvertently sent” when it is retrieved by a third person from a public or private place where it is stored or left.

While noting that some local jurisdictions provide an expansive view of the duty to disclose when “confidential documents are sent intentionally and without permission” and that “other law might prevent the receiving lawyer from retaining and using the materials,” the Formal Opinion finds that Rule 4.4(b) has never been interpreted so broadly to cover this specific situation. Thus, the Formal Opinion concludes that the Model Rules do not require such disclosure, but stresses that both local rules and courts could require such disclosure depending upon the circumstances. Finally, it closes by emphasizing that “[e]ven when there is no clear notification obligation, it often will be in the employer-client’s best interest to give notice and obtain a judicial ruling as to the admissibility of the employee’s attorney-client communication before attempting to use them and, if possible, before the employer’s lawyer reviews them.”

2. Guidance from Courts on Privilege Issues

As demonstrated in the following cases, an employer’s policy plays a significant role in determining privilege issues. These cases -- as well as Formal Opinion 11-460 -- are sure to not be the last on this issue, but at the least, they provide significant guidance to employees and employers in the meantime and could likely be analogized to situations involving accessing similar communications via social media.

277 Id. at 1.
278 Id. at 2.
279 Id. at 2–3.
280 Id. at 3.
281 See e.g., United States v. Finazzo, No. 10-CR-457, 2013 WL 619572 (E.D.N.Y. Feb. 19, 2013) (emails that employee sent to his attorney from work email account were not privileged because there was no expectation of privacy in use of the employer provided email account under its policy which stated that email may be used for company business only and “you should have no expectation of privacy when using the Web/Internet Email. Your use may be monitored and disclosed at anytime without your permission.”).
a. Cases finding communications were privileged

(i) Stengart v. Loving Care Agency, Inc

In Stengart v. Loving Care Agency, Inc., the plaintiff used her employer-provided laptop to send emails via her web-based and password-protected personal Yahoo! account -- not her work-provided account -- to her attorney. Unknown to the plaintiff was the fact that the company’s Internet browsing software automatically made a copy of each page the plaintiff viewed and then stored the page on her computer. Shortly after the plaintiff filed suit, the employer forensically imaged the plaintiff’s hard drive and discovered the emails between the plaintiff and her attorney.

At issue in Stengart was whether plaintiff had an expectation of privacy in her emails and whether plaintiff’s emails were covered by the attorney-client privilege. The court first turned to the company’s policy, which stated:

The company reserves and will exercise the right to review, audit, intercept, access, and disclose all matters on the company’s media systems and services at any time, with or without notice.

... Email and voice mail messages, internet use and communication and computer files are considered part of the company’s business and client records. Such communications are not to be considered private or personal to any individual employee.

The purpose of electronic mail (e-mail) is for company business communications. Occasional personal use is permitted; however, the system should not be used to solicit for outside business ventures, charitable organizations, or for any political or religious purpose, unless authorized by the Director of Human Resources.

In rejecting the employer’s argument that the plaintiff did not have a reasonable expectation of privacy and had thus waived the attorney-client privilege, the court emphasized two specific considerations: (1) “the adequacy of the notice provided by the Policy” and (2) “the important public policy concerns raised by the attorney-client privilege.” To the former, the court quickly determined that the employer’s policy was not clear on the issue and thus plaintiff “did not have express notice that messages sent or received on a personal, web-based email account [were] subject to monitoring if company equipment is used to access the account.” The policy

---

283 Id. at 657.
284 Id. at 659.
285 Id.
also did not warn employees that personal, web-based emails could be forensically retrieved. Finally, the court found the policy to be ambiguous “about whether personal email use is company or private property.”

Turning to the issue of whether the plaintiff’s communications were privileged, the court found that the plaintiff “had a subjective expectation of privacy in messages to and from her lawyer discussing the subject of a future lawsuit.” In part, this was because the plaintiff “took steps to protect the privacy,” including using her personal, password-protected Yahoo! account instead of her company email address, and because she did not save her password on her computer. Plaintiff’s expectation of privacy was also objectively reasonable, the court continued, due to (1) the problems with the policy discussed above, (2) the email communications not being illegal or inappropriate, and (3) the fact that the “e-mails bear a standard hallmark of attorney-client privilege” -- the warning the communication was personal, confidential, and may be privileged communications. Thus the court held that the plaintiff “could reasonably expect that e-mails she exchanged with her attorney on her personal, password-protected, web-based e-mail account, accessed on a company laptop, would remain private” and that the plaintiff did not waive the privilege.

Finally, the court specifically stated that its ruling “does not mean that employers cannot monitor or regulate the use of workplace computers.” Rather, employers “can adopt lawful policies relating to computer use to protect the assets, reputation, and productivity of a business and to ensure compliance with legitimate corporate policies.” Employers may even discipline an employee “who spends long stretches of the workday getting personal, confidential legal advice from a private lawyer . . . for violating a policy permitting only occasional personal use on the Internet.” To enforce such a policy, however, the employer has “no need or basis to read the specific contents of personal, privileged, attorney-client communications in order to enforce corporate policy.”

(ii) Sims v. Lakeside School

At issue in Sims v. Lakeside School was the employer’s motion to compel a former employee to turn over her laptop -- furnished by the employer while he was employed -- for forensic review. First, the court -- and plaintiff -- conceded that the former employee had “no

---

286 Id.
287 Id. at 663.
288 Id. at 664.
289 Id. See also Curto v. Med. World Commc’n, Inc., No. 03CV6327, 2006 WL 1318387, at *4 (E.D.N.Y. May 15, 2006) (personal emails sent via personal AOL account from work provided computer to attorney were privileged despite company’s policy that prohibited the personal use of work -provided computers); Convertino v. U.S. Dep’t of Justice, 674 F. Supp. 2d 97, 110 (D.D.C. 2009) (“Because his expectations were reasonable, [plaintiff]’s private e-mails will remain protected by the attorney-client privilege.”).
290 Id. at 665.
reasonable expectation of privacy in the contents of the laptop that was furnished by defendant Lakeside, including e-mails he sent and received on his Lakeside e-mail account” based upon the employer’s broad policy.\textsuperscript{292} The policy generally provided that “the e-mail system [was] the property of Lakeside School . . . [and] does not assure the confidentiality of e-mail.”\textsuperscript{293} Such a policy, found the court, \textit{did not} cause the former employee to waive the attorney-client privilege with respect to “web-based e-mails sent and received by [the former employee] and other material prepared by [the former employee] to communicate with his counsel.”\textsuperscript{294} Thus the court permitted discovery of the former employee’s laptop, but limited the extent to which the employer was permitted to “review any web-based generated emails, or materials created by [the former employee] to communicate with his counsel.”\textsuperscript{295}

b. \textbf{Cases finding communications not privileged}

(i) \textit{Holmes v. Petrovich Development Company}

In \textit{Holmes v. Petrovich Development Company},\textsuperscript{296} the plaintiff sent emails to her attorney using her work provided computer and using her \textit{work} email. The employer’s policy -- in contrast to \textit{Stengart} -- was much more specific:

(1) she had been told of the company’s policy that its computers were to be used only for company business and that employees were prohibited from using them to send or receive personal e-mail, (2) she had been warned that the company would monitor its computers for compliance with this company policy and thus might “inspect all files and messages . . . at any time,” and (3) she had been explicitly advised that employees using company computers to create or maintain personal information or messages “have no right of privacy with respect to that information or message.”\textsuperscript{297}

The court relied upon this policy to find that plaintiff’s belief that her personal emails were private was unreasonable: “[S]he was warned that the company would monitor email to ensure employees were complying with office policy not to use company computers for personal matters, and she was told that she had no expectation of privacy in any messages she sent via the company computer.”\textsuperscript{298} By ignoring this policy and sending a message to her attorney about the case via a work-provided email account, according to the court, plaintiff’s actions were “akin to consulting her attorney in one of defendant’s conference rooms, in a loud voice, with the door open, yet unreasonably expecting that the conversation overheard by [the employer] would be

\textsuperscript{292} \textit{Id.} at *1–*2.
\textsuperscript{293} \textit{Id.} at *1.
\textsuperscript{294} \textit{Id.} at *2.
\textsuperscript{295} \textit{Id.}
\textsuperscript{297} \textit{Id.} at 883.
\textsuperscript{298} \textit{Id.}

© 2014 Miller Canfield, Paddock and Stone, P.L.C. All Rights Reserved.
privileged."\textsuperscript{299} It was also unreasonable for plaintiff “to believe that her personal e-mail sent by company computer was private simply because, to her knowledge, the company had never enforced its computer monitoring policy.”\textsuperscript{300}

Therefore, the California Court of Appeal upheld the trial court’s decision that the plaintiff’s communications were not communications protected by the attorney-client privilege.\textsuperscript{301}

(ii) Aventa Learning, Inc. v. K12, Inc.

One of the issues addressed in \textit{Aventa Learning Inc. v. K12, Inc.}\textsuperscript{302} was the extent to which communications saved by a former employee onto employer-provided computers -- even from web-based personal email accounts -- are protected from disclosure. The applicable employer policy was straightforward: “[e]lectronic communications are not private”; “[a]ll resources used for electronic communications are KLC property”; and “KLC reserves the right to access, search, inspect, monitor, record, and disclose any file or stored communication . . . at any time and for any reason.”\textsuperscript{303} Based on this policy, reasoned the court, the employee could not have had a reasonable expectation of confidentiality with regard to communications or other materials that he created or received on his KCDL laptop . . . and that were saved or stored on his KCDL laptop or the Defendants’ servers. The laptop itself was not his property, and the company reserved the right to access and disclose any file or stored communication at any time. Thus, [the former employee] cannot meet his burden of proving that any expectation of confidentiality he might have entertained was reasonable.\textsuperscript{304} Accordingly, the court found that privilege never attached to the former employee’s emails.

Going further, the court found that even if such communications were privileged, the employee waived the privilege, reasoning the employer’s broad policy that covered “all resources used for electronic communications” also applied to accessing and storing web-based emails onto the employer’s laptop.\textsuperscript{305} In so doing, the court distinguished \textit{Stengart} and \textit{Sims v.}

\textsuperscript{299} Id. at 896. \textit{See also Scott v. Beth Israel Med. Ctr., Inc.}, 847 N.Y.S. 2d 436, 440 (N.Y. App. Div. 2007) (emails to attorney not privileged; “For example, a spouse who sends her spouse a confidential e-mail from her workplace with a business associate looking over her shoulder as she types, the privilege does not attach.”).
\textsuperscript{300} Id. at 898.
\textsuperscript{301} \textit{See also Fazio v. Temp. Excellence, Inc.}, No. L-9353-06, 2012 WL 300634 (N.J. Super. Ct. App. Div. Feb. 2, 2012) (distinguishing \textit{Stengart} and finding attorney-client privilege did not apply to non-password-protected emails from employee to attorney utilizing employer’s email and computer system as the employee “took no steps whatsoever to shield the e-mails from his employer” despite fact that employer maintained no policy governing electronic communications).
\textsuperscript{302} \textit{Aventa Learning, Inc. v. K12, Inc.}, 830 F. Supp. 2d 1083 (W.D. Wash. 2011).
\textsuperscript{303} Id. at 1107 (alterations in original).
\textsuperscript{304} Id. at 1108.
\textsuperscript{305} Id. at 1108–09.
Lakeside School (discussed above) on state-law grounds, which according to the court, “adopt a no-waiver rule concerning web-based personal email accounts accessed through an employee’s company-issued computer or laptop.”

