SEYFARTH SHAW

Navigating Workplace Privacy Issues

Karla Grossenbacher
Meredith-Anne Berger
Stacey Blecher
Ari Hersher
Selyn Hong
Elizabeth Levy

TABLE OF CONTENTS

I. Introduction 1

II. Monitoring Employee E-Communications 1

A. Relevant Laws 2

B. Reviewing Employee's Web-based Email Accounts 2

III. The Implications of Bring Your Own Device Policies 4

A. Privacy Concerns 5

B. Cost Implications 6

1. Reimbursements and Kickbacks 6

2. Allocating Responsibility for Costs Associated With the Use of Personal Devices 7

3. Litigation Revolving Around the Costs Associated With the Use of Personal Devices 7

C. Additional Wage & Hour Issues 8

D. Data Security Issues 11

E. Safety and Liability Concerns Arising from Cell Phone Use in the Workplace 13

F. Litigation Concerns 14

G. Tax Implications of BYOD 14

IV. Restricting, Monitoring and Scrutinizing Employee, Applicant and Litigant Use of the Cloud 15

A. Security Breaches and Misappropriation of Trade Secrets 15

B. Wage & Hour Issues Arising From The Cloud 16

C. Specific Legal Pitfalls, Including Compliance With The Health Insurance Portability and Accountability Act (HIPAA) 17

D. Litigation Challenges Presented By The Cloud 18

V. Employee Internet Activity 19

A. Risks Associated with Internet Activity 19

B. Job Applicants 19

VI. Employer Control Over Employee Social Networking Service (SNS) Posting 20

A. National Labor Relations Act (NLRA) 20

1. Language of the Act 20

2. Determining Whether or Not a Policy Will Have a Chilling Effect 21

3. Implementation of Section 7 21

4. Effectiveness of Savings Clauses 23

5. Constructing a Compliant Policy 23

B. Data Theft Issues 24

C. Prohibitions on Forced Disclosure of Personal Logins & Passwords 24

1. Federal Law 24

2. State Law 24

3. Creating a Compliant Policy 25

D. Litigation Discoverability of SNS Posts, Photos, and Messages 26

1. eDiscovery of Social Media 26

2. Standards and Methods of Access 27

E. Social Media's Role in Emotional Distress Claims 27

F. Tips for Employers 28

The eWorkforce: Restricting Employees' Use of Technology, Social Media and The Cloud

Laura J. Maechtlen* and Karla Grossenbacher
Seyfarth Shaw LLP

I. Introduction

Employers have a variety of legitimate reasons to monitor their employees' use of technology, social media and the cloud. Indeed, the "e-workplace" continues to expand—from basic internet usage and social media by employees, to user generated content such as blogs, wikis, social networking sites and microblogging sites. For this reason, the problems facing today's employers[1] who manage the "e-workplace" continue to expand, and include combating security breaches in the face of cloud storage and Bring-your-own-device (BYOD) policies, complying with state and federal law in monitoring employees and limiting employee internet activity and understanding the discovery limitations related to social network posts, as well as a variety of statutory obligations governing use and protection of data, among a variety of other related issues.

Although not an exhaustive summary, we discuss a variety of key topics related to the "e-workplace" below.

II. Monitoring Employee E-Communications

Over the last decade, communication via email and text has become a vital part of how many of us communicate in the workplace. In fact, most employees could not fathom the idea of performing their jobs without the use of email. For convenience, employees often use one device for both personal and work-related communications, whether that device is employee-owned or employer-provided. Some employees even combine their personal and work email accounts into one inbox (which sometimes results in work emails being accidentally sent from a personal account). The use of email, text and other electronic communications, as well as the blurring of the lines between personal and work-related communications, creates novel legal issues when it comes to determining whether an employer has the right to access and review all work-related communications made by its employees.

Employers have legitimate business reasons for monitoring employee communications. Take, for example, the scenario in which an employee leaves her employment, and the employer is concerned that she has taken proprietary information or solicited clients in violation of her duty of loyalty or a contractual agreement. Another common scenario that gives rise to the need for employers to review all of an employee's work-related emails is when the employer is in litigation that requires production of employee communications.

[1] This paper focuses on private, rather than public, employers.

A. Relevant Laws

An employer's ability to review electronic communications is governed generally by the Electronic Communication Privacy Act (ECPA) [2] and the Stored Communications Act (SCA) [3]. The ECPA prohibits the interception of electronic communications, and the term "interception" as used in the ECPA has been interpreted so narrowly that this title of the ECPA rarely comes into play in cases involving an employer's review of employee email or texts.

Through the SCA, Congress later added provisions to the law that would limit access to stored electronic communications. The SCA prohibits employers from intentionally accessing "without authorization a facility through which an electronic communication service is provided."[4] However, there is an exception to this prohibition for "the person or entity providing a wire or electronic communications service." Thus, employers can generally access emails that are on the email server it maintains and provides for employee use. However, to avoid a common law invasion of privacy claim, caution should be used in reviewing sensitive emails of a personal nature sent through the employer's email server unless the employer has a policy that expressly states employees have no expectation of privacy in emails sent on the employer's email server and reserving the right to monitor.

B. Reviewing Employee's Web-based Email Accounts

With regard to an employer's review of employee emails sent through web-based email accounts like Gmail or Hotmail, the most frequent scenario confronted by courts is one in which a former employer accesses the web-based email of a former employee, looking for evidence of malfeasance. In these cases, the former employer is typically able to access the former employee's web-based email account because the employee has saved her username and password on a device provided by the employer, which was returned at termination, or failed to delink an account from such a device. In these cases, courts have been reluctant to punish the former employee for failing to take appropriate steps to secure their own personal, and allegedly private, communications.

For example, a district court in New York[5] considered an employee's claim that his former employer's review of emails in his Hotmail account after his termination violated the SCA because it was unauthorized. The defendant argued that its review of the emails did not violate the SCA because the employee had implicitly authorized its review of the emails on his Hotmail account because the employee had stored his username and password on the employer's computer system or forgot to remove such an account from an employer-provided phone before returning it.

The court rejected this argument, holding that it was tantamount to arguing that, if the employee had left his house keys on the reception desk at the office, he would have

[2] 18 U.S.C. § 2510 et seq.
[3] 18 U.S.C. § 2701.
[4] *Id.*
[5] *Pure Power Boot Camp v. Warrior Fitness Boot Camp*, 587 F. Supp.2d 548 (S.D.N.Y. 2008).

been implicitly authorizing his employer to enter his home without his knowledge. The court also noted that the employer's computer usage policy did not provide the necessary authorization because it only referred to communications sent over the employer's systems.

Likewise, a district court in Ohio[6] confronted with similar facts, refused to hold the plaintiff responsible for his own failure to safeguard his information. In this case, the employee had turned in a company-issued blackberry upon termination without first deleting the Gmail account he had added to the phone. The former employer reviewed the emails in the former employee's Gmail account, and the former employee alleged that this violated the SCA. The former employer argued that the former employee had negligently or implicitly consented to their review of the emails in her Gmail account by returning the blackberry to the company without deleting the account. However, the court held that the employee's "negligence" in leaving the Gmail account on her phone when she turned it in was not tantamount to her authorizing the defendant to review the emails on her Gmail account.

However, a federal district court in California[7] reached a different result in a case involving text messages. In this case, a company had sued its former employee for misappropriating trade secrets when it discovered, upon his termination, a number of text messages on the former employee's company-issued iPhone that documented his misappropriation. The former employee had forgotten to delink his Apple account from the company phone he returned, and thus, his text messages continued to go to the phone — and his former employer. The court granted the company's motion to dismiss the former employee's counterclaim that the company's review of his text messages violated the SCA. The court held that text messages stored on phones are not in "electronic storage" within the meaning of the SCA, citing a Fifth Circuit case that reached the same conclusion about text messages. Of course, a violation of the SCA is not the only issue in these cases.

For example, in this case, the employee also alleged that his employer had invaded his privacy. However, the court held that the employee had no reasonable expectation of privacy in a company-owned phone that was no longer in his possession. In contrast to the two cases above, the court found that the employee's failure to undertake precautions to maintain the privacy of his text messages showed he had no right to exclude others from accessing them.

There are some inconsistent holdings under the ECPA, which was enacted in 1986, due to Congress' failure to act to bring amend the statutory provisions to take into consideration modern technologies. However, the main lesson from the cases is that, if an employer wants to have the ability to review all employee communications that take place in the workplace, the employer needs to have, at a minimum, a policy that specifically provides for the right to monitor and review, for legitimate business reasons, any work-related communications made by the employee on a device provided by the

[6] *Lazette v. Kulmatycki*, 949 F.Suup.2d 748 (N.D. Ohio 2013).
[7] *Sunbelt Rentals v. Victor*, 43 F. Supp. 3d (N.D. Cal. 2014).

company or a personal device used for work purposes. (Although the SCA does not require any showing about the employer's motives in accessing the emails, a traditional invasion of privacy analysis would take this into account.) As a practical matter, the employer may not have the ability to access such accounts, but where access is available, this policy language is critical.