Such non-waiver rules are “inconsistent with Washington’s policy,” and therefore the court applied the Asia Global balancing test to find that the employee had waived the privilege.

c. Other Considerations

A recent case from the Southern District of New York considered the discoverability of Facebook posts between plaintiffs and potential putative class members. In In re Penthouse Executive Club Compensation Litigation, the employer sought discovery regarding communications via Facebook between named plaintiffs -- who were alleging wage/overtime allegations in violation of the Fair Labor Standards Act and state law -- and putative class members. The court evaluated the communications under both the attorney work-product doctrine and the attorney-client privilege.

Addressing the attorney work-product doctrine, the court -- after an in-camera review -- found some messages to be protected, as they were “descriptions of conversations with [p]laintiffs’ counsel regarding litigation strategy, as well as responses to questions about the lawsuit. These messages were not correspondence prepared in the ordinary course of business or personal life, but rather were directly prompted by the litigation and prepared because of the action at bar.” Rejecting plaintiffs’ contention that all of the messages were protected from disclosure under the “common interest rule” of the attorney-client privilege, the court allowed discovery concerning Facebook communications between plaintiffs and other nonparty dancers.

3. Other Privileges for Communications via Employer Technology

Other privileges that have recently been at issue with respect to electronic communications suggest that they also will apply to social media. For example, the Fourth Circuit in U.S. v. Hamilton recently found in a criminal case that a defendant waived the marital

---

306 Id. at 1110.
308 Id. The Asia Global balancing test provides that courts consider the following factors: (1) does the company maintain a policy banning personal or other objectionable use, (2) does the company monitor the use of the employee’s computer or email, (3) do third parties have a right of access to the computer or emails, and (4) did the corporation notify the employee, or was the employee aware, of the policy? See In re Asia Global, 322 B.R. 247, 257 (S.D.N.Y. 2005). See also, In re Info. Mgmt. Servs., Inc., No. 8168 (Del. Ch. 2013) (applying Asia Global and finding that executives did not have a reasonable expectations of privacy in the contents of emails because company’s policy expressly warned that employee emails were “open to access”).
310 Id. at 2–6.
311 Id. at 4.
312 Id. at 5–6.
communication privilege when he sent emails to and received emails from his wife using his work email account. At the time the defendant sent and received the emails, his employer did not have a computer usage policy. The employer subsequently instituted such a policy, expressly stating that users had “no expectation of privacy in their use of the Computer System,” including “stored” information. Affirming the lower court’s finding that the defendant waived the marital privilege, the Fourth Circuit noted that “one who is on notice that the allegedly privileged material is subject to search may waive the privilege when he makes no efforts to protect it.” Thus, since the defendant affirmatively acknowledged the policy and had not taken “any steps to protect the emails in question, even after he was on notice of his employer’s policy permitting inspection of emails stored on the system at the employer’s discretion,” the defendant waived the marital privilege.

III. CASE LAW REGARDING MONITORING ISSUES IN THE WORKPLACE

Generally speaking, employers monitor employees for reasons that include, protecting intellectual property assets, productivity, and avoiding liability. Employers, however, monitor at their own peril. By gathering exponentially more information about their employees, employers increase their legal exposure when faced with decisions that result in adverse actions like hiring, discipline, and discharge.

There are also issues related to increased use of social media. Social media allows employees to broadcast infinite amounts of information – from their desk, home or from a growing number of mobile devices with Internet access, such as cell phones, netbooks and tablets. The risks are not just contained to whether an employer can use information on an employee’s social media page to take an action, like discipline or discharge, against the employee. From a business perspective, employee postings can damage an employer’s reputation; embarrass customers; and reveal trade secrets. The computer security

---

313 701 F.3d 404 (4th Cir. 2012).
314 Id. at 408.
315 Id.
316 Id. at 409.
317 Id. at 408-09.
318 Employee use of social media can and should be a positive for employers. Social media use by employees can lead to things like improved client relations, exposure to new customers, and can foster professional development and new ideas.
software corporation Symantec conducted a survey in 2011 assessing the financial implications of social media misuse, including (in average costs per incident): reduced stock price ($1,038,401); litigation costs ($650,361); direct financial costs ($641,993); damaged brand reputation/loss of customer trust ($638,496); and lost revenue ($619,360). As to legal risks, postings on social media sites can expose employers to claims that run the gamut from civil liability under copyright, trade secret, security, trademark, and patent statutes, to liability

---

320 Consider the Tweet sent from Chrysler’s official Twitter account by an employee of a social media agency: “I find it ironic that Detroit is known as the #motorcity and yet no one here knows how to (expletive) drive.” Not only did the employee lose his job with the social media agency, Chrysler decided to not renew its contract with the agency. See Chris Woodyard, Chrysler dumps social media firm over Twitter f-bomb, USA TODAY, Mar. 11, 2011, available at http://content.usatoday.com/communities/driveon/post/2011/03/chrysler-fires-its-social-media-firm-over-twitter-f-bomb-/1 (last visited Aug. 30, 2012).


under common law torts like tortious interference with contractual relations,\textsuperscript{324} defamation,\textsuperscript{325} fraudulent misrepresentation,\textsuperscript{326} and invasion of privacy.\textsuperscript{327}

In addition to these risks, social media now allows easier monitoring of employees. Monitoring can help employers keep tabs on whether employees are actually working as most social media posts are time stamped as to when employees “posted” information and some even provide the location from where the employee “posted” information. Employers can also closely monitor employees who are on leave and possibly determine whether the leave is legitimate.\textsuperscript{328}


\textsuperscript{325} For example, an NBA official filed a defamation suit against an Associated Press reporter for a “tweet” he claimed disparaged his “professional and business reputation as a working, officiating NBA Referee . . . .” See Spooner v. Associated Press, No. 11-cv-00642 (D. Minn. 2011).

\textsuperscript{326} Jefferson Audio Visual Systems, Inc. v. Light, No. 3:12-CV-00019-H, 2013 WL 1947625 (W.D. Ky. May 9, 2013) (employer failed to state a claim for fraudulent misrepresentation against former employee who failed to update his social media accounts after termination to reflect that he was no longer an employee).

\textsuperscript{327} See, e.g., Maremont v. Susan Fredman Design Grp., Ltd., No. 10 C 7811, 2011 WL 6101949 (N.D. Ill. Dec. 7, 2011) (denying summary judgment on plaintiff’s Lanham Act and Stored Communication Act claims but granting summary judgment on plaintiff’s Right to Publicity and Right to Privacy claims when employer used plaintiff’s Facebook and Twitter accounts to send marketing messages while plaintiff was on medical leave); see also Murdock v. L.A. Fitness Intern., LLC, No. CIV. 12-975, 2012 WL 5331224 (D. Minn. Oct. 29, 2012) (dismissing former employee’s claims for, among other things, invasion of privacy and intentional infliction of emotional distress based on Facebook posts by his manager and other employees).

\textsuperscript{328} See Jaszczyszyn v. Advantage Health Physician Network, 504 Fed. Appx. 440 (6th Cir. Nov. 6, 2012) (affirming summary judgment for employer in FMLA interference case where the former employee was terminated for fraud while on intermittent FMLA leave after several coworkers saw pictures of the former employee drinking at a local festival on her Facebook page); Ainsworth v. Loudon Cnty. Sch. Bd., 851 F. Supp. 2d 963 (E.D. Va. 2012) (employer confronted employee for “call[ing] in sick late mornings when teachers [were] aware the day before due to [Facebook] postings that [the employee was] . . . not coming to work the next day”); Cf Shan Li, Insurers are scoring social media for evidence of fraud, Chi. TRIB., Jan. 27, 2011, available at http://articles.chicagotribune.com/2011-01-27/business/ct-biz-0128-facebook-evidence-20110127_l_social-media-facebook-manulife (last visited Aug. 30, 2012) (detailing an insurance company’s decision to stop paying disability benefits for depression after it found pictures on the employee’s Facebook page “show[ing] her frolicking at a beach and hanging out at a pub . . . .”).
as well as to check former employee’s activities in relation to non-compete and non-solicitation agreements.\textsuperscript{329}

A. Social Media as a Tool in Hiring and Recruitment

1. Screening Job Applicant’s Social Media Presence/Online Reputation

Employers are increasingly using social media as part of the job-interview process. Gathering information from social media to use in the hiring process and assessing an applicant’s online reputation have become essentially a “reference check” to a candidate’s résumé.\textsuperscript{330} The information collected can help employers weed out potential problem employees, as well as reinforce a good applicant’s chances of being hired.

A 2013 study by CareerBuilder revealed that 39\% of employers surveyed screen potential hires using social media, and nearly the same amount – 43\% – found information that caused


\textsuperscript{330} This is especially the case given that the default settings of most social media sites are as “open” as possible -- that a user shares the most amount of information with the most amount of people. A bill in the California Senate sought to partially change this process by prohibiting the display of personal information other than name and city without the user’s permission. In other words, the users must affirmatively agree to release such information. The bill failed to pass the California Senate. See S.B. 242, 2011 Leg. (Cal. 2011).
them not to hire a particular candidate. Some of the reasons given for not hiring candidates include:

- Candidate posted provocative/inappropriate photos/info (50%);
- There was information about candidate drinking or using drugs (48%);
- Candidate had poor communication skills (30%);
- Candidate bad mouthed previous employer (33%);
- Candidate made discriminatory remarks related to race, gender, religion, etc. (28%); and
- Candidate lied about qualifications (24%).

The same study, however, also found that 19% of hiring managers surveyed found information that caused them to hire a particular candidate. Such information includes:

- Good feel for candidate’s personality (50%);
- Conveyed a professional image (57%);
- Background information supported professional qualifications (49%);
- Well-rounded, showed a wide range of interests (50%);
- Great communication skills (43%);
- Candidate was creative (46%); and
- Other people posted great references about the candidate (38%).

---

332 Id.
333 Id.
334 Id.
In September 2013, the recruiting company Jobvite published its 6th Annual Social Recruiting Survey Results.\(^{335}\) According to Jobvite, 98% of recruiters are using some form of social networking to source candidates for jobs and 78% have hired via social media.\(^{336}\) Perhaps most troubling, however, is that according to Jobvite, 28% of recruiters reported that they would react negatively to overly religious posts or tweets on a candidate’s social media profile.\(^{337}\) Obviously, a recruiter passing on a candidate because of the religious nature of a Facebook post or Tweet, exposes the employer to potential liability under state and federal law.

An employer’s take-away from the CareerBuilder and Jobvite studies that while using online reputations as “reference checks” is growing increasingly more common, it is what employers do with that information that can cause risks. Because social media remains a potential window into the type of employee that an employer is contemplating hiring, one solution may be to consider having individuals outside of the hiring process review a candidate’s social media profiles. The individual should be trained to eliminate all information of protected categories (e.g., age, race, religion, etc.) and provide to the decision maker a sterilized report. By doing so, an unsuccessful will have difficulty arguing that the employer’s hiring decision was based on protected information from his/her social media sites.

a. Applicant’s “Protected Class” Status

Social media profiles can provide a torrent of information about job applicants and potential employees -- information that is generally not provided during a “normal” application process. For example, social media profiles often readily allow visitors to determine certain demographic information about a user that is otherwise protected by federal law: race, color, religion, sex, national origin, age, disability, pregnancy status, and genetic information.\(^{338}\) More expansive state and local nondiscrimination laws also cover other classifications, including height, weight, familial status, marital status, gender identity, and sexual orientation. Thus, employers who access social media may potentially waive any future argument that they were not aware of an applicant’s protected status. In effect, by utilizing social media, employers risk


\(^{336}\) Id.

\(^{337}\) Id.

\(^{338}\) For the first time, the EEOC issued regulations specifically addressing the use of social media by employers (in the context of implementing the Genetic Information Nondiscrimination Act). See 29 C.F.R. § 1635.8(b)(1)(ii)(D) (providing an exception where one “inadvertently learns genetic information from a social media platform which he or she was given permission to access by the creator of the profile at issue”).

© 2014 Miller Canfield, Paddock and Stone, P.L.C. All Rights Reserved.
losing an argument based upon “lack of notice” and are forced to prove a negative: that they did not consider the applicant’s protected status. 339

b. Employer’s Affirmative Obligation to Search All Publicly Available Information

One question that has not yet been addressed by the courts is whether employers have an affirmative obligation to search for and review publicly available information on social media sites. 340 Given the sheer amount of public information available on the web and the number of applicants who likely maintain some presence on social media sites, plaintiffs have now started alleging that employers negligently hired or retained an employee who is either known or should have been known to harm individuals with whom he/she has contact within the scope of his/her employment (co-workers and the public). 341

c. Discoverability of Collected Information and Record Retention

An employer’s practice and process of obtaining information from social media networks, as well as the specific information acquired from such networks is generally discoverable in employment litigation. Not only is it discoverable, employers have some obligations to maintain documentation about the process and information obtained in making employment decisions. Analogously, the Equal Employment Opportunity Commission (“EEOC”) published an informal letter on October 5, 2004 finding that an employer’s obligation to keep video resumes is the same as its normal obligations to keep regular paper applications and all other records relating to recruitment. 342 In other words, solicited resumes from applicants, regardless of paper or electronic, should be retained for at least one year. Resumes

339 See, e.g., Nieman v. Grange Mut. Casualty Co., No. 11-3404 (C.D. Ill. Apr. 27, 2012) (applicant put employer on notice that he was subject to protection of the ADEA where information on his LinkedIn account – which the employer asked about – contained his college graduation year).

340 In fact, some websites offer to review social media profiles for employers in order to avoid some of the legal issues associated with gathering information contained on applicants’ social media pages. See, e.g., Social Intelligence, www.socialintel.com (last visited Aug. 30, 2012).

341 See, e.g., Schneider v. City of Grand Junction Police Dep’t, No. 10-cv-01719, 2012 WL 683516 (D. Colo. Mar. 2, 2012) (granting employer’s motion for summary judgment in case arising out of a sexual assault by a police officer where plaintiff alleged that the police department “fail[ed] to check any internet or social media reviews of [the officer] (such as Facebook or Linked In)” as part of its background investigation prior to hiring the police officer). For cases generally discussing negligent hiring theories, compare Doe v. XYC Corp., 887 A.2d 1156, 1168 (N.J. Sup. Ct. 2005) (employer breached its duty to exercise reasonable care when it knew about and failed to prevent an employee from using the employer’s computer and network to view and transmit child pornography), with Maypark v. Securitas Sec. Servs. USA, Inc, 775 N.W.2d 270, 272, 275-76 (Wis. Ct. App. 2009) (employer not liable for negligent supervision where employee uploaded altered pictures from home of other employees on adult websites).

for those who are hired should become part of a personnel file and maintained for at least three years. Unsolicited resumes, however, need not be kept.

(i)    Hiring Process – Federal Contractors

Federal contractors have even more record retention requirements for “Internet applicants.” Under regulations promulgated by the Office of Federal Contract Compliance Programs (OFCCP), federal contractors must obtain and retain records relating to the gender, race, and ethnicity of every Internet applicant. An “Internet applicant” is defined as:

. . . any individual as to whom the following four criteria are satisfied:
(i) The individual submits an expression of interest in employment through the Internet or related electronic data technologies;
(ii) The contractor considers the individual for employment in a particular position;
(iii) The individual’s expression of interest indicates the individual possesses the basic qualifications for the position; and,
(iv) The individual at no point in the contractor’s selection process prior to receiving an offer of employment from the contractor, removes himself or herself from further consideration or otherwise indicates that he or she is no longer interested in the position. 343

This regulation potentially affects applications through social media.

2.  Internet Searches and Social Media in Recruitment

Gone are the days when an employer simply places an advertisement in the newspapers or hangs a “help wanted” sign in the window. Employers now extensively advertise job positions online, including through their own websites, “traditional” job search engines like monster.com or careerbuilder.com, as well as through social media sites. A 2012 study finds that over ninety percent of employers use social media to recruit applicants. 344 For example, some employers announce job positions on their own social media pages. 345 Others utilize the virtual advertisement space on social media sites to announce job openings and then link to the company’s general hiring website. 346

Using Internet searches to gain information itself is legal; it is what employers do with that information that can cause risks. Employers should be wary of using information gained as the basis for decisions where doing so would be unlawful under federal and state laws. Searching social networking sites is a relative new area of the law. It appears unlikely that an employer’s

343 See generally 41 C.F.R. § 60-1.3 (definition of “Internet applicant”).
346 Jason Cartwright, Apple Advertising Jobs on Facebook, TECHAU BLOG (Oct. 4, 2010), www.techau.tv/blog/apple-advertising-jobs-on-facebook/.

© 2014 Miller Canfield, Paddock and Stone, P.L.C. All Rights Reserved.
unauthorized use of information on a social networker’s profile in hiring could create liability for invasion of privacy because there is no reasonable expectation of privacy for publicly available information. Whether a person retains a reasonable expectation of privacy when the information he keeps private is shared unintentionally is unclear, however.

Federal and state employment laws require employers to recruit in a nondiscriminatory manner. Using social media as a recruitment source presents several issues to employers. How an employer recruits potential employees affects the composition of the employer’s workforce. By relying exclusively upon social media or by not utilizing it at all, employers run the risk of denying potentially protected classes access to information about job openings. While not intentional, such actions might expose employers to “disparate impact” discrimination claims. A disparate impact occurs generally when facially neutral criteria results in a disproportionate result due to protected characteristics. For example, by relying on an applicant pool generated exclusively from a social media network, an employer risks recruiting from a less diverse applicant pool. This risk is compounded by the fact that several social media networks are specifically designed to target demographic characteristics that are protected by state and federal employment laws such as race, color, religion, sex, national origin, disability and age.

3. Pre-Employment Checks

a. Criminal Background Checks

Inquiries into an applicant’s arrest record are generally improper, and may lead to liability for discrimination under Title VII or state anti-discrimination laws. For example, on January 11, 2012, the EEOC settled a charge of race discrimination with Pepsi Beverages for $3.13 million, where the EEOC alleged that Pepsi’s criminal background check policy “disproportionately excluded black applicants from permanent employment.” Pepsi also agreed to other remedies, including revising its background check policy.

On April 25, 2012, the EEOC issued updated enforcement guidance concerning the use of arrest and conviction records in employment decisions. The updated guidance focuses mostly on the potential disparate impact background checks may have on racial minorities, thus shifting the burden to employers to show that using background checks are job related for the positions in question and consistent with business necessity. Such issues are generally outside the scope of this paper, but employers should take note of this updated guidance as it clearly differentiates between arrests and convictions, provides several best practice suggestions, and discusses several factors to evaluate when examining whether using arrest and conviction records.

348 Id.
are job-related and consistent with business necessity: the nature and gravity of the offense or conduct; the time that has passed since the offense or conduct and/or completion of the sentence; and the nature of the job held or sought. More than anything else, the updated guidance stresses that employers should conduct an individualized assessment of applicants and employees as doing so would “provide[] an opportunity to the individual to demonstrate . . . the exclusion does not properly apply to him” and to “consider[] whether the individual’s additional information shows that the policy as applied is not job related and consistent with business necessity.” In addition to guidance from the EEOC, employers can look to state law which usually tends to allow private employers to base employment decision on criminal convictions found in background checks.

In addition, several jurisdictions have enacted “ban-the-box” legislation that generally prohibit employers from requesting criminal history information on an employment application. Jurisdictions with ban-the-box laws include Minnesota, Rhode Island, Buffalo, New York, Hawaii, Massachusetts, Newark, New Jersey, Philadelphia, Pennsylvania and Seattle, Washington. Similar bills are pending in 26 states.

b. Credit Checks

As a preliminary matter, the EEOC has ramped up its review of the possible disparate impact credit checks may have on minority applicants. In late 2010, for example, the EEOC filed suit against Kaplan Higher Education for its use of “credit history information.” On November 29, 2013, Kaplan won summary judgment after the court concluded that the EEOC did not set forth a prima facie case of disparate impact racial discrimination. Though this litigation has now concluded, it serves as a reminder that employment practices that cause

350 See Green v. Mo. Pac. R.R., 523 F.2d 1290, 1293 (8th Cir. 1975).
352 For example, effective January 1, 2014, California law prohibits employers from asking about or considering information concerning applicants’ criminal convictions that were judicially dismissed or ordered sealed. Cal. Labor Code § 432.9
353 Minn. Stat. § 364
354 R.G. Gen. Laws §§ 28-5-6, 28-5-7
355 Code of the City of Buffalo, Chap. 154, § 154-25
356 HRS §§ 378-2, 378-2.5
357 M.G.L. Ch. 6 §§ 151B, 168-173
358 Newark Ordinance #12-1630 (Sept. 19, 2012)
359 Philadelphia Code, Title 9, Chap. 9-3000 (Regulation of Businesses, Trades and Professions)
360 Seattle Municipal Code, Chap. 14.17
disparate impacts must be job-related and consistent with business necessity, and less discriminatory alternatives must not be available. 363

The Fair Credit Reporting Act ("FCRA") provides, among other things, applicants and current employees procedural and notice rights when employers seek information from a "consumer reporting agency." 364 A "Consumer report" is any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for . . . employment . . . ." 365 Before an employer can conduct such a credit check, the employer must disclose the fact to the applicant and obtain a written authorization. 366 Further, before taking adverse action against an applicant or employee based in whole or in part on the report, the employer must provide the applicant with a copy of the report, along with a description in writing of the applicant’s rights as prescribed by the Federal Trade Commission. 367 Note, however, that at least one District Court has found that the FCRA does not apply to independent contractors. 368

As defined by the statute, social media is not a "consumer reporting agency," and thus an employer’s search of social media alone does not trigger the Act’s procedural and notice requirements. On the other hand, employers who retain third party vendors to conduct background checks likely do. For example, on June 12, 2012, the FTC announced an $800,000 settlement with the online data broker Spokeo where the FTC alleged that Spokeo operated as a consumer reporting agency and violated the FCRA. 369 Spokeo "collects personal information about consumers from hundreds of online and offline data sources, including social networks" and then "merges the data to create detailed personal profiles of consumers" which includes "such information as name, address, age range, and email address" as well as "hobbies, ethnicity, religion, participation on social networking sites, and photos." 370 It then sells the information to companies in the human resources, background screening and recruiting industries. 371 According to the FTC, Spokeo violated the FCRA by "failing to make sure that the information it sold would be used only for legally permissible purposes; failing to ensure the information was

363 Similarly, while a number of Circuit Courts have recently found that the Bankruptcy Code does not prevent employers from refusing to hire candidates because they have filed for bankruptcy, see, e.g., Myers v. Toojay's Corp., 640 F.3d 1278 (11th Cir. 2011), such hiring practices may also have disparate impact issues.
365 § 1681a.
366 § 1681b.
367 § 1681b.
369 Press Release, Spokeo to Pay $800,000 to Settle FTC Charges Company Allegedly Marketed Information to Employers and Recruiters in Violation of FCRA, Fed. Trade Comm’n (June 12, 2012).
370 Id.
371 Id.
accurate; and failing to tell users of its consumer reports about their obligation under the FCRA, including the requirement to notify consumers if the user took an adverse action against the consumer based on information contained in the consumer report.”