III. The Implications of Bring Your Own Device Policies

Bring-your-own-device ("BYOD") policies are being utilized more than ever. Studies show that more than half of North American and European companies are implementing these policies.[8] There are both "pros" and "cons" in adopting a BYOD policy.

Benefits of adopting a BYOD policy[9] can include:

- Lower equipment costs for the employer;
- Convenience for employees, including a general boost to employee morale;
- Higher productivity, with easier access to company information and methods of work; and,
- Greater flexibility for workers.

Cons of BYOD policy[10] might include:

- Strain on a company IT Department, with more types of phones/devices to support;
- Increased compliance concerns, such as loss of data, potential exposure of confidential information, and cost-sharing, and off-the-clock work;
- Potential loss of bulk purchasing power in equipment and cell phone use/data packages;
- Heightened need to have the right to control, access, and monitor devices since equipment is not owned by the Company;

[8] Allyson Haynes Stuart, *Making Sure BYOD Does Not Stand for "Breach Your Organization's Data*," 27 S. CAROLINA LAWYER 45, 45 (2016).
[9] Robert Milligan & Michael Wexler, *Frequently Asked Questions Regarding Trade Secret Disputes and Employment Risks Answered*, TRADING SECRETS (Sept. 18, 2015), http://www.tradesecretslaw.com/2015/09/articles/computer-fraud-and-abuse-act/frequently-asked-questions-regarding-trade-secret-disputes-and-employment-risks/?utm_source=Seyfarth+Shaw+-.
[10] *Id*.; *see also* Karla Grossenbacher, Stacey L. Blecher & Meredith-Anne Berger, *8 Key Components of An Effective BYOD Policy*, LAW 360 (June 17, 2016, 11:49 AM), https://www.law360.com/articles/807542/8-key-components-of-an-effective-byod-policy.

- Risks to the employer's information security due to lost or stolen devices, failure to return devices and software and apps added by employee to phone;

- Difficulties in corralling data in response to litigation or other government process; and,

- Compliance risks if BYOD policy is not implemented correctly and/or policy is not followed in day-to-day business (wage and hour issues, security, litigation, intellectual property, etc.).

A. Privacy Concerns

With the increasing popularity of BYOD in the workplace, it is crucial for an employer to manage employee privacy expectations, which must strike a balance between an employee's reasonable expectation of privacy, and the employer's control over its own information.

The very nature of BYOD highlights the employee privacy challenges at issue. With a BYOD policy, employees use the same devices they use for work to engage in personal computing that involves a host of private activities and content, including web history, personal email, photos, social media profiles, chat histories, personally identifiable information, music, software, user names and passwords and financial information, such as Apple "iPay". For all these reasons, use of a BYOD policy requires employer to determine how they should monitor employee behavior while they are using personal devices for work related activities because—when it comes to personal devices—it is known that personal and private activities are likely to take place on the device, and for privacy reasons, the same types of monitoring used for company devices and equipment may not be appropriate for reasons cited above.

Overall, private employers need to carefully consider their intended goals when it comes to monitoring their employees' use of their own devices, and balance those goals against these privacy concerns and potential legal limitations. Employers should make their employees aware of the privacy trade-offs and the reasonable expectations of privacy related to their use of a personal device for work. For example, a BYOD policy should provide clear notice to the employee that the company information on the device belongs to the employer, and that this may lead to diminished privacy for the employee, and the employer should obtain a signed acknowledgement of this policy.[11] In addition, employers should reserve the right to monitor, and employees should give consent to be monitored in writing.

[11] Justin T. Curley & Laura Maechtlen, *No LOL Matter: Employers Must Take Care When Adopting BYOD Policies*, EMP'T. L. LOOKOUT (May 15, 2014), http://www.laborandemploymentlawcounsel.com/2014/05/no-lol-matter-employers-must-take-care-when-adopting-byod-policies/?utm_source=Seyfarth+Shaw+-+Employment+Law+Lookout&utm_campaign=42403c7678-RSS_EMAIL_CAMPAIGN&utm_medium=email&utm_term=0_0dfec06b7a-42403c7678-70405893.

B. Cost Implications

1. Reimbursements and Kickbacks

The Fair Labor Standards Act (FLSA) does not explicitly require employers to reimburse employees for work-related expenses. The FLSA only mentions reimbursement in the context of "regular rates."[12] The act states that properly reimbursable work-related expenses incurred by employees need not be considered a part of the "regular rate" of payment for the purposes of calculating overtime.[13] Still, when employees are expected to provide tools necessary for job performance, their employers are required to pay them back "to the extent that the cost of such tools purchased by the employee cuts into the minimum or overtime wages required to be paid him under the [FLSA]."[14] Thus, an employer is in violation of federal law where its employees are paid the minimum wage but are required to use their own cell phone devices without reimbursement.

Employers should also consult their state's law requirements about whether or not employees are entitled to reimbursements for work-related use of their mobile devices. For instance, under California Labor Code section 2802, employers are required to indemnify employees for reasonable and necessary expenses incurred as a direct consequence of the discharge of their duties.[15] Under California law, an employee must be permitted to challenge the amount of any lump-sum payment and if employee shows that lump sum is inadequate, and employer must make up the difference. Other states, such as New York (for non-exempt employees)[16], Massachusetts[17] and New Jersey[18], provide statutory guidance or case law that suggests where an employer voluntarily agrees to reimburse expenses in a company policy, it must abide by that agreement (i.e. relating back to language similar to contractual law). We believe this to be the case in each state where a BYOD policy is created. Moreover, Washington, DC, requires employers to pay for "cost of . . . maintaining any tools required of the employee in the performance of the business of

[12] See Section 7(e)(2).
[13] 29 U.S.C. § 207.
[14] 29 C.F.R. § 531.35.
[15] Cal. Lab. Code § 2802; *see also Gattuso v. Harte-Hanks Shoppers, Inc.*, 42 Cal. 4th 554, 575, 169 P.3d 889, 902 (2007).
[16] *See* New York Lab. L. § 198c (providing reimbursements must be paid in accordance with an agreement with non-exempt employees within thirty days).
[17] *Fraelick v. PerkettPR*, Inc., 83 Mass. App. Ct. 698, 708, 989 N.E.2d 517, 524 (Mass. App. Ct. 2013) ("employer engaged in a pattern of nonpayment, coupled with continued demands that the employee advance expense monies in ever-increasing amounts, and fired her turned an otherwise "permissible expense reimbursement arrangement designed to benefit employees" and "abandoned and replaced with a policy and practice which required the employee' to advance expenses for the "employer's benefit").
[18] The New Jersey Department of Labor considers this a "fringe benefit" which is an obligation for the employer and the employee, under which both must comply with the terms of the agreement and may establish the conditions under which the employee would be entitled to expense reimbursement. The NJ DOL will enforce an employer's agreed-upon obligation to provide a fringe benefit or that pursuant to an employment agreement. *See* McGillivary, Wage & Hour Laws, Vol. II, § IV.B.

the employer." However, we are not aware of any guidance relating to the determination of whether a cell phone is a "required" "tool."[19]

2. Allocating Responsibility for Costs Associated With the Use of Personal Devices

Employers that do not reimburse work-related cell phone expenses must make sure that each employee's total wages less the work-related cell phone expense he or she incurs is higher than the federal (or state) minimum wage.[20] This method might prove to be tedious, so as an alternative employers should consider implementing an expense reimbursement policy. Specifically, employers operating in California must have a reimbursement policy in place, or they run a risk of claims arising under Labor Code Section 2802. [21]

Compliance is not easy, but there are a variety of best practices. An employer's BYOD policy should clearly state the costs that each party is responsible for related to the use of personal mobile devices in the workplace.[22] Where the employee does not incur additional costs for business usage, the employer may provide a reimbursement for time the employee spent on the device. However, where an employee incurs expenses outside of his or her normal plan due to business use, the employer must reimburse the employee for the actual expenses incurred. This is especially true in California, which requires reimbursement for all reasonable and necessary business expenses.[23]

3. Litigation Revolving Around the Costs Associated With the Use of Personal Devices

A California court held in *Cochran v. Schwan's Home Service, Inc.* that employees who are required to use personal cell phones for work are entitled to reimbursement for "some reasonable percentage" of the personal cell phone bill, regardless of whether the cost is incurred "by a third party or at all."[24] The plaintiff in

---

[19] D.C. Municipal Rules §910.