Finally, note that ten states have passed laws restricting the use of credit reports by employers. Similar legislation is pending before Congress and many other state legislatures.

c. Health Checks

There are four main statutes that employers should be cognizant of before requesting or obtaining health information. These statutes outline permissible situations where an employer may obtain or ask for health information, but also outline situations where such inquiries can lead to unlawful discrimination or other statutory violation. First, the Americans with Disabilities Act (“ADA”) and state anti-discrimination laws prohibit an employer from asking questions related to an applicant’s disability, physical or mental health, prior to job offer. Post-offer medical examinations are permissible so long as the same process is followed for all individuals in the same job category. After an employee begins work, an employer may ask disability and health related questions to the extent the questions are job-related and consistent with business necessity. Generally speaking, medical information obtained in the employment process must be kept on separate forms and maintained in separate confidential medical files, subject to a few exceptions, i.e. managers and supervisors may be informed of any restriction on

---


373 California (CAL. LAB. § 1024.5); Colorado (C.R.S. § 24-5-101); Connecticut (CONN. GEN. STAT. § 31-51tt); Hawaii (HAW. REV. STAT. § 378-2(8)); Illinois (820 ILL. COMP. STAT. 70/10); Maryland (Md. CODE ANN., LAB. & EMPL. § 3-711); Nevada (Senate Bill 128, effective October 1, 2013); Oregon (OR. REV. STAT. § 659A,885); Vermont (VT Act No. 154, effective July 1, 2012); and Washington (WASH. REV. CODE § 19.182.005 et. seq.).

374 In December 2013, Senator Elizabeth Warren introduced a bill, called the Equal Employment for All Act of 2013, that would impose restriction on employers’ use of credit information for employment purposes, which are more stringent than any state laws.

375 42 § 12112(d)(2).

376 § 12112(d)(3).

377 § 12112(d)(4)(a).
the employee’s work and/or job duties and necessary accommodations, etc. Employers must be mindful of maintaining appropriate confidentiality of an employee’s medical information.\(^{378}\)

Second, the Health Insurance Portability and Accountability Act (“HIPAA”\(^{379}\)) provides a basis for protection of protected health information (“PHI”) and is applicable if the employer is a covered entity.\(^{380}\) HIPAA allows disclosure of PHI only under specific circumstances and with prior consent. Employers who have access to PHI are responsible for ensuring HIPAA compliance. The statute’s regulations provide extensive reporting, disclosure and documentation requirements, as well as monetary penalties for non-compliance.\(^{381}\) Employers who have access to PHI must have written privacy procedures in place.

Third, the Family and Medical Leave Act (“FMLA”) allows employers to require a medical certification from employees for certain types of leaves covered by the FMLA.\(^{382}\) Employers may ask for a clarification of the certification or challenge its adequacy.

Finally, the Genetic Information Nondiscrimination Act (“GINA”) prohibits the improper use of genetic information by employers in employment decisions and prohibits intentional acquisition of genetic information about applicants and employees while imposing confidentiality requirements.\(^{383}\) “Genetic information” includes information about an individual’s genetic test, genetic tests of family members, and family medical history. It does not include information about the sex or age of an individual or an individual’s family member, or information that an individual currently has a disease or disorder. It also does not include tests for alcohol or drug use.

\(^{378}\) See, e.g., McPherson v. O’Reilly Autom., Inc., 491 F.3d 726 (8th Cir. 2007) (evidence that vocational counselor was told by employer in phone call that former employee was completely disabled, coupled with employee’s inability to secure new job despite initial interest of prospective employers, was insufficient to support inference that employer was disclosing confidential information to prospective employers in violation of ADA); see also EEOC v. Ford Motor Credit Co., 531 F. Supp. 2d 930 (M.D. Tenn. 2008) (employee with HIV was subject to “job-related” inquiry and thus subject to ADA’s confidentiality requirement, when his manager disseminated his condition throughout the office, the court held that shame, embarrassment and depression suffered by employee as result of supervisor’s disclosure satisfied ADA’s “tangible injury” requirement to recover for wrongful disclosure of confidential information); Loschen v. Trinity United Methodist Church of Lincoln, No. 4:08CV3143, 2009 WL 2902956 (D. Neb. Sept. 9, 2009) (denying child-care facility’s summary judgment motion where employer gained information about employee’s seizures and then disclosed medical information to other employees and families who used the child-care facility).

\(^{379}\) 42 U.S.C. § 201 et seq.

\(^{380}\) A covered entity is a health care provider, a health care plan, or a health care clearinghouse. 42 U.S.C. § 1320d-9(b)(3).

\(^{381}\) See 45 C.F.R. § 164.

\(^{382}\) 29 U.S.C. § 2601 et seq.

\(^{383}\) 42 U.S.C. § 2000ff et seq.
d. Drug Tests

Private sector employees do not enjoy federal protection against workplace drug testing. There are no laws that prohibit conditioning a job offer on successful results of a drug test. Mandatory drug testing does raise privacy concerns because some tests can disclose information like legally consumed alcohol. Accordingly, drug tests should follow narrowly tailored procedural safeguards. Prospective employees should be given advance notice of any requirements and should be required to sign authorization forms.

Most states have enacted laws imposing procedural requirements and privacy safeguards on employers who utilize drug testing and some have either banned or restricted random drug testing of current employees. These laws tend to balance an employer’s interests in a “drug free workplace” and an employee’s legitimate expectation for privacy.

Public employees are entitled to constitutional protections under the Fourth Amendment against “unreasonable searches.” The U.S. Supreme Court issued two critical opinions regarding public employee drug testing, *Skinner v. Railway Executives’ Ass’n*, and *National Treasury Employees Union v. Von Raab*. Essentially, these two opinions permit public employers to drug test their employees provided the employer has “individualized suspicion” (i.e. “reasonable suspicion”). The only exception is where the public employer can show a “special need” for testing sufficient to outweigh the employee’s Constitutional rights.

Courts have rejected a public employer’s argument that maintaining the integrity of all government employees constitutes a “special need.” Rather, the U.S. Supreme Court in *Chandler v. Miller*, stated “the proffered special need for drug testing must be substantial – important enough to override the individual’s acknowledged privacy interest, sufficiently vital to suppress the Fourth Amendment’s normal requirement of individualized suspicion.” Public safety is the most widely accepted “special need.” As such, public employers have had success in requiring, for example, police officers, fire fighters, and transportation operators, to submit to random drug testing under the “special needs” (i.e. “public safety”) exception.

388 But see *Nat’l Fed’n of Fed. Employees-IAM v. Vilsak*, 681 F.3d 483 (D.C. Cir. 2012) (government failed to demonstrate “special needs” to justify random drug testing of all Forest Service employees who worked with at-risk youth); *Lanier v. City of Woodburn*, 518 F.3d 1147, 1150-51 (9th Cir. 2008) (finding that, as applied to an applicant for a library page position, the city’s policy of rescinding employment offers to applicants who refused to be tested for drug use violated the applicant’s privacy rights under the federal and state constitutions because the city had not articulated any special need to screen the applicant without suspicion).
Union employees are protected by the NLRA, which mandates that private sector employers must bargain collectively over terms and conditions of employment. The NLRA has ruled that drug testing of current employees (but not applicants) is a term or condition of employment and therefore drug testing of current employees is a mandatory subject of bargaining.  

389

390

391

392

393


392 29 U.S.C. § 2006(d)(1-4). See also Cummings v. Washington Mut., 650 F.3d 1386 (11th Cir. 2011) (employer met EPPA exceptions when it reasonably suspected plaintiff was involved in the disappearance of $58,000 and requested plaintiff to submit to a polygraph test in connection with an ongoing investigation).

a. Email & Internet

Employers likely can – with appropriate notice in employee policies – monitor work
emails on company servers. Some courts have found that, even where employers have detailed
technology policies, employers cannot access employee’s personal email accounts without
employee’s express permission under the SCA. In Pure Power Boot Camp, Inc. v. Warrior
Fitness Boot Camp, LLC, for example, the employer maintained a broad computer use policy
stating that employees had no right of personal privacy in any matter stored in or created on the
company’s system, including personal email accounts accessed on the company’s system, and
that computer usage was subject to monitoring without additional notice. After the employee
left the employer, the employer accessed two of the employee’s personal online email accounts
(Hotmail and Gmail) by using the username and password saved on his computer. Finding that
the employer violated the SCA, the court reasoned that the employer’s computer use policy that
prohibited personal use of Internet and provided notice of monitoring did not create implied
consent to access the employee’s personal emails stored with an outside provider, even if
accessed at work. Employers also risk violating the SCA where they access otherwise
restricted personal websites, such as social networking sites and password-protected chat
groups.

395 Id. at 559.
396 See e.g., Pietrylo v. Hillstone Restaurant Group, No. 06-5754, 2009 WL 3128420 (D.N.J. Sept. 25,
2009), discussed supra. See also Lazette v. Kulmatycki, 949 F. Supp. 2d 748 (N.D. Ohio 2013) (SCA
may prohibit employer who owns and pay for a phone to access an employee’s personal email account
after the employee returns the phone but does not erase their personal email from the device).
b. Video

Workplace video surveillance by private sector non-union employees is generally permissible, depending on the area covered and reason for their placement. As mentioned, for example, surveillance of bathroom, locker room, or dressing room would likely trigger invasion of privacy claims. Employers are also cautioned from monitoring areas such as break rooms or employee lounges where employees go to relax. Also, selective monitoring, such as of a specific employee may appear overly invasive, however surveillance of a larger appropriate area such as an inventory room for employer’s purpose of monitoring theft may withstand a court’s scrutiny. As for union employees, remember that any surveillance intended to monitor union activity or intimidate employees from engaging in union activities violates the NLRA and that “installation and use of hidden surveillance cameras in the workplace constitutes a mandatory subject of bargaining . . . .”

There have been a number of recent cases regarding employer video surveillance. For example, in Avila v. Sylvia Valentin-Maldonado, police officers claimed that surreptitious video surveillance of them in the locker-break room violated their Fourth Amendment rights. The police department installed a video camera in the locker-break room after a female employee had complained of receiving a harassing note in her locker. The court granted the employer’s motion for summary judgment, finding that the employer’s stated purpose of eradicating sexual harassment in the workplace, after having taken prior ineffective steps, was related to a legitimate work-related objective and not excessively intrusive because the surveillance was targeted to the female employee’s locker and a few lockers nearby. On the other hand, in Carter v. County of Los Angeles, the court concluded that the employer’s secret video

---

398 Brewers and Maltsters v. NLRB, 414 F.3d 36, 44 (D.C. Cir. 2005).
399 See, e.g., Robbins v. Lower Merion Sch. Dist., No. 10-665, 2010 WL 1957103 (E.D. Pa. May 14, 2010) (court ordered preliminary injunction and parties eventually settled for $610,000 where two high school student challenged their school’s secret surveillance of students in their homes through remotely activated webcams embedded in school-issued laptops); see also Bernhard v. City of Ontario, 270 Fed. Appx. 518, 2008 WL 687352 (9th Cir. 2008) (city police officers claimed Fourth Amendment violations based on covert video surveillance of their employee locker area while investigating a reported flashlight theft and court found that the officers had a reasonable expectation of privacy in the locker area where they dressed and action infringed on their privacy right); Smith v. Methodist Hosp. of Dallas, No. 3:07-CV-1230-P, 2008 WL 5336342 (N.D. Tex. Dec. 19, 2008) (summary judgment granted for employer hospital on invasion of privacy where employee was discharged after he was filmed sleeping on the job in a vacant “float” cubicle that was not his assigned work area or a designated break area); Miller v. Great Falls Athletic Club LLC, 242 P.3d 1286 (Mont. Sup. Ct. 2010) (court rejected invasion of privacy claim brought by employee who claimed total disability and entitlement to worker’s compensation benefits based on the employer’s videotaping of him exercising in a crowded athletic club where he had no expectation of privacy).
400 Nos. 06-1285, 1517, 2185, 2010 WL 936202 (D.P.R. March 12, 2010).
401 Id. at *2.
402 Id. at *3-6.
surveillance of employees in secured and restricted dispatch room, based solely on anonymous complaint, violated the plaintiffs’ Fourth Amendment and right to privacy under the California Constitution. According to the court, “[o]utside of a strip search or a body cavity search, a covert video search is the most intrusive method of investigation a government employer could select.”

c. Workplace and Physical Searches

Employers may need to conduct physical searches of the workplace to prevent theft, employee use or sale of drugs, or simply locate a file in an employee’s desk. Searches, however, may sometimes intrude into one’s reasonable expectation of privacy. Personal searches are more intrusive than work area searches and therefore can only be justified by an employer’s strong showing of need.

2. Social Media in Employment/Workplace Actions

Taking adverse action against an employee because of his or her use of social media may trigger several federal and state constitutional protections and employment statutes, as well as other common law protected areas. The sections that follow discuss some of the types of legal actions undertaken by employers and employees that involve the use of social media and some of the issues raised by those claims, followed by the kinds of state and federal constitutional and statutory protections such claims and actions might trigger.

a. Adverse Action by Employer and Subsequent Discrimination Claim by Employee

Discrimination charges by employees whose use of social media led to their adverse action are becoming more prevalent. The basis for the charges themselves is not novel -- they

---

404  Id. at 1050-51.
405 For example, in True v. Nebraska, 612 F.3d 676 (8th Cir. 2010), the Eighth Circuit examined a prison’s policy of randomly searching employee’s vehicles to prevent contraband from entering the prison and found that the fact that the cars were in a guarded parking area protected from inmate access supported the employee’s claims that the searches were unreasonable.
406 Although generally outside the scope of this article, it is worth noting employers have been successful in defending against administrative actions where former employees were terminated for social media use in violation of work rules. See, e.g., Chapman v. Unemployment Comp. Bd. of Review, 20 A.3d 603 (Pa. Cmwlth. 2011) (affirming Board’s decision that since employee violated employer’s cell phone policy by using her cell phone to make postings about her co-worker to Facebook, she was not entitled to unemployment compensation benefits); see also Clement v. Johnson’s Warehouse Showroom, Inc., 388 S.W.3d 469 (Ark. Ct. App. 2012) (Workers’ Compensation Commission did not abuse discretion by admitting pictures from plaintiff’s Facebook and Myspace pages that showed “him drinking and partying” where plaintiff claimed that he was “in excruciating pain” as a result of his workplace injury because such “pictures could have a bearing on [plaintiff]’s credibility”).
tend to make the following standard employment discrimination argument: “I was disciplined or discharged for doing X; I am a member of Y protected group; and employee Z did X as well, but was not disciplined or discharged as was I.”

Such was the case with Ellen Simonetti, a Delta Airlines flight attendant. Simonetti maintained a blog entitled “Diary of a Flight Attendant,” in which she mused about her travel and experiences as a flight attendant. In one post, she uploaded several pictures of herself on an airplane in uniform -- including one with her blouse partially unbuttoned, exposing part of her bra. Delta deemed her pictures inappropriate and terminated Simonetti. She filed suit against Delta alleging, among other things, that other similarly situated male flight attendants had posted similar pictures but were not terminated and, thus, Delta’s action constituted sex discrimination.407 The merits of Simonetti’s case were never decided due to Delta’s filing for bankruptcy. Ellen Simonetti’s suit is a case study in why employers should consider the extent to which it should investigate how they responded to other “comparable employee” actions in the social media sphere prior to taking an adverse action against an employee.408

More recently, Sam’s Club (a subsidiary of Wal-Mart Inc.) fired an employee for a Facebook comment that violated its social media policy.409 The employee had commented about

408 See also Marshall v. Mayor & Alderman of City of Savannah, Ga., 366 Fed. Appx. 91, 99, 100 (11th Cir. 2010) (probationary firefighter who posted pictures of firefighters taken from the city’s website on her Myspace page next to revealing pictures of herself failed to establish a prima facie case of sex discrimination because no other similarly situated employee was treated more favorably); Rodriguez v. Wal-Mart Stores, Inc., No. 3:11-CV-2129, 2013 WL 102674 at *9 (N.D. Tex. Jan. 9, 2013) (summary judgment for employer in age and race discrimination case where employer terminated employee for “publicly-rather than privately-chastised employees under her management on a social media website”); Gaskell v. Univ. of Ky., No. 09-244, 2010 WL 4867630 (E.D. Ky. Nov. 23, 2010) (finding plaintiff raised a triable issue of fact as to whether defendant failed to hire him due to his religious beliefs, as decision makers’ comments about plaintiff’s website containing his thoughts on creationism constituted direct evidence of religious discrimination); Mai-Trang Thi Nguyen v. Starbucks Coffee Corp., Nos. CV 08-3354 CRB, CV 09-0047, 2009 WL 4730899 (N.D. Cal. Dec. 7, 2009) (granting employer’s motion to dismiss where former employee posted comments on her MySpace page containing threats against company and coworkers, as well as vague references to her religion); Williams v. Wells Fargo Fin. Acceptance, 564 F. Supp. 2d 441, 449–50 (E.D. Pa. 2008) (denying employer’s summary judgment motion where plaintiff -- who was fired for sending “sexually suggestive and otherwise inappropriate jokes or pictures” -- put forth evidence that a similarly situated employee had sent inappropriate emails from his MySpace account but was not fired); See also Shaver v. Davie Cnty. Pub. Schs., No. 1:07cv00176, 2008 WL 943035, at *1–*2 (M.D.N.C. Apr. 7, 2008) (dismissing plaintiff’s claim for failing to exhaust administrative remedies for his claim that he was fired for information contained on his MySpace page that “reveal[ed] he practices the Wicca religion. . . .”). CF.Peer v. F5 Networks, Inc., No. C11-0879, 2012 WL 924349 (W.D. Wash. Mar. 19, 2012) (denying motion for summary judgment in direct threat/ADA case where employee used Facebook to communicate with her manager about her suicidal thoughts).
a photo depicting two coworkers at a party, hosted by a third coworker, when they had called in sick. Specifically, the employee wrote, “I hear that Caleb didn’t show up for work on this day what’s up with that???? He is partying with you guys?? WOW and Carrie tried to call in for him and knew about this . . . you guys are amazing and bold enough to post these [pictures] hahahahaha.” Wal-Mart’s social media policy prohibited any conduct that adversely affects job performance or other associates, but allows employees to post complaints online as long as the comments do not appear “unprofessional, insulting, embarrassing, untrue [or] harmful.” The coworker who hosted the party complained to her managers who determined that the post violated policy. After being discharged, the employee sued for national origin and age discrimination. Affirming the lower court’s grant of summary judgment, the Fifth Circuit held that Wal-Mart’s legitimate reason for terminating her, violation of the social media policy, was not a pretext for discrimination.

The Fifth Circuit noted that plaintiff admitted to facts that formed the basis of Wal-Mart’s belief that she violated the policy on multiple occasions and that Wal-Mart “certainly could have concluded” that plaintiff violated the policy.

It is also worth remembering that, just as in non-social media contexts, an employer that discharges an employee based on an honest, but mistaken belief, that the employee violated its social media policy, is not liable for discrimination. This point was recently confirmed by the Seventh Circuit in Smizer v. Community Mennonite Early Learning Center. In that case, the plaintiff worked as a teacher’s aide at a church-affiliated daycare center run by his mother. His mother informed the board that he had posted “horrible stuff” on his Facebook page, she no longer felt safe in his presence and that she wanted him discharged for “creating a hostile work environment.” Granting the mother’s request, the board discharged the plaintiff for “insubordination and unprofessional conduct” based on his alleged Facebook postings, but without ever receiving a copy of the alleged posts. Denying that he wrote any inappropriate posts, the plaintiff sued for gender discrimination, alleging that he was discharged because the employer was losing potential business from parents unwilling to leave their infant girls in the care of a man. Affirming summary judgment in favor of the employer, the court held even if the employer’s reason for discharging the plaintiff was not a good one, that fact was irrelevant if the employer honestly believed that the employee wrote offensive Facebook posts.

b. Harassment and Hostile Work Environment Claims

The nature of social media makes both the notice and content requirements of hostile work environment claims much more dangerous than “traditional” claims. Social media sites

---

410 Id. at *1-2.
411 Id.
412 Id. at *3-6.
413 Id.
414 Smizer v. Community Mennonite Early Learning Center, 538 Fed. Appx. 711 (7th Cir. 2013).
415 Id. at 713
416 Id. at 711 (per curiam).
417 Id. at 714
often blur the line between colleagues, friends, and family members, granting access to messages, pictures, and videos that have traditionally been separate. These “virtual water coolers” facilitate more communication before, after, and in all likelihood during work hours. Given human nature, it is inevitable that employees will not only network with each other on social media sites, but also use social media to discuss things like working conditions and other co-workers. There is a good chance that if one employee is publicly harassing another employee via social media, other employees will likely know about it.