[20] *See Oram v. SoulCycle LLC*, 979 F. Supp. 2d 498, 507 (S.D.N.Y. 2013) ("[U]nder New York law, employers do not have to reimburse employees for business expenses, including "tools of the trade," so long as not doing so does not reduce the employee's wage below the minimum wage.") *See also* See *Lin v. Benihana Nat'l Corp*., 755 F.Supp.2d 504, 511–12 (S.D.N.Y.2010) (finding that as employers can require employees to bear the costs of tools of the trade as long as it does not reduce their wages below minimum wage, plaintiffs failed to present their allegations with sufficient specificity because they did not provide details regarding the cost of the tools each purchased, nor did they state whether those costs reduce their wages below the minimum threshold); see also *Maldonado v. La Nueva Rampa, Inc*., 10 Civ. 8195(LLS)(JLC), 2012 WL 1669341, *7–8, 2012 U.S. Dist. LEXIS 67058, *25 (S.D.N.Y. May 14, 2012) (holding that employees could recover the costs of their equipment and repairs because such costs dropped the employees below the minimum wage).

[21] *Id.*

[22] Curley, *supra* note 4.

[23] Cal. Lab. Code § 2802.

[24] *Cochran v. Schwan's Home Service, Inc.*, 228 Cal. App. 4th 1137, 1144 (2014).

Cochran brought a class action on behalf of customer service managers whom Home Service failed to reimburse for work-related use of their personal mobile devices.[25]

Unfortunately, post-Cochran, there have been Cochran-inspired class actions. In *Araiza v. The Scotts Company, LLC*, Los Angeles Superior Court Case No. BC570350 (filed January 26, 2015), the plaintiffs asserted class claims alleging a failure to reimburse employee business expenses, in violation of Section 2802, and also alleged a violation of Section 17200 of the Business and Professions Code. The plaintiffs expressly cited *Cochran*, arguing that *Cochran* requires the defendant employer to "maintain an expense reimbursement policy and/or practice stating that Defendant will affirmatively reimburse Class Members for a reasonable portion of their monthly personal cell phone bills and expenses necessarily incurred in their discharge of their duties." This case joins the many pre-Cochran class actions already invoking Section 2802 to claim expense reimbursement for work-related personal mobile device usage.

As another example, the holding in *Cochran* was recently cited by Judge Edward Chen of the United States District Court for the Northern District of California in *O'Connor v. Uber Techs., Inc*.[26] There, Uber argued that it should not be liable for phone expenses to drivers where said expenses were not actually incurred (i.e., where the driver had an unlimited data plan).[27] In rejecting this argument, Judge Chen referenced *Cochran's* language stating that whether or not the cell phone plan is unlimited is irrelevant.[28] O'Connor demonstrates that plaintiffs in class actions may rely on *Cochran* (or arguments similar to those asserted in Cochran) in seeking reimbursement for work-related cell phone expenses.[29]

C. Additional Wage & Hour Issues

The FLSA defines "employ" as, to "suffer or permit to work."[30] This means that if an employer has required or allowed an employee to work, then the time spent is considered "hours worked."[31] The FSLA also sets forth the minimum hourly rates of compensation for employees and federal rules for overtime pay.[32] Under the FLSA, employees are generally entitled to one-and-a-half times their regular rate of compensation when they work more than forty hours in a workweek.[33] Failure to comply with the FLSA minimum wage and overtime provisions can subject employers to penalties.[34]

---

[25] *Id.* at 1140.
[26] *O'Connor v. Uber Techs.*, Inc., 311 F.R.D. 547 (N.D. Cal. 2015).
[27] *Id.* at 567.
[28] *Id.*
[29] *See, e.g.*, *Tehrani v. Macy's W. Stores, Inc.*, No. 07286, 2016 U.S. Dist. LEXIS 51713, at *22 (C.D. Cal. Apr. 18, 2016).
[30] *FLSA Overtime Calculator Advisor*, UNITED STATES DEP'T OF LABOR, http://webapps.dol.gov/elaws/whd/flsa/hoursworked/screen1d.asp.
[31] *Id.*
[32] 29 U.S.C. § 206.
[33] 29 U.S.C. § 207.
[34] *See* 29 U.S.C. § 216.

Many states and municipalities have also enacted their own minimum wage laws.[35] Some states have laws governing overtime as well. Many of the states have laws similar to the FLSA: namely, laws that require employers to pay employees at one-and-a-half times their regular rate of compensation when they work more than forty hours a week and/or more than eight hours a day.[36] There are certain states whose laws differ, such as Kansas and Minnesota, which have longer workweeks.[37]

The significant danger for employers with BYOD policies is off-the-clock work performed by non-exempt employees, including overtime work. Employees who are not exempt from overtime pay must be paid for all work performed, whether in the office, at home, or commuting — a "suffer or permit" standard as the FLSA instructs.[38] The use of smartphones and remote access work, the line between "working hours" and "non-working hours" can easily become blurred. This often occurs with remote access to email outside of work through a smart phone, the ability to "log in" to work through a remote device and/or workers ability to be contacted with "24/7" accessibility.

---

[35] *See* Alaska Stat. Ann. § 23.10.065(a); Ariz. Rev. Stat. Ann. § 23-363; Ark. Code Ann. § 11-4-210(a)(2); S.B. 3, 2015-2016 Leg., Reg. Sess. (Cal. 2016); Cal. Lab. Code § 1182.12.); Wage Order No. 32 § 3; Conn. Gen. Stat. Ann. § 31-58(i); 19 Del. C. § 902(a)(1); D.C. Code § 32-1003(a)(3); Fla. Stat. § 448.110; Ga. Code Ann. § 34-4-3; Haw. Rev. Stat. § 387-2(a); Idaho Code § 44-1502(1); 820 Ill. Comp. Stat. 105/4(a)(1); Ind. Code Ann. § 22-2-2-4; Iowa Code § 91D.1(1); Iowa Admin. Code r. 875-215.1(1); Kan. Stat. Ann. § 44-1203(a)(2); Ky. Rev. Stat. Ann. § 337.275(1); Me. Rev. Stat. tit. 26 § 664(1); Md. Code Ann., Lab. & Empl. § 3-413; Mass. Gen. Laws ch. 151, § 1; Mich. Comp. Laws § 408.414(1); Minn. Stat. § 177.24; Mo. Rev. Stat. § 290.502; Mont. Code Ann. § 39-3-409; Neb. Rev. Stat. § 48-1203(1)(c); N.J. Admin. Code § 12:56-3.1(a); N.J. Stat. Ann. § 34:11-56a4; N.M. Stat. Ann. § 50-4-22(A); N.Y. Lab. Law § 652(1); N.Y. Lab. Law § 652(1); N.C. Gen. Stat. Ann. § 95-25.3(a); N.D. Cent. Code § 34-06-22; Ohio Const. art. II, § 34a; S.B. 1532, 2016 Reg. Sess. (Or. 2016); 43 Pa. Stat. Ann. § 333.104(a.1); R.I. Gen. Laws § 28-12-3(h); S.D. Codified Laws § 60-11-3; Tex. Lab. Code § 62.051; Utah Admin. Code r. 610-1-3; Vt. Stat. Ann. tit. 21, § 384; W. Va. Code § 21-5C-2(a)(4); Wyo. Stat. Ann.§ 27-4-202.

[36] These states include California, Connecticut, the District of Columbia, Hawaii, Indiana, Kentucky, Maine, Maryland, Massachusetts, Michigan, Missouri, Montana, Nevada, New Jersey, New York, North Carolina, North Dakota, Ohio, Oregon, Pennsylvania, Rhode Island, Vermont, Washington, West Virginia and Wyoming. *See* Cal. Lab. Code § 510; Conn. Gen. Stat. Ann. § 31-76C; D.C. Code § 32-1003(c); Haw. Rev. Stat. § 387-3(a); Ind. Code Ann. § 22-2-2-4(k); Ky. Rev. Stat. Ann. § 337.285(l); Me. Rev. Stat. tit. 26 § 664(3); Md. Code Ann., Lab. & Empl. § 3-420(a); Mass. Gen. Law ch. 151, § 1A; Mich. Comp. Laws § 408.414a(1); Mo. Rev. Stat. § 290.505(1); Mont. Code Ann. § 39-3-405(1); Nev. Rev. Stat. § 608.018; N.J. Stat. Ann. § 34:11-56a4; N.M. Stat. Ann. § 50-4-22; N.Y. Comp. Codes R. & Regs. tit. 12, § 142-3.2; N.C. Gen. Stat. Ann. § 95-25.4; N.D. Admin. Code 46-02-07-02(4); Ohio Rev. Code Ann. § 4111.03(A); Or. Rev. Stat. § 653.261; Or. Admin R. 839-020-0030(1); 43 Pa. Stat. Ann. § 333.104(c); 34 Pa. Code 231.41; R.I. Gen. Laws § 28-12-4.1(a); Vt. Stat. Ann. tit. 21, §§ 382, 384; Wash. Rev. Code § 49.46.130(1); W. Va. Code § 21-5C-3(a); Wyo. Stat. Ann. § 16-6-110.

[37] *See* Kan. Stat. Ann. § 44-1204(a); Minn. Stat. § 177.25.