Applying the traditional harassment rubric, employers might be liable for harassment on social media depending upon several factors. First, “[a]n employer is subject to vicarious liability to a victimized employee for an actionable hostile environment created by a supervisor with immediate (or successively higher) authority over the employee.” 418 Put another way, an employer is presumed liable for a supervisor’s harassment that results in a tangible employment action like “hiring, firing, failing to promote, reassignment with significantly different responsibilities, or a decision causing a significant change in benefits.” 419 An employer may escape liability or damages stemming from a supervisor’s harassment by proving that: (1) there was no tangible employment action; (2) it “exercised reasonable care to prevent and correct promptly any . . . harassing behavior”; and (3) the “employee unreasonably failed to take advantage of any preventive or corrective opportunities provided by the employer or to avoid harm otherwise.” 420

Second, employers may also be liable for harassment on social media by co-workers or even non-employees. If an employer either knows or has a reason to know of work-related harassment occurring on social media, then an employer might be liable under federal and state hostile work environment claims. 421 This was the exact issue at hand in Blakey v. Continental Airlines. 422 There a female pilot made hostile work environment and harassment complaints to the company “based on conduct and comments directed at her by male co-employees.” 423 After her complaints and the subsequent litigation that occurred, fellow pilots began posting “derogatory and insulting remarks about Blakey on the pilots[‘] on-line computer bulletin board,” which was accessible to all of Continental’s pilots and crew members. 424 Noting that other courts “have held that ‘an employer can be liable for coworkers’ retaliatory

419 Id. at 761.
420 Id. at 765.
421 Faragher v. City of Boca Raton, 524 U.S. 775, 779, 118 S. Ct. 2275 (1998) (“[The federal courts have] uniformly judg[ed] employer liability for co-worker harassment under a negligence standard . . . .”); Folkerson v. Circus Enters, Inc., 107 F.3d 754, 756 (9th Cir. 1997) (employer liable for non-employee’s harassment “where the employer either ratifies or acquiesces in the harassment by not taking immediate and/or correction actions when it knew or should have known of the conduct”).
423 Id. at 47.
424 Id. at 48.
harassment," the New Jersey Supreme Court stressed that “employers do have a duty to take effective measures to stop co-employee harassment when the employer knows or has reason to know that such harassment is part of a pattern of harassment that is taking place in the workplace and in settings that are related to the workplace.”

In *Amira-Jabbar v. Travel Services, Inc.*, the plaintiff’s co-worker posted pictures from a company outing on a Facebook page. The plaintiff then “commented” on a picture of herself, stating, “remind me that taking pictures in the shade is really disservice to my wonderful chocolate skin.” Another co-worker responded to the plaintiff’s comment saying, “[t]hat is why you always have to smile!!!!” Plaintiff interpreted this comment as racist, resigned, and eventually filed a discrimination suit in part because of the Facebook “incident.” Among other things, the plaintiff argued that the employer should be liable “because it allowed its employees to post photos and comments on the website during company time for company purposes.” The court dismissed plaintiff’s claim of a hostile work environment because the

---

425 *Id.* at 58 (citation omitted).
428 *Id.*
429 *Id.*
430 *Id.*
431 *Id.* at 83.
employer had promptly and appropriately responded to plaintiff’s internal complaints.  

A sexual harassment/hostile work environment case from Wisconsin addressing a situation in which an employee alleging sexual harassment had herself made “some off-color, sexual jokes on the online community ‘Myspace’. . . .” raises discovery-related issues that are worth noting. An employee’s own social media sites are likely to produce relevant and discoverable information relating either to his or her claims or the employer’s defenses. One area for discovery -- by either side -- is the extent that an employee participates in conduct about which she later complains. In the Wisconsin decision, the jury found the employer liable for a hostile work environment, and the employer challenged (as relevant here) the jury’s finding that the employee was offended by her supervisor’s sexual harassment despite her own “off-color, sexual jokes” posted on Myspace.

The court refused to overturn the jury’s finding, juxtaposing the behavior alleged in supporting the hostile work environment with those comments posted on Myspace: “However, sharing jokes with friends in an online community is vastly different than being propositioned for sex by a supervisor at work. Thus, the jury

---

432 Id. at 86–87. See also Debord v. Mercy Health Sys. of Kan., Inc., 737 F.3d 642 (10th Cir. 2013) (affirming trial court’s ruling that employee’s Facebook post that her manager “needs to keep his creepy [sic] hands to himself” did not constitute proper notice to trigger the employer’s duty to take remedial action and held that plaintiff could not show retaliation where plaintiff repeatedly, falsely denying having authored Facebook posts accusing her supervisor of misconduct); Summa v. Hofstra Univ., 708 F.3d 115 (2d Cir. 2013) (Facebook postings made by football team members about team manager could not be imputed to employer because football coach took remedial action when made aware of the alleged harassment); Garvin v. Siouxland Mental Health Serv., Inc, No. C10-4107, 2012 WL 1820647, at *26-27 (N.D. Iowa May 18, 2012) (material fact dispute as to whether supervisor sexually harassed plaintiff, where, among other things, supervisor asked plaintiff during a Facebook chat “if, hypothetically, she would have a relationship with her.”); Yancy v. U.S. Airways, Inc., No. 10-983, 2011 WL 2945758, at *1 (E.D. La. July 20, 2011) (employee who complained that a supervisor posted a picture of plaintiff on Facebook “showcas[ing] at least part of her buttocks and the meager lines of her thong underwear” could not establish a prima facie case of retaliation because she could not show a causal connection between her alleged protected activity and her suspension for violating the company’s sexual harassment policy for a different incident); Urban v. Capital Fitness, No. CV8-3858, 2010 WL 4878987, at *9, 10 (E.D.N.Y. Nov. 23, 2010) (employee’s personal Myspace page did not lend evidence to plaintiff’s hostile work environment claim because it was “something that an employee had to go out of his or her way to view, and not pervasive in the workplace environment”). One commentator takes the position that due to “confusion and a dearth of case law regarding what role evidence of social media harassment should have in a hostile work environment claim . . . courts should examine whether the employer derived a substantial benefit from the social media forum utilized by the harasser” to determine an employer’s liability. See Jeremy Gelms, Comment, High-Tech Harassment: Employer Liability Under Title VII for Employee Social Media Misconduct, 87 WASH. L. REV. 249, 272 (2012); Commonwealth v. Cox, No. 2196, 72 A.3d 719 (Pa. Sup. Ct. 2013) (Pa. Super. Ct., Aug. 2, 2013) (finding that Facebook comments support verdict of harassment).


434 Id. at 811
reasonably concluded that [the employee] subjectively believed that the harassment was severe or pervasive.”

Perhaps different facts here would have diminished the employee’s claims, but it is clear that social media sites should not be ignored during discovery to better flesh out employee claims and employer defenses.

c. Age Discrimination

Despite the statistics suggesting that social media usage is not just limited to younger employees, it is possible that an employer’s reference to social media sites might be interpreted as evidence of age discrimination. For example, in *Fisher v. Department of Veterans Affairs,* one of the pieces of evidence the plaintiff used to try to support her hostile work environment claim was that one of her managers allegedly said that “he was happy to see young workers at the VA because ‘they understand computers. They know Facebook.’”

The court dismissed plaintiff’s claim, but it stands to reason that use of terms generally associated with younger generations might be used in the future in an attempt to support age discrimination and hostile work environment claims.

d. Retaliation

Social media affords employees more opportunities than ever to publicly share their thoughts about their employers. In some cases, such thoughts can put employers on notice of an employee’s opposition to an alleged unlawful practice or participation in a statutory complaint process. Any subsequent adverse action by the employer can then be possibly construed as retaliation for the employee’s protected activity.

In *Zakrzewska v. The New School,* 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.

---

435 *Id.*

436 See also *Coates v. Mystic Blue Cruises, Inc,* No. 11-C-1986, 2012 WL 3860036 (N.D. Ill. Aug. 9, 2012) (compelling sexual harassment plaintiff to produce Facebook and Twitter messages “which reveal intimate conversations between her and certain male employees”); *Targonski v. City of Oak Ridge,* No. 3:11-CV-269, 2012 WL 2930813 (E.D. Tenn. July 18, 2012) (denying summary judgment on former employee’s sexually hostile work environment claim where supervisor allegedly spread rumors about plaintiff, but permitting jury to consider comments made on plaintiff’s Facebook page regarding her “desire for a female friend to join her ‘naked in the hot tub,’” “discussing ‘naked twister,’” and taking about “female orgies involving plaintiff, [another female], and others, to be filmed by plaintiff’s husband.”).


438 *Id.* at *3. See also *Gifford v. Target Corp.***, No. 10-2049, 2011 WL 3876420 (D. Minn. Aug. 31, 2011) (supervisor’s comment that plaintiff was lucky to have her granddaughters keep her young after plaintiff mentioned that her granddaughters introduced her to Facebook was not direct evidence of age discrimination).

it occurred. Disagreeing, the court stated, “I cannot foreclose the possibility that a trier of fact reasonably could find that defendants’ alleged covert monitoring of plaintiff’s personal Internet use at work ‘well might have dissuaded a reasonable worker from making or supporting a charge of discrimination,’” and granted the employee leave to amend.440

Similarly, in Dotson v. City of Syracuse, the plaintiff alleged that after making her initial complaint of sexual harassment she was subjected to numerous acts of retaliation by her employer, including, among other things, eavesdropping on her telephone conversations.441 The court found that a reasonable fact finder could conclude that “the requisition and monitoring of plaintiff’s telephone conversations was intrusive and could have dissuaded plaintiff from filing a claim.”442 The court found that the eavesdropping occurred in temporal proximity to the complaints and for this and other reasons, denied the employer’s motion for summary judgment and dismissal of the plaintiff’s Title VII retaliation claim.

The case of extreme sexual harassment by a supervisor in Forsberg v. Pefanis443 is instructive. In that case, the supervisor’s extreme sexual harassment allegedly forced the plaintiff to resign, and she then sued her supervisor and her former employer.444 Plaintiff asserted that after finding out about the lawsuit, the supervisor and the co-owner sought to gain access to plaintiff’s Myspace page through one of plaintiff’s mutual friends445 and that they did so in order to “obtain personal and private information about plaintiff and her family,” which they would then use to disseminate false information about the plaintiff.446 Such actions by the employer,

440 Id. at 187.
442 Id. at *19.
444 Id. at *4.
445 Id. at *14.
446 Id. at *14–15.
concluded the court, were “evidence of ‘post-employment blacklisting’” and thus actionable retaliation.\[447\]

In Deneau v. Orkin, LLC, one week prior to plaintiff’s termination for repeatedly working overtime without authorization, plaintiff posted the following on her personal Facebook page: “anyone know a good EEOC Lawyer? Need one now.”\[448\] At his deposition, the branch manager testified that he saw the comment on the plaintiff’s Facebook and faxed it to the division human resources manager who later testified that there was a management level discussion about the Facebook post that preceded the termination.\[449\] The court concluded that the Facebook post qualified as protected activity to support a retaliation claim.\[450\] Ultimately, the plaintiff’s claim failed, however, because she could not prove that the employer’s legitimate non-retaliatory reason for termination was a pretext for discrimination.\[451\]