[38] California employers must take extra precaution to avoid liability for hours worked because the law diverges from the FLSA in many respects. *See Complying with California Overtime Payment Law*, SOC'Y FOR HUM. RESOURCE MGMT. (January 1, 2014), https://www.shrm.org/templatestools/toolkits/pages/californiacomplyingwithcaliforniaovertimeandwagepaymentlaw.aspx; *Morillion v. Royal Packing Co*., 22 Cal.. 4th 575 (2000) (holding that hours worked is the time spent subject to the employer's control, not simply the time spent on activities required by the employer); *Lenahan v. Sears, Roebuck & Co*., 266 F. App'x 114, 118-19 (3d Cir. 2008) (Washington law is similar to California law in this respect); *but see* Conn. Agencies Regs. § 31-60-11(a) (where hours worked is defined as "all time during which an employee is required by the employer to be on the employer's premises or to be on duty, or to be at the prescribed work place, and all time during which an employee is employed or permitted to work, whether or not required to do so.")

Indeed, organizational expectations or the culture of certain workplaces may dictate a "24/7" expectation of work. While the ease of access on a personal device is certainly valuable to the business, such ease can be a double-edged sword when it comes to properly compensating non-exempt employees.

For all these reasons, it is critical to monitor and track off-the-clock work to accurately compensate employees, which can be difficult for many employers. Most timekeeping by non-exempt employees is self-reported, either on a physical timesheet or timekeeping software.

Establishing strict policies against off-the-clock work for non-exempt employees is a good first-step to circumvent wage and hour actions. A program that tracks the amount of time logged on to a remote access site would solve overtime concerns, but potentially raises privacy issues. If litigation arises and/or an administrative wage claim is filed, a factfinder will be more concerned with the number of hours actually worked and compensated, rather than what a policy says or the employer's inadequate records that may tell part of a story. Accordingly, employers and managers of non-exempt employees need to train their employees on recording working hours and to set expectations about off-the-clock work.

In an effort to avoid off-the-clock work, employers should consider:

- Prohibiting all off-the clock work and instruct non-exempt employees to record all time worked;
- Developing a policy and procedure for non-exempt employees to easily capture and report such time so that these employees will be paid for all hours worked;
- Including a statement in the policy stating that time spent by non-exempt employees responding to e-mails and answering telephone calls while out of the office should be considered "hours worked";
- Prohibiting non-exempt employees from responding to e-mails or telephone calls after work hours;
- Requiring prior written authorization to work remotely or via mobile device;
- Training managers to minimize sending e-mails to or calling non-exempt employees before or after regular work hours to mitigate the risk of off-the-clock work;
- Training managers to indicate in before or after hours e-mails whether an immediate response is required or whether it can wait until regular business hours;

- Ensuring leave of absence policies state that employees should not perform work during a leave of absence, including responding to calls and e-mails received during a leave of absence;

- A timecard "certification" whereby each employee certifies the accuracy of their time reported each pay period; and,

- A robust reporting and complaint procedure, so employees have many avenues to complain about any actual or perceived requests by managers or supervisors to work off-the-clock.

D. Data Security Issues

Failing to implement a clear BYOD policy can lead to serious consequences for the security of an employer's data, and subsequently, that of its clients or customers. BYOD users should be aware of the risks associated with accessing and exchanging data over unsecured networks. Employers will also want to ensure both data security and appropriate data privacy.

Erosion of data security issues could result from routine use of personal devices. No matter how hard they try, employers may never be able to ensure that only pre-approved and authorized persons have access to their employees' devices. For example, if an employee takes her device for repair, she has to give the device password to a repair-person, or may be required to leave the phone in the store overnight or ship it to a remote location. If an employer handles financial data or healthcare data as part of its business, leaving a device store may be considered a data breach and trigger reporting requirements.

In addition, the use of third-party apps can be problematic. For instance, many people use tools such as Siri or other personal assistant apps to send e-mails, make calendar appointments, etc. Apple stores (in the cloud) everything you tell Siri for two years. Therefore, without intending to, employees may be sharing sensitive information with unauthorized parties simply by using the common features on their phone or tablet.

Alarmingly, and potentially more concerning than data security issues arising from typical device use by well-intentioned employees, BYOD policies have "introduced an entirely new way to pilfer corporate information. It may be as simple as a contact list, or as complex as a source code for a new software release. Given that the total losses attributed to IP theft of all types are in the hundreds of billions of dollar annually, it is not something to ignore."[39]

There are several steps that employers can take to prevent the disclosure of sensitive information, including an employer's trade secrets, private third-party information, and other confidential and proprietary information. For instance, employers

[39] Trent Livingston, *Today's Connected Employee: A License to Steal*, TRADING SECRETS (Sept. 25, 2014), http://www.tradesecretslaw.com/2014/09/articles/trade-secrets/todays-connected-employee-a-license-to-steal/.

can create a policy making it clear that the employer has an unfettered right to access and monitor work-related data on the device.[40] Employers should require employees to:

- Use strong passwords;
- Install encryption software provided by the employer, and agree to not modify the software;
- Install any security updates provided by the device-maker or the employer;
- Notify the employer immediately if their device is lost or stolen;
- Provide adequate physical protection for devices;
- Permit and enable a remote-wipe feature applicable to the employer-related data, so that sensitive employer data can be erased if the device is lost or stolen;
- Purge data from devices before they are replaced or redeployed;
- Install appropriate safeguards against malware or spyware;
- Ensure frequent backups of data;
- Update computer operating systems to ensure they contain the latest security protections;
- Configure software and network settings to minimize risk;
- Encrypt sensitive information and identify metadata from electronic documents before transmission;
- Avoid "wifi hotspots" in public places when transmitting confidential information;[41]
- Create culture of confidentiality through training and other communications; and,
- Collect and image devices of departing employees.

Further, employers should conduct a thorough exit interview prior to any employee separation. Employees should be given a written reminder of their ongoing obligations relating to trade secrets, as well as confidentiality and social networking

[40] Grossenbacher, et al., *supra* note 3.
[41] *Id.*

obligations. The employer should also ensure that all company property is returned, including that which is on personal devices.[42]

Employers that suffer a loss from employee data theft are not always left without a remedy. The Computer Fraud and Abuse Act (CFAA) exposes those who misappropriate information located on a protected computer to criminal liability. The CFAA defines "protected computer" as a computer exclusively used by a financial institution or by the United States Government, or a computer not exclusively used by the U.S. Government or a financial institution if the offense affects the government's or financial institution's use of said computer.[43] When an employee misappropriates sensitive information or sabotages employer computers, the employer might have a claim under the Computer Fraud and Abuse Act (CFAA) if it suffered loss or damage.[44]

E. Safety and Liability Concerns Arising from Cell Phone Use in the Workplace

Security is not the only concern. OSHA concerns may also arise. Distracted driving is the most common cause of workplace deaths. Cell phones distract employees with a constant temptation to text, make calls, and play games.[45] Certainly this risk is not limited to a BYOD program. However, if the employer is formally allowing the employees to use personal devices for work through such a program, the lines of liability blur when accidents occur when the employee is using his/her phone for work purposes.

In a 2010 open letter to employers, Assistant Secretary of Labor for the Occupational Safety and Health Administration (OSHA) David Michaels said, "It is your responsibility and legal obligation to have a clear, unequivocal and enforced policy against texting while driving….Companies are in violation of the Occupational Safety and Health Act if, by policy or practice, they require texting while driving, or create incentives that encourage or condone it, or they structure work so that texting is a practical necessity for workers to carry out their jobs. OSHA will investigate worker complaints, and employers who violate the law will be subject to citations and penalties." OSHA has used its General Duty Clause, Section 5(a)(1) of the Occupational Safety and Health Act, to issue citations and proposed penalties in these circumstances. OSHA has placed "distracted driving" which can include texting, and possibly cell phones used for telephone calls while driving (which is becoming increasingly regulated in many states) among the "recognized hazards" under the General Duty Clause to employee safety. Penalties for willful violations of OSHA under the General Duty Clause can be as high as $124,709.[46]

---

[42] Milligan, *supra* note 2.
[43] 18 U.S.C. § 1030.
[44] *Id.*
[45] Mark A. Lies, II and Adam R. Young, *Cell Phones in the Workplace: Protecting Employee Safety*, EMP'T. L. LOOKOUT (Oct. 13, 2016), http://www.laborandemploymentlawcounsel.com/2016/10/cell-phones-at-the-workplace-protecting-employee-safety/.
[46] *Id.*

There are also risks for employees who use their own devices to play games, such as the popular "Pokemon Go" app, which encourages users to follow and "catch" Pokemon using their cell phones to pin their location. If used in the workplace, or while off-site while working in the scope of the employer's business, liability is a concern with respect to both personal injury and employment actions.[47] Employers should consider prohibiting employees from downloading programs that may expose employers to liability, as well as enforcing a rule prohibiting distracting or dangerous conduct while working.[48]

F. Litigation Concerns

BYOD also raises a variety of litigation concerns for employers. As an initial matter, workplace investigations involving personal devices may create additional hurdles for an employer. If an image of a device's hard drive is needed for an investigation of a security breach or for e-Discovery purposes, the captured data is likely to include private/personal information of the employee. Organizations can try to limit the scope of an investigation or data capture involving a personal device, but if they fail to preserve data that may be evidence in litigation they could face spoliation problems in court or miss key information needed for an investigation or remediation of a breach. BYOD policies can also present problems during the discovery process, the litigation hold process, and in preserving privilege.