A claim for retaliatory discharge will not succeed where the evidence reveals that the employee repeatedly and falsely denied having authored Facebook posts accusing her supervisor of misconduct. In Debord v. Mercy Health System of Kansas Inc., the plaintiff posted a series of posts on her Facebook page accusing her supervisor of padding paychecks of workers he favored. During the investigation, plaintiff denied authoring the posts, stating three times that someone posted them from her cellphone. Finally, she admitted that she wrote them. The employer discharged plaintiff for her dishonesty and for making other comments about the investigation which disrupted the workday for her coworkers. Affirming the lower court’s dismissal of plaintiff’s retaliation claim, the court held: “She admits posting inflammatory material about her supervisor on the Internet, sending text messages to co-workers bad-mouthing

\[447\] Id. at *15. See also Stewart v. CUS Nashville, No. 3:11-cv-0342, 2013 WL 456482 (M.D. Tenn. Feb. 6, 2013) (plaintiffs established prima facie case of retaliation where, in part, their supervisor posted comments to his blog accusing one plaintiff of theft and stating “Dear God, please don’t let me kill the girl that is suing me” regarding the other plaintiff on his Facebook while drunk); Morse v. J.P. Morgan Chase & Co., No 8:11-cv-00779-JDW-EAJ (M.D. Fla. Jun. 24, 2011) (plaintiff who “simply voiced her disagreement with her employer’s payment practices on her Facebook page” failed to state a claim for retaliation, as her “letting off steam” on her Facebook page did not constitute a “complaint” under the Fair Labor Standards Act); Williams v. Singing River Hosp. Sys., No. 08cv86, 2009 WL 484587, at *3–*4 (S.D. Miss. Feb. 26, 2009) (dismissing plaintiff’s retaliation complaint predicated upon being shown an allegedly racist video by a co-worker because she complained about the video after the adverse action); Derrick v. Metro. Gov. of Nashville & Davidson Cnty., Tenn., No. 3-06-1222, 2007 WL 4468673, at *10 (M.D. Tenn. Dec. 17, 2007) (plaintiff did not establish a prima facie case of retaliation where, in part, her supervisor had “posted rhetorical questions such as ‘what is wrong with women these days?’ and [had] mad[e] statements such as ‘Chicks seem to have more issues these days than Jet Magazine, and keep up more drama than daytime television and Jerry Springer combined’”; the statements did not show pretext because they did not relate to the employer’s legitimate nondiscriminatory reason for its adverse action -- plaintiff’s poor performance.).


\[449\] Id. at *15-18.

\[450\] Id.

\[451\] Id.
her supervisor (unrelated to the alleged sexual harassment), discussing the overpay and harassment investigations with others, knowingly pocketing overpayment in 2007, and thrice lying about posting information on Facebook while at work,” according to the opinion. “No reasonable jury could find these reasons ‘unconvincing.’”

3. Ownership of Employer-Sponsored Social Media Accounts

At first glance, the issue of who owns an employer-sponsored social media account appears to be straightforward and noncontroversial: employers own their own social media accounts. Some employees, however, have challenged this assumption. In PhoneDog v. Kravitz, for example, Noah Kravitz worked for the website PhoneDog.com as a product reviewer and blogger. PhoneDog provided Kravitz the use of a Twitter account, “@PhoneDog_Noah,” so that Kravitz could disseminate information and promote the company’s services. When Kravitz subsequently resigned, PhoneDog asked him to stop using the Twitter account. Kravitz refused. Instead, possessing the login and password credentials for the Twitter account, Kravitz changed the name of the account to “@noahkravitz” and continued using it. PhoneDog sued Kravitz alleging, among other things, that Kravitz stole its trade secrets and other proprietary and confidential information. For his first responsive pleading, Kravitz moved to dismiss the lawsuit, arguing that there was no clear policy defining ownership of the Twitter account and that PhoneDog could not otherwise prove that it owned the account. He also argued that, while employed, he used the account for personal matters unrelated to his employment. The district court rejected Kravitz’s argument and permitted the case to proceed.\(^{453}\) In December 2012, the parties settled their dispute, leaving the ultimate ownership issue unresolved by the court.

The case of Eagle v. Morgan is also instructive on this issue. In that case, plaintiff, the founder and executive of a company, established and maintained a LinkedIn account for her company. The plaintiff’s company was purchased by another company, which ultimately resulted in the employee’s termination. When the plaintiff attempted to later access the LinkedIn account, she could not as the purchasing company changed the password. Not only had the password changed, the purchasing company also changed the information on the account to make it look as if it were the plaintiff’s immediate successor’s account, despite the fact that the account was still titled in the plaintiff’s name. A few weeks later, the plaintiff eventually gained back full access and control of the LinkedIn account and then sued the purchasing company under two federal claims – Computer Fraud and Abuse Act and the Lanham Act – and several state torts, including invasion of privacy by misappropriation of identity, misappropriation of publicity, identify theft, and conversion. A federal court dismissed the plaintiff’s federal claims and the state claims went to trial. On March 12, 2013, the court found that the purchasing

\(^{452}\) Debord, 737 at 655.

company was liable for misappropriation of identity and misappropriation of publicity, but did not award damages because the employee failed to show any economic damages.\(^{454}\)

Both PhoneDog and Eagle are prime examples of how the pace of technological advances can quickly raise employment law issues. Employers should take an important lesson from these cases – be proactive and constantly draft and revise policies that keep up with technological advances. As to the issue of social media ownership, employers should adopt a policy clarifying that employer-sponsored social media accounts are the property of the employer and that employees must relinquish login credentials upon their departure.\(^{455}\)

4. **Bring Your Own Device (“BYOD”)**

Employers cannot ignore the ubiquitous nature of mobile devices in today’s society: nearly half of all American adults use smartphones and over thirty-percent own a tablet.\(^{456}\) Prior to a couple of years ago, using these personal mobile devices as the sole access point to an employer’s information technology system was almost unheard of. Though employers still issue mobile devices to their employees, the recent “Bring Your Own Device” (“BYOD”) trend is becoming the norm. Recent surveys suggest that over fifty percent of employers permit employees to access work-related material via their personal mobile devices.\(^{457}\) Many employers are adopting BYOD policies as a way to keep up with the pervasive and fast growing nature of mobile devices – they see it as a way to increase employee productivity, customer response times and work processes.\(^{458}\) They are also adopting them to remain competitive in the Twenty-First

\(^{454}\) Eagle v. Morgan, No. 11-4303, 2013 WL 943350 (E.D. Pa. Mar. 12, 2011); see also Maremont v. Susan Fredman Design Group, Ltd., No. 10 C 7811, 2011 WL 6101949 (N.D. Ill. Dec. 7, 2011) (denying summary judgment on plaintiff’s Lanham Act and Stored Communication Act claims but granting summary judgment on plaintiff’s Right to Publicity and Right to Privacy claims when employer used plaintiff’s Facebook and Twitter accounts to send marketing messages while plaintiff was on medical leave).

\(^{455}\) See Ardis Health, LLC v. Nankivell, No. 11 Civ. 5013, 2011 WL 4965172, at *1 (S.D.N.Y. Oct. 19, 2011) (ordering former employee who was responsible for “maintaining websites, blogs, and social media pages in connection with online marking of [the employer]’s products” to turn over login information post-termination); see also S.B. 2306, 98th Gen. Assem. (Ill. 2013) (Signed by Governor Pat Quinn on August 16, 2013 amending Right to Privacy in the Workplace Act to allow employers access to information regarding “professional” social media accounts, which are defined as those ‘created, maintained, used, or accessed by a current or prospective employee for business purposes of the employer’).


With the adoption of these policies, however, comes risk, generally divided into two main categories: (1) control of employer data; and (2) compliance with employment and labor laws. The discussion below offers a basic primer on some of the issues raised by BYOD.

a. Control of Employer Data

(i) Keeping Information Secure

Mobile devices connected to an employer’s network often permit access to almost all elements of an employee’s work: email and other communication systems; contacts; and documents – stored either on the employer’s network or in the cloud. The risks associated with permitting employees to access employer information – including, for example, information that is considered a trade secret, confidential, or proprietary – via a mobile device is not a new concern. For years, employers have developed various protocols for providing employees with company-owned mobile devices, including how to address information security of that device. Most adopt various security measures – like passwords and other secure login credentials – to inhibit access to mobile devices that are lost or stolen. Employers may also “remote wipe” the device, erasing all information contained on the mobile device.

BYOD, however, heightens the risk to employer information in many ways:

1. BYOD breaks down barriers between work and personal life, increasing the risk that the mobile device can be lost or stolen. The nature of BYOD simply exposes employer information to places where in the past, it has not gone. Employees bring their own mobile devices with them to places where they might not bring a work device – like while out drinking on St. Patrick’s day. Moreover, BYOD facilitates the theft of employer information by employee’s themselves, seamlessly allowing employees access to employer information and personal information on the same device. In addition to raising information security concerns for an employer or civil/criminal liability for an employee, it also raises misappropriation concerns for employers who hire competitor’s employees.

459 Id.
460 The remote wipe function is not something that is just limited to employers. Apple, for example, permits users to erase personal information contained on its devices. See iCloud: Erase your device remotely, http://support.apple.com/kb/ph2701
461 A 2012 Symantec study finds that thirty-five percent of all adults have either lost their mobile device, or had it stolen. SYMANTEC, 2012 NORTON CYBERCRIME REPORT 12 (2012).
462 Cf USI Ins. Servs. LLC v. Miner, 801 F. Supp. 2d 175, 196 n.21 (S.D.N.Y. 2011) (denying summary judgment on misappropriation claim where former employee forwarded email to his personal account and then to his new employer).
2. BYOD exposes employer information to more people, even if the device is not lost or stolen. Consider, for example, the ease with which an employee may provide access to his or her mobile device to a family or friend, often after having satisfying security measures intended to keep non-employees out.

3. Because personal mobile devices cannot be totally controlled by the employer, BYOD increases the risk that the mobile device will be “hacked” or exposed to viruses or malware. A 2011 study from the Ponemon Institute illustrates this risk, finding, among other things, that twenty-three percent of all information losses resulted from hacking, twenty-one percent from web-based application or file sharing sites, and thirteen percent from unsecured mobile devices.\(^{463}\) By accessing websites, file sharing programs, or downloading applications for their own personal use, employees may unknowingly and unintentionally expose the employer’s information to third-parties.

Consequences for the loss or theft of such information go beyond economic or reputational damages. Information security breaches can result in significant legal liability. For example, several state and federal laws require companies to take affirmative steps to protect an individual’s personal information – like health information and social security and credit card numbers – and impose penalties upon companies for failing to maintain the security of information regarding its customers, clients, and/or employees.\(^{464}\) Other laws mandate that companies notify individuals when their personal information has been compromised.\(^{465}\)

(ii) Recordkeeping and Discovery Obligations

BYOD also implicates an employer’s recordkeeping and discovery obligations. To the former, several state and federal laws require employers to either preserve or destroy certain electronic records.\(^{466}\) As to the latter, employers are obligated to both preserve and produce

---

\(^{463}\) **PONEMON INSTITUTE, UNDERSTANDING SECURITY COMPLEXITY IN 21\(^{ST}\) CENTURYY IT ENVIRONMENTS** 10 (FEB. 2011).

\(^{464}\) HIPAA’s Privacy Rule, for example, makes it clear that all “individually identifiable health information” is protected, whether held or transmitted by a covered entity in any form, whether electronic, paper, or oral. See 45 C.F.R. §§ 160; 164.

\(^{465}\) See, e.g., Michigan’s Identify Theft Protection Act, codified at MCL § 445.72.

\(^{466}\) See, e.g., 16 C.F.R. § 682.3. (Under the Fair Credit Reporting Act, “[a]ny person who maintains or otherwise possesses consumer information for a business purpose must properly dispose of such information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal.”)
electronic documents, and failing to do so can lead to court imposed sanctions. Courts are just beginning to address these issues in the context of BYOD. For example, in Cotton v. Costco Wholesale Corp., the court denied the employee-plaintiff’s motion to compel text messages sent or received by employees on their personal cell phones because the employee had not shown that the employer had any legal right to obtain the text messages or that they were in their “possession, control or custody.” In P.R. Telephone Co., Inc. v. San Juan Cable, however, the court found that the company did have a duty to preserve relevant email from the personal email accounts of three of the company’s former officers. Without a great deal of analysis, the court reasoned that the company presumably knew that its officers had used their personal email accounts to manage the company for seven years.

b. Compliance with Employment and Labor Laws

BYOD raises significant issues impacting employer compliance with state and federal employment and labor laws.

(i) Equal Employment Opportunity Laws

The various state and federal anti-discrimination laws generally prohibit employers from taking employment actions against employees on the basis of their protected category. It is likely that employee-owned mobile devices contain information regarding certain demographic statuses protected by federal law: race, color, religion, sex, national origin, age, disability, pregnancy status, and genetic information. More expansive state and local non-discrimination laws also cover other classifications, including height, weight, familial status, marital status, gender identity, and sexual orientation. If the employer legally accesses this information – discussed more below – doing so could potentially waive any future argument that they were not aware of an employee’s protected status.

467 Fed. R. Civ. P. 34. The comments to the amendments provide that “[t]he change clarifies that Rule 34 applies to information that is fixed in a tangible form and to information that is stored in a medium from which it can be retrieved and examined. At the same time, a Rule 34 request for production of “documents” should be understood to encompass, and the response should include, electronically stored information unless discovery in the action has clearly distinguished between electronically stored information and ‘documents.’” Zubulake v. UBS Warburg LLC, 220 F.R.D. 212, 217-18 (S.D.N.Y. 2003) (Zubulake IV).


470 Analogously, the EEOC issued regulations specifically addressing the use of social media by employers (in the context of implementing the Genetic Information Nondiscrimination Act). See 29 C.F.R. § 1635.8(b)(1)(ii)(D) (providing an exception where one “inadvertently learns genetic information from a social media platform which he or she was given permission to access by the creator of the profile at issue”).
Though no court has expressly addressed the issue of the relationship between BYOD and an employer’s obligations to prevent hostile work environments, it is possible that allowing employees to use their personal devices at work could facilitate such claims. In short, employees may see the use of personal devices as separate from work, and thus use the device to send or post messages that constitute sexual or racial harassment. Whether or not an employer is ultimately liable under a hostile work environment theory depends upon several factors – including the identity of the alleged harasser and the steps the employer took to remedy the harassment\(^{471}\) – but it is likely that as technology blurs the line between personal and professional lives, employers will see an uptick in such claims.\(^{472}\)

Additionally, it is feasible that employees could bring traditional adverse action claims involving the inconsistent application of BYOD policies. For instance, an employee claiming that he/she was disciplined for violating a BYOD policy while another employee, who did not belong to a protected category, did the same thing and was not disciplined. Another issue is whether an employer utilizing BYOD would be required to provide accommodations, such as additional software, to the personal device(s) of an employee who is disabled.

(ii) Labor Laws

For those unionized employers, BYOD can expose the employer to significant obligations or liability under state and federal labor laws. First, depending upon the employer’s collective bargaining agreement, it is likely that implementing a BYOD policy is a mandatory subject of bargaining.\(^{473}\) An employer may also need to bargain over the effects of using mobile devices as it relates to how employees perform their job duties. Second, it is possible that BYOD implicates surveillance/monitoring issues. Though employee privacy issues are generally addressed below, to the extent an employer wishes to monitor an employee’s use of his/her personal mobile device to, for example, ensure that the employee is not downloading applications corrupted by malware, an employer may risk an argument that such monitoring constitutes unlawful surveillance of protected, concerted activity under the NLRA. Finally, a union might be able to argue that it has the right to access information contained on personal devices connected to an employer’s network as it relates to, for example, a grievance.


\(^{473}\) In re King Soopers, Inc., 340 N.L.R.B. 628, 628 (2003) (“It is well established that work rules that can be grounds for discipline are mandatory subjects of bargaining.”).
(iii) Wage and Hour Laws

The primary risk associated with BYOD in terms of wage and hour compliance is that BYOD fosters an environment in which non-exempt employees might “work” during non-working time. The general rule under the Fair Labor Standards Act (“FLSA”) is that non-exempt employees must be paid for all hours worked. Unfortunately, there is scant guidance from the courts or the Department of Labor (“DOL”) as to whether the time spent by non-exempt employees accessing work information on their personal device, such as reading or responding to email sent to their company email address on a mobile device, constitutes hours worked for the purposes of the FLSA. There are, however, three compelling reasons why an employer should treat such time as compensable work time.

First, pursuant to the DOL regulations, the term “employ” includes the words “suffer or permit to work.” “Suffer or permit to work” means that if an employer requires or allows employees to work, the time spent is generally hours worked. Thus, time spent doing work not requested by the employer, but still allowed, is generally hours worked, where the employer knows or has reason to believe that the employees are continuing to work and the employer is benefiting from the work being done. Providing non-exempt employees with access to an employer’s network via a mobile device could suggest that employees are expected – infrequently or otherwise – to perform work outside of their regular scheduled working hours. Moreover, permitting such access outside of regularly scheduled working hours would likely undermine an employer’s defense that it did not know or had no reason to believe that its employees were continuing to work.

Second, depending upon the types of activities non-exempt employees would be performing on their mobile devices, it is likely that by accessing an employer’s network, non-exempt employees could engage in activity that is “integral and indispensable” to their everyday on-the-clock “principal activities” which would thus be compensable as “preliminary” or “postliminary” activities.

Another risk raised by the FLSA depends upon whether – and how – the employer reimburses an employee for an employee’s access to the employer’s network. It is likely that BYOD could require employers to reimburse an employee for the added expenses required to access the employer’s network under the FLSA and state laws.

[474] Another risk raised by the FLSA depends upon whether – and how – the employer reimburses an employee for an employee’s access to the employer’s network. It is likely that BYOD could require employers to reimburse an employee for the added expenses required to access the employer’s network under the FLSA and state laws.


[476] Steiner v. Mitchell, 350 U.S. 247, 252-53, 76 S. Ct. 330 (1956); 29 C.F.R. § 790.8. Compare Rutti v. LoJack Corp., Inc., 596 F.3d 1046 (9th Cir. 2010) (car alarm technician’s postliminary activity of required daily portable data transmissions may be compensable time because it is “necessary” to the business and is performed by the employee “primarily for the benefit of the employer”) with Kuebel v. Black & Decker, Inc., 643 F.3d 352 (2d. Cir. 2011) (responding to emails and synchronizing phone before and after work were not integral and indispensable to sales representative’s principal activity so as to render his commute time compensable).
Third, since most email messages only take a short time – seconds to a few minutes – it is possible that non-exempt employees would be engaging in *de minimus* activity that is not compensable under the FLSA. Where a minute here or there checking email might fall within the *de minimus* exception, spending a substantial amount of time on after-hours emails, in excess of a few minutes, may be considered compensable.

It is also worth noting that several employees have recently challenged employer policies – AT&T; Black & Decker; C.B. Richard Ellis; City of Chicago; T-Mobile, USA; and Verizon – requiring non-exempt employees to have access to and respond to emails on mobile devices without proper compensation under the FLSA. Many of these lawsuits resulted in the employees successfully getting their claims conditionally certified as collective actions under 29 U.S.C. § 216(b). Note that at least one of these collective actions was later decertified as the district court determined that determining the company’s liability required a highly individualized analysis as to how each employee used their mobile devices and what expectations were placed on employees by managers for responding to emails during off hours.

Given the uncertain state of the law and the general focus by the plaintiff’s bar on FLSA collective actions, implementing BYOD for non-exempt employees is risky. If employers do choose to grant such access, they should develop a policy with some of the following considerations:

- Limit the non-exempt classifications that are provided access, thus limiting potential exposure to liability.
- Prohibit non-exempt employees from accessing the employer’s network during non-work hours without prior permission (e.g., they are just allowed to check email during work hours but away from their computer).
- Require employees to record all time spent accessing the employer’s network during non-work hours.
- If possible, turn off access to during non-work hours. For example, Volkswagen recently implemented a system that kept its servers from routing messages to Blackberries starting 30 minutes after each shift and ending 30 minutes before the start of the next shift.

---

477 29 C.F.R. § 785.47. *See also Ratti*, supra (remanding to consider whether technician’s postliminary activity fell within the *de minimis* exception).
478 *See, e.g.*, *Allen v. City of Chicago*, No. 10 C 3183, 2013 WL 146389 (N.D. Ill. Jan. 14, 2013) (conditionally certifying FLSA claim where plaintiffs alleged that they were “required to use” work issued mobile devices outside of normal working hours without receiving compensation).
479 *See Zivali v. AT&T Mobility, LLC*, 784 F. Supp. 2d 456 (S.D.N.Y. 2011).
• Train supervisors to not expect or demand non-exempt employees to access the network or check email during non-work hours.

• Enforce the policy by monitoring usage or employing technological solutions to rule out such usage.

• Impose consequences for violations of the policy, while compensating the employee for actual time worked (paying overtime where required).

(iv) Other Laws

Finally BYOD may implicate several other areas of the law. First, employers that access personal information contained on employee personal devices risk liability under various privacy laws, including under the Electronic Communications Privacy Act, state anti-wiretapping and monitoring statutes, and common-law privacy torts. Compounding this risk is, as mentioned above, the ability of employers to “remotely wipe” devices, since such a wipe could destroy not only employer information, but personal information as well. Second, BYOD could exacerbate some of the health risks associated with using mobile devices – like texting and driving, mobile device radiation, and repetitive stress injuries – since BYOD essentially increases employee use of mobile devices. It is possible, therefore, that such health risks could lead to increased liability under state and federal laws designed to protect employee health, such as workers’ compensation laws and those that come under the purview of the Occupational Health and Safety Administration. Finally, employee communications on their personal devices raise privilege questions in the context of litigation. If an employee uses BYOD to communicate with an attorney, for example, whether or not the attorney-client privilege protects the communication likely depends on whether the employee used his/her work account or his/her personal account, as well as the scope of the employer’s policy.  

In addition to the foregoing legal considerations, some issues to consider when implementing a BYOD policy include: (1) what happens to the device and information when employment ends;  

(2) does the employer have the ability to remotely wipe the device; (3) does the employee have a duty to notify the employer if the device is lost or stolen; and (4) do you require the device to have a password or limited access.

Perhaps one of the newest issues to consider with BYOD is the potential liability when an employee uses his or her personal device for work, while engaging in other unlawful behavior.


482 See e.g. Lazette v. Kulmatycki, 949 F. Supp. 2d 748 (N.D. Ohio 2013) (it may be legal under the SCA for an employer who owns and pay for a phone to access an employee’s personal email account after the employee returns the phone but does not erase their personal email from the device).
For example, Connecticut prohibits cell phone use by drivers while “operating” a motor vehicle. 483 “Operating a motor vehicle” means operating a motor vehicle on any highway . . . including being temporarily stationary due to traffic, road conditions or a traffic control sign or signal, but no including being parked on the side or shoulder of any highway where such vehicle is safely able to remain stationary. 484 Employers should make sure that their BYOD policies are updated and consistent with their cell phone use policy.

In sum, BYOD raises a variety of concerns for employers, most of which have not been directly addressed by the Courts. Accordingly, employers should tread cautiously as they institute such policies.

483 Conn. Gen. Stat, § 14-296aa(b)(1)