G. Tax Implications of BYOD

The complexity of the tax implications of BYOD policies makes it very important for employers to clearly define the tax aspect of the policy at the early stages of development. The Internal Revenue Service (IRS) released Notice 2011-72, which was intended as guidance regarding employers that reimburse employees for the business use of their personal cell phones. This Notice was silent on the treatment of reimbursements resulting from BYOD policies, so the IRS released a subsequent Memorandum, which provided guidance on the tax treatment of BYOD devices.[49] Essentially, the IRS intended for BYOD policies and employer-provided cell phone policies to have similar tax treatment.[50]

For employers this means "when an employer provides an employee with a cell phone [or the employee provides his or her own cell phone] primarily for noncompensatory business reasons, the IRS will treat the employee's use of the cell phone for reasons related to the employer's trade or business as a working condition fringe benefit," which is excludable from the employee's income.[51] Examples of

---

[47] Karen Kidd, *'Any Day Now': Lawsuits Inevitable Over Pokemon Go, Labor Attorney Says*, FORBES (July 27, 2016, 1:11 PM), http://www.forbes.com/sites/legalnewsline/2016/07/27/any-day-now-lawsuits-inevitable-over-pokemon-go-labor-attorney-says/#2c446e6f46e1.

[48] Karla Grossenbacher & Parnian Vafeenia, *Pokemon NO: New App Creates Risks for Employers*, GLOBAL PRIVACY WATCH (July 20, 2016), http://www.globalprivacywatch.com/2016/07/pokemon-no-new-app-creates-risks-for-employers/.

[49] I.R.S. Mem. SBSE-04-0911-083 (Sept. 14, 2011).

[50] *Id.*

[51] *Id.*

noncompensatory business reasons include, the "employer's need to contact the employee at all times for work-related emergencies, the employer's requirement that the employee be available to speak with clients at times when the employee is away from the office, and the employee's need to speak with clients located in other time zones at times outside of the employee's normal work day."[52] These guidelines are important to note because whether reimbursements are excludable from the employee's income has a direct effect on the amount of income to be reported, and thus taxable income.

IV. Restricting, Monitoring and Scrutinizing Employee, Applicant and Litigant Use of the Cloud

Cloud services include software and services that run on the internet, and allow employees and employers alike to store and access data over the internet, rather than on hard drives or other storage devices.[53] The cloud is a collection of larger servers located elsewhere (e.g., data centers) and maintained by a vendor. The data or application becomes accessible to users anywhere there is an Internet connection. Dropbox, Netflix, Amazon Cloud Drive, Flickr, Google Drive, Apple iCloud, Microsoft Office 365 and Yahoo Mail are all cloud services.[54]

Whether an employer utilizes public or private cloud-based storage, and whether the delivery model is Software as a Service ("SaaS"), Platform as a Service ("PaaS"), or Infrastructure as a Service ("IaaS"), cloud computing provides employers tremendous cost savings, logistical advantages, and increased efficiencies and collaborative opportunities.

According to recent reports, more than 81 percent of U.S. businesses with 100 or more employees now use cloud computing.[55] The pace of utilization and investment are projected to rise dramatically in the coming years.

A. Security Breaches and Misappropriation of Trade Secrets

Though there are many well-documented benefits associated with cloud computing, the growing use of cloud services has made it possible for rogue employees to take valuable trade secrets and other proprietary company electronic files, in the matter of minutes, if not seconds.[56] Employers should implement preventative measures in order to ensure protection from the threats posed by cloud computing and to manage and mitigate the consequences data theft of confidential information. "Analog" protections, such as employee training, and basic security safeguards can help

---

[52] *Id.*
[53] David Goldman, *What Is the Cloud?*, CNN MONEY (Sept. 3, 2014, 9:05 PM), http://money.cnn.com/2014/09/03/technology/enterprise/what-is-the-cloud/index.html.
[54] *Id.*
[55] Louis Columbus, *Roundup of Small & Medium Business Cloud Computing Forecasts and Market Estimates, 2015*, FORBES (May 4, 2015), http://www.forbes.com/sites/louiscolumbus/2015/05/04/roundup-of-small-medium-business-cloud-computing-forecasts-and-market-estimates-2015/#16c3e6751646.
[56] Robert B. Milligan & Daniel Joshua Salinas, *Top 10 Developments/Headlines in Trade Secrets, Computer Fraud, and Non-Compete Law in 2013*, SEYFARTH SHAW (Mar. 6, 2014), http://www.seyfarth.com/publications/MA030614-TS.

in this respect. Furthermore, "cloud" protections should be added. It is important to keep in mind that the compromise of proprietary information that includes personal information may trigger federal and/or state breach notification obligations.[57]

Employers should be careful to protect data when they enable cloud computing. They should consider:

- Researching cloud computing provider security features;
- Negotiating maximum protection terms of service;
- Requiring a confidentiality agreement;
- Limit access to trade secrets and PII on a need to know basis;
- Monitor emails and access and downloading of files; and,
- Prohibit unauthorized cloud storage (e.g. Dropbox or Box).

Employers that suffer a loss through cloud services are not always left without a remedy. The Computer Fraud and Abuse Act exposes employees who misappropriate information located on a protected computer to criminal liability.[58] However, employers cannot bring a claim against authorized users. There is a circuit split regarding which employees are considered authorized users under the CFAA. Some courts hold that if an employee did not have management's approval to transmit company files, they are unauthorized users.[59] Other courts hold that when an employee is authorized to use a company computer subject to limitations, the employee is an authorized user even if he or she uses the computer in violation of the limitations.[60]

B. Wage & Hour Issues Arising From The Cloud

Similar to BYOD policies, the availability of cloud storage makes it easier for employees to work afterhours. Because cloud computing allows employees to upload documents, non-exempt employees can work on assignments while they are at home and off the clock.[61] In order to avoid making themselves vulnerable to class actions, employers must monitor off-the-clock work.[62]

---

[57] *Id.*
[58] *Id.*
[59] *See Frisco Med. Ctr., L.L.P. v. Bledsoe*, No. 4:12-CV-37, 2015 U.S. Dist. LEXIS 159915, at *30 (E.D. Tex. Nov. 30, 2015).
[60] *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1133 (9th Cir. 2009).
[61] Off-the-clock work violates state and federal minimum wage laws and may violate overtime laws. *See supra* notes 31, 34 and 38.
[62] *Id.*

C. Specific Legal Pitfalls, Including Compliance With The Health Insurance Portability and Accountability Act (HIPAA)

Companies and their HR and benefits departments that utilize cloud platforms to store and access personnel records, benefits information, and the like are likely storing protected health information ("PHI"). The obligations and restrictions regarding PHI are governed by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").[63]

In March 2013, the Department of Health and Human Services ("HHS") finalized the HIPAA Omnibus Rule, which expanded HIPAA's applicability beyond covered entities (health care providers, health plans, and health clearinghouses) to business associates. By definition, a "business associate" is a person or entity that creates, receives, maintains, or transmits PHI in fulfilling certain functions or activities for a HIPAA covered entity, and business associates are required to adhere to the HIPAA Privacy and Security Rules.[64] For the purposes of HIPAA, cloud service providers are often considered business associates.[65] This means that when companies use cloud platforms to store protected health information (PHI), the cloud vendors must adhere to business associate agreements.[66]

If there is a breach of PHI, employers and their business associates must comply with HIPAA's breach notification rule[67] which requires notification of the breach to affected individuals, the Secretary of HHS, and, in certain circumstances, to the media. In addition, business associates must notify covered entities if a breach occurs at or by the business associate.

When moving to the cloud, employers should remain aware that while business associates are directly liable under HIPAA, covered entities may also be directly held responsible for any actions of their business associates if their business associates are acting as agents of the employers. Noncompliance with HIPAA can result in costly fines and penalties. The fines and penalties for a HIPAA violation range from $100 per violation with a maximum fine of $25,000 for repeat violations, to $50,000 per violation with a maximum fine of $1.5 million. Ultimately, subject to any indemnification within the

---

[63] 42 U.S.C. § 1320d et seq.
[64] 45 C.F.R. § 164.504.
[65] *Id.*
[66] *Id.*
[67] 45 CFR §§ 164.400-414. A breach is generally an impermissible use or disclosure under the HIPAA Privacy Rule that compromises the security or privacy of the PHI. The breach notification rule provides three exceptions to the definition of "breach." The first exception applies to the unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of a covered entity or business associate if such acquisition, access, or use was made in good faith and within the scope of authority. The second exception applies to the inadvertent disclosure of PHI by a person authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the covered entity or business associate, or organized health care arrangement in which the covered entity participates. The final exception applies if the covered entity or business associate has a good faith belief that the unauthorized person to whom the impermissible disclosure was made would not have been able to retain the information.

BAA, covered entities are held responsible when it comes to monetary and reputational consequences; however, both a covered entity and business associate assume responsibility under recent revisions to the HIPAA rules.

Employers using cloud-based platforms should do their due diligence as covered entities throughout the vendor selection process. Employers must make continuous efforts to ensure that the integrity, confidentiality, and availability of PHI are consistent with federal standards.

D. Litigation Challenges Presented By The Cloud

The beauty and power of cloud computing is that a company's information is available wherever you are and whenever you need to access it. However, the data may not necessarily be located in a single place. Typically, a vendor will host the data in a physical location (in large data centers, in remote and secure locations) that may have no correlation with where the company otherwise conducts business. These servers housing your data can move for various reasons, such as if the servers outgrow their physical space or if the vendor relocates for business purposes.

While these logistical happenings may have little impact your company's day-to-day use of the server, such changes have the potential to pose challenges should litigation arise. Therefore, for all employers, jurisdiction is an important factor to consider when managing data in the cloud. The geographical location of an employer's data can potentially expose employers, for litigation purposes, to jurisdiction in a state or country where they do not want or expect to be "doing business."

Employers should consider drafting vendor contracts to protect the company's interests. A vendor contract can be written to include both choice of law and choice of forum clauses, to dictate where and under what law any disputes will be resolved — and not based on the vendor's location. Also, as part of any vendor contract, it is important to ensure that the vendor cannot move your data/server before giving sufficient notice. If the vendor plans to move to a state in which you don't want to potentially be subject to suit, the vendor needs to give the employer sufficient time to find a new host in a more favorable location. You may wish to consider a contract that specifically limits the states or countries where data may be stored, to avoid surprise transfers.

In some cases, multiple vendors may be used at a single time. Different offices may host data through local vendors. A single office may use more than one data hosting vendor to handle different data, based on department, client, or project. When data is hosted by various vendors, it's essential to establish each contract to protect the company's jurisdictional presence and to stay on top of any changes with the vendor.

Companies should take stock of where they currently do business, and add jurisdictional exposure to the list of considerations in moving data to the cloud.

V. Employee Internet Activity

A. Risks Associated with Internet Activity

An employer's failure to monitor employee internet activity could lead to serious legal consequences. For example, an employee's internet activity could lead to a claim for sexual harassment, specifically a hostile work environment claim if they are visiting pornographic websites or are sending inappropriate emails.[68] In addition, employers may find themselves exposed to liability for intentional and negligent infliction of emotional distress,[69] defamation, libel, and slander,[70] or copyright infringement. As discussed previously, internet and device misuse can also result in security breaches.

B. Job Applicants

An individual's internet activity can also greatly affect employment opportunities prior to employment. Employers sometimes conduct some type of social media screening of job applicants even though this practice poses potential legal ramifications. In a 2015 survey of over 1,400 organizations, only 5% of the organizations said they used social media information to make hiring decisions.[71] The other 95% of the surveyed organizations avoided the use of social media background searches for various reasons.[72]

The potential liability for employers in conducting social media background checks is far-reaching. Social media surfing can open the door to potential claims under Title VII of the Civil Rights Act of 1964, the Americans with Disabilities Act (ADA), the Age Discrimination in Employment Act (ADEA), and various state laws. It is easy to see how applicants or employees could post pictures or information describing their race, color, religion, sex, national origin, disability, age, sexual preference, or genetics on their social media accounts. For example, a woman may post pictures of her seven children on her Facebook page. Someone else could post pictures celebrating a 50th birthday. Another applicant may have photos of excessive drinking. Employers that make employment decisions based on such pictures risk running afoul of not only state and federal discrimination statutes, i.e. sex, age, perceived disability discrimination, but

---

[68] *See Gallagher v. C.H. Robinson Worldwide, Inc*., 567 F.3d 263 (6th Cir. 2009) (reversing trial court's grant of summary judgment to employer because employees' viewing of sexual explicit material on their computers, in combination with other acts, could reasonably create a hostile environment, and a reasonable jury could find that the employer knew or should have known about the harassment and failed to respond appropriately).

[69] *See Delfino v. Agilent Techs., Inc*., 145 Cal. App. 4th 790 (2006) (affirming trial court's grant of summary judgment in favor of employer because a reasonable jury could not find that the employer owed a duty to recipients of an employee's email threats sent using employer's computer).

[70] *See Gavrilovic v. Worldwide Language Res*., Inc., 441 F. Supp. 2d 163 (D. Me. 2006) (awarding damages to employee for defamation because employee's supervisor referred to her as a "Fuck toy" in an email, but reducing damages because employer took immediate steps to discipline the supervisor).

[71] Greg Wright, *Despite Legal Risks, Companies Still Use Social Media to Screen Employees,* SOC'Y FOR HUM. RESOURCE MGMT. (May 19, 2015), https://www.shrm.org/hrdisciplines/technology/articles/pages/social-media-to-screen-employees.aspx.

[72] *Id.*

also various state laws that prohibit adverse employment actions based on otherwise legal conduct.

Even if employers do not make hiring decisions based on online content, they may still face discrimination lawsuits. The applicant could easily point to the employer's practice of viewing the applicant's social media pages to prove constructive knowledge of the applicant's protected status and the employer's discriminatory intent. At the very least, this presumption could create liability if a lawsuit is filed. Plaintiffs can also use evidence of discriminatory intent to extract large settlements or awards if their case is taken to trial.[73]

In addition to the above legal concerns, employers must consider the Fair Credit Reporting Act (FCRA) when conducting pre-employment screenings. In *Sweet et al. v. LinkedIn Corporation*, employees challenged an employer's decision not to hire them based on a reference check that was conducted via LinkedIn's reference search function that generates a list of individuals who have worked with the job applicant in the past.[74] The employees argued that this function violates the FCRA because it is acting as a consumer reporting agency.[75] The Northern District of California held that LinkedIn was not a consumer reporting agency under the FCRA because it was merely assembling information that its users had voluntarily provided.[76] However, this holding is not binding of=n any other courts consideration of the issue, and another court could reach a different conclusion.

VI. Employer Control Over Employee Social Networking Service (SNS) Posting

A. National Labor Relations Act (NLRA)

1. Language of the Act

Section 7 of the NLRA states that "[e]mployees 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."[77] Section 8(a) of the NLRA prohibits employers from interfering with, restraining or coercing employees in exercising the rights they are guaranteed under section 7.[78] Therefore, employers' social media policies cannot limit their employees' rights under the NLRA.

---

[73] Erin Dougherty Foley & Lily Strumwasser, *With a Few Clicks of the Mouse You Can Uncover What Job Applicants Leave Off Their Resumes,* EMP'T. L. LOOKOUT (Nov. 26, 2013), http://www.laborandemploymentlawcounsel.com/2013/11/with-a-few-clicks-of-the-mouse-you-can-uncover-what-job-applicants-leave-off-their-resumes/.
[74] *Sweet v. LinkedIn Corp*., No. 5:14-CV-04531-PSG, 2015 WL 1744254 (N.D. Cal. Apr. 14, 2015).
[75] *Id.*
[76] *Id.*
[77] 29 U.S.C. § 157.
[78] 29 U.S.C. § 158.

2. Determining Whether or Not a Policy Will Have a Chilling Effect

The National Labor Relations Board (NLRB) implements a two-step test in determining whether or not a social media policy violates employee rights under the NLRA. Under the first prong, the inquiry focuses on whether the provision explicitly restricts protected concerted activities.[79] If it does, it is invalid. The second prong comes into play if the provision does not explicitly restrict the activity but: "(1) employees may reasonably construe the language to prohibit protected concerted activity; (2) the rule was promulgated in response to union activity; or (3) the rule was applied to restrict the exercise of concerted activity."[80]

3. Implementation of Section 7

There are a multitude of NLRB decisions interpreting Section 7 in this context, all of which create an untenable landscape for employers. For example, in a recent decision, the NLRB reviewed the social media policy of U.S. Cosmetics Corporation.[81] The policy included the following provisions:

- "Under no circumstances may an employee . . . [p]ost financial, confidential, sensitive or proprietary information about the Company, clients, employees or applicants on social media. Additionally, employees may not post obscenities, slurs or personal attacks that can damage the reputation of the Company, clients, employees or applicants. . . ."[82]

- Employees are prohibited from ""using disparaging, abusive, profane or offensive language; creating, viewing or displaying materials that might adversely or negatively reflect upon USCC or be contrary to USCC's best interests. . . ."[83]

- "Employees may not post obscenities, slurs or personal attacks that can damage the reputation of the company, clients, employees or applicants."[84]

- "Under no circumstances may an employee . . . prematurely disclose confidential and proprietary information to any unauthorized person."[85]

- "It is our policy that all information considered confidential will not be disclosed to external parties or to employees without a 'need to know.' If an employee questions whether certain information is considered

[79] Molly Considine, *Exercising Caution Before Action*, 36 HAMLINE L. REV. 517, 526 (2013).
[80] *Id.*
[81] *U.S. Cosmetics Corp.*, 2016 NLRB LEXIS 355, *46-55 (N.L.R.B. May 17, 2016).
[82] *Id.* at 46-47.
[83] *Id.* at 47.
[84] *Id.*
[85] *Id.* at 47-48.

confidential, he/she should first check with his/her immediate supervisor. "[86]

- "Employees may not post financial, confidential, sensitive or proprietary information about the company, clients, employees or applicants."[87]

The NLRB held that an employee could reasonably believe that posting statements of protest or criticism would be damaging or would adversely or negatively reflect upon the Company's reputation.[88] Furthermore, the NLRB ruled that all of the provisions could be interpreted as encompassing information about pay and other benefits.[89] Thus, the NLRB held that the policy was invalid.[90]

The holding in this decision is similar to other NLRB holdings over the past five years in that it disfavors vague language.[91] However, the NLRB does not require the language to be too specific. For instance, in June 2014, an administrative judge reviewed a social media policy asking employees not to post information about the company that would "lead to morale issues in the workplace or detrimentally affect the company's business."[92] The judge held that the policy did not violate Section 7.[93]

The NLRB also recently ruled that Chipotle's former social media policy violated the NLRA.[94] Though the policy was not in place, it was applied to an employee in early 2015.[95] The employee posted a series of negative tweets about Chipotle. One tweet insinuated that Chipotle employees were not given the day off on one particular occasion even though it was snowing and public transportation was down.[96] On another occasion the employee tweeted a customer saying that Chipotle employees only make $8.50 an hour.[97] Chipotle instructed the employee to delete the tweets and gave him a copy of the outdated social media policy.[98] The employee was later terminated for unrelated reasons.[99] The NLRB ruled that the employee's tweets constituted concerted activity because they discussed issues common to Chipotle

[86] *Id.* at 48.
[87] *Id.* at 48.
[88] *Id.* at 52-53.
[89] *Id.* at 53.
[90] *Id.* at 117-18.
[91] *See* Susan C. Hudson & Karla K. Roberts, *Drafting and Implementing an Effective Social Media Policy*, 18 TEX. WESLEYAN L. REV. 767, 780-82 (2012).
[92] Jonathan L. Brophy, *#Trending Now –NLRB and Social Policy Guidance*, EMP'T L. LOOKOUT (Sept. 23, 2014), http://www.laborandemploymentlawcounsel.com/2014/09/trending-now-nlrb-and-social-media-policy-guidance/.
[93] *Id.*
[94] Farrah N.W. Rifelj & Holly E. Courtney, *More Trouble for Chipotle: NLRB Rules Social Media Policy and Practice Unlawful*, NAT'L L. REV. (Mar. 31, 2016), http://www.natlawreview.com/article/more-trouble-chipotle-nlrb-rules-social-media-policy-and-practice-unlawful.
[95] *Id.*
[96] *Id.*
[97] *Id.*
[98] *Id.*
[99] *Id.*

employees.[100] Therefore, they held that Chipotle violated the NLRA by asking the employee to delete the tweets and to refrain from engaging in that kind of activity in the future.[101]

4. Effectiveness of Savings Clauses

The NLRB recently invalidated Macy's social media policy. The policy had a savings clause stating than nothing in the policy "is intended or will be applied, to prohibit employees from exercising their rights protected under federal labor law, including concerted discussion of wages, hours or other terms and conditions of employment."[102] The NLRB held that this savings clause was invalid because it was too generic.[103]

5. Constructing a Compliant Policy

The NLRB has decided to focus on social media issues in both union and non-union workplaces alike.[104] Common policies that are overbroad or vague are easy potential targets, regardless of the employer's intent in implementing them.[105] Social media policies (and other policies, generally) should provide fairly specific examples of prohibited conduct under their policies. Savings clauses likely will no longer survive NLRB scrutiny. Ultimately, policies should be crafted to avoid being overly broad, but specific enough to accomplish the protections desired.[106] And, employees should be entitled to post on SNS sites on their employers' premises as long as they do so on non-work time, in non-work areas and posting constitutes engaging in concerted activities.[107]

Employers do have a right to take an adverse employment action against employees based on social media posting in certain instances. For example, companies do not have to tolerate posts complaining about and threatening their customers, harassing co-workers or disclosing confidential information about the company or its clients.[108]

---

[100] *Id.*
[101] *Id.*
[102] J. Ian Downes & Kate Ericsson, *Hold On to Your Employer Handbooks: Part 1*, LAW 360 (Nov. 6, 2015, 11:47 AM), http://www.law360.com/articles/723201/hold-on-to-your-employer-handbooks-part-1.
[103] *Id.*
[104] Lynn Kappelman & John Duke, *Retail Detail: Your Retail Employees Who Blog, Tweet and Post About the Business May Be Protected*, SEYFARTH SHAW (July 7, 2011), http://www.seyfarth.com/publications/Retail-Detail-Your-Retail-Employees.
[105] *Id.*
[106] Douglas B. Mishkin, Po Yi & Jennifer G. Prozinski, *For Advertising Employers, NLRA Giveth and FTC Taketh Away*, LAW 360 (Oct. 28, 2015), http://www.law360.com/articles/718947/for-advertising-employers-nlra-giveth-and-ftc-taketh-away.
[107] Raphael Rajendra, *Employee-Owned Devices, Social Media, and the NLRA*, 30 ABA J. LAB. & EMP. L. 47, 52 (2014).
[108] Arthur V. Lambert, *5 Ways Social Media Can Land Employers In Court*, LAW 360 (Feb. 22, 2016); http://www.law360.com/articles/761008/5-ways-social-media-can-land-employers-in-court.

B. Data Theft Issues

Social Media provides a means to obfuscate data theft, essentially allowing a perpetrator to leave with information outside of the company's firewall. Social networking applications such as LinkedIn, Facebook, and Twitter all have means of private communication. Access to these accounts is easy with any type of mobile device capable of running a social application.

C. Prohibitions on Forced Disclosure of Personal Logins & Passwords

1. Federal Law

There is no federal law explicitly prohibiting employers from requesting personal login information from applicants and employees. However as was mentioned above, the SCA prohibits employers from intentionally accessing "without authorization a facility through which an electronic communication service is provided."[109] Courts have held employers accessing private websites in violation of SCA.[110] However, SCA is only applicable where the employer gains access without authorization.[111] Thus, in instances where an employee gives his or her employer personal login information upon request, the employer can argue that SCA does not apply because they were authorized to log onto the account.

2. State Law

On the state level, legislation barring employers from asking employees and applicants for login information is becoming more prevalent. As of April 4th, 2016 twenty-four states–Arkansas, California, Colorado, Connecticut, Delaware, Illinois, Louisiana, Maine, Maryland, Michigan, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New Mexico, Oklahoma, Oregon, Rhode Island, Tennessee, Utah, Virginia, Washington, and Wisconsin–have enacted some type of password protection law.[112] Currently, seven states —Alaska, Florida, Georgia, Massachusetts, Minnesota, Missouri, and West Virginia —are considering some type of relevant legislation, and

[109] 18 U.S.C. § 2701.
[110] *See, e.g.*, *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868 (9th Cir. 2002).
[111] 18 U.S.C. § 2701.
[112] *See* H.R. 1901, 89th Gen. Assemb., Reg. Sess. (Ark. 2013); Cal. Leg. 25, 2013--24 Leg., Reg. Sess. (Cal. 2012); H.R. 13-1046, 2013 Gen. Assemb., Reg. Sess. (Colo. 2013); S.B. 426, Reg. Sess. (Conn. 2015); H.R. 109, 148th Gen. Assemb., Reg. Sess. (Del. 2015); H.R. 1047, 98th Gen. Assemb., Reg. Sess. (Ill. 2013); H.R. 314, 2014 Leg., Reg. Sess. (La. 2014); H.B. 640, 2015 Leg., 127th Sess. (Me. 2015); H.R. 1332, 2013 Gen. Assemb., Reg. Sess. (Md. 2013); H.R. 5523, 96th Leg., Reg. Sess. (Mich. 2012); H.B. 343, 63d Leg., Reg. Sess. (Mont. 2015); H. R. 142, Reg. Sess. (N.H. 2015); H.R. 2878, 215th Leg., Reg. Sess. (N.J. 2013); N.M. Leg. 371, 51st Leg., 1st Sess. (N.M. 2013); Nev. Leg. 181, 2013 Leg., Reg. Sess. (Nev. 2013); H.R. 2372, 2014 Leg., Reg. Sess. (Okla. 2014); H.R. 2654, 77th Legis. Assemb., Reg. Sess. (Or. 2013); H.R. 5255, 2013 Gen. Assemb., Jan. Sess. (R.I. 2013); H.R. 1852, 2014 Gen. Assemb., Reg. Sess. (Tenn. 2014); H.R. 100, 2013 Leg., 2013 Gen. Sess. (Utah 2013); H.R. 2081, Reg. Sess. (Va. 2015); Wash. Leg. 5211, 63d Leg., Reg. Sess. (Wash. 2013); H.R. 218, 2013 Gen. Assemb., Reg. Sess. (Wis. 2013).

numerous other states considered passing such legislation as well.[113] Conversely, some states, such as Vermont, declined to pass such laws due to potential conflicts with federal online privacy laws and superseding law enforcement needs.

The language of these laws are fairly straightforward. For instance, California law states that "[a]n employer shall not require or request an employee or applicant for employment to … [d]isclose a username or password for the purpose of accessing personal social media."[114] Critics of California's legislation believe that it will limit employers in their ability to regulate the workplace and investigate misconduct.[115] Proponents of the legislation feel that the law will shield businesses from liability in cases where employees allege that these businesses have a duty to monitor employee social media accounts.[116]

3. Creating a Compliant Policy

A company's policy regarding personal login information requests will differ depending on the state in which the company operates. If the state is among the twenty-four states that has passed legislation prohibiting employers from requesting such information, the company should implement a policy that makes it clear that managers, supervisors and HR personnel are prohibited from requesting applicants and employees to disclose their personal login information.

Companies operating in states without password privacy legislation must ensure that they act in compliance with the SCA. Therefore, it is important that companies clarify in their policies that authorization is necessary in accessing employees' and applicants' personal accounts. This is true even where the employer gains access to an employee's or applicant's account through the account of another person who can see the account.[117] Ultimately, if a company is able to procure authorization from the employee or applicant whose account it wishes to view, it can do so.

Additionally, companies that wish to prepare effective social media policies should incorporate existing policies — e.g., electronic equipment and systems use, confidentiality, code of conduct, harassment — and make clear that failure to abide by these guidelines in the social media sphere may subject employees to discipline as well as legal action by the company (or others). Such policies should also distinguish "personal" versus "non-personal" social media accounts (i.e. those used by the business versus those that are meant as entirely personal accounts). The policy should also state that the employee does not have a reasonable expectation of privacy in social

---

[113] *Access to Social Media Usernames and Passwords*, NAT'L CONF. OF STATE LEGISLATURES (Apr. 6, 2016), http://www.ncsl.org/research/telecommunications-and-information-technology/employer-access-to-social-media-passwords-2013.aspx.
[114] Cal. Leg. 25, 2013--24 Leg., Reg. Sess. (Cal. 2012).
[115] Robert B. Milligan & Daniel Joshua Salinas, *New Law Protecting Personal Social Media Of California Employees and Students Adopted In California*, SEYFARTH SHAW (Oct. 1, 2012), http://www.seyfarth.com/publications/MA100112.
[116] *Id.*
[117] *See, e.g.*, *Konop*, 302 F.3d at 873.

media activities using company equipment or systems, nor while using business-related social media accounts.

D. Litigation Discoverability of SNS Posts, Photos, and Messages

1. eDiscovery of Social Media

Courts have seen a dramatic increase in the number of social media postings on social networking websites, such as Facebook and Twitter, and various blogging platforms, that parties have requested to be produced in discovery. Although emails and other electronic documents have flooded the courts for decades, the uniqueness of social media platforms presents various questions of privacy, accessibility, preservation, and admissibility. But, courts have predominantly interpreted these questions in the same way as with emails, text messages, and other electronically stored information (ESI). Courts continue to require relevancy and forbid fishing expeditions.[118]

In 2009, California passed the Electronic Discovery Act, in order to bring the rules up to date and in line with the eDiscovery updates to the Federal Rules of Civil Procedure.[119] For the most part, the rules reflect the principles in the Federal Rules. Many other states have adopted similar updates to their rules regulating eDiscovery.

There is no judicially accepted social media privilege or blanket of privacy when it comes to social media sites.[120] Information posted on the Internet and made available to the public is generally considered to be public information because the poster has no reasonable expectation of privacy in the published material.[121] But, when certain information is restricted from the general public's eyes, then more formal discovery methods will need to be utilized.[122] *Crispin v. Audigier* found that whether the social media information should be disclosed to the opposing party depended on the plaintiff's privacy settings.[123] The public information was available to the company, but the company needed a subpoena pursuant to the Stored Communications Act to access the information that was limited to certain viewers.[124]

---

[118] Rick E. Kubler & Holly A. Miller, *Recent Developments in Discovery of Social Media Content*, ABA SEC. OF LITIGATION (Mar. 4-7, 2015), http://www.americanbar.org/content/dam/aba/administrative/litigation/materials/2015_inscle_materials/written_materials/24_1_recent_developements_in_discovery_of_social_media_content.authcheckdam.pdf.

[119] California Electronic Discovery Act, CCP 2016.020.

[120] *See Davenport v. State Farm Mut. Auto. Ins. Co*., 2012 WL 555759 at *1 (M.D.Fla. Feb. 21, 2012).

[121] *Moreno v. Hanford Sentinel, Inc*., 172 Cal. App. 4th 1125, 1130 (2009); *but see Nucci v. Target Corp*., __ So.3d ___, 2014 WL 71726 (Fla. Dist. Ct. App. Jan. 7, 2015) (holding that photos posted on a social networking site are not privileged or protected by any privacy rights, even if the user utilized a privacy setting).

[122] "[E]ven though certain SNS content may be available for public view, the Federal Rules do not grant a requesting party "a generalized right to rummage at will through information that [the responding party] has limited from public view"; *Tompkins v. Detroit Metropolitan Airport*, 278 F.R.D. 387, 388 (E.D. Mich. 2012); *EEOC v. Simply Storage Mgmt., LLC*, 270 F.R.D. 430, 434 (S.D. Ind. 2010) ("merely locking a profile from public access does not prevent discovery").

[123] *Crispin v. Christian Audigier, Inc*., 717 F. Supp. 2d 965 (C.D. Cal. 2010).

[124] *Id.*

In general, it is important for lawyers to keep traditional discovery rules in mind when requesting social media information. Also, traditional evidence rules are crucial to such requests. A litigant will have to be able to demonstrate that the requested social media information is relevant to any claim or defense, and will then have to select the most effective method to obtain the information.

2. Standards and Methods of Access

State bar associations have recognized the need for attorneys to conform to certain ethical standards when accessing the social media accounts of their clients and non-clients.[125] The sensitive and unique nature of social media carries with it a realm of concerns. These ethical considerations include the ABA Model Rules of Professional Conduct addressing the confidentiality of information, truthfulness in statements to others, responsibility regarding non-lawyer assistants, and misconduct.[126]

Aside from publicly available social media information, an attorney has a few different avenues to obtain a party's social media postings while abiding by these ethical standards of conduct. In addition to the commonly utilized discovery request, some other methods include, direct access via consent, third party subpoenas, in camera review, and attorney's eyes only.[127]

As previously mentioned, the discovery of social media evidence must adhere to the applicable discovery rules. Requests for social media content must be "reasonably calculated to lead to the discovery of admissible evidence"[128] and should "put a reasonable person of ordinary intelligence on notice of which specific documents or information would be responsive to the request."[129] The time frame and subject matter of social media requests should be carefully noted to increase the likelihood of receiving the requested information.

E. Social Media's Role in Emotional Distress Claims

Social media evidence is particularly probative in employment litigation because individuals are becoming more willing to share personal details of their lives on social media. Damaging social media evidence can harm a plaintiff's case and can be used as a vehicle to lower or eliminate damages. Notably, there is a disagreement in case law as to whether social media evidence is relevant to emotional distress claims.

In *EEOC v. Simply Storage Mgmt., LLC*, the Court held that it is too restrictive to limit the production of communications from a plaintiff's social media account to only those matters directly alleged in the complaint and called for a broader definition of

---

[125] Seth Muse, *Ethics of Using Social Media During Case Investigation and Discovery,* ABA SEC. OF LITIGATION (June 13, 2012), http://apps.americanbar.org/litigation/committees/pretrial/email/spring2012/spring2012-0612-ethics-using-social-media-during-case-investigation-discovery.html.
[126] *Id.*
[127] Margaret DiBianca, *Discovery and Preservation of Social Media Evidence,* ABA BUS. LAW TODAY (Jan. 2014), http://www.americanbar.org/publications/blt/2014/01/02_dibianca.html.
[128] *Tompkins v. Detroit Metropolitan Airport*, 278 F.R.D. 387, 388 (E.D. Mich.2012).
[129] *Mailhoit v. Home Depot U.S.A., Inc*., 285 F.R.D. 566, 571 (C.D. Cal. 2012).

relevant social media content.[130] The Court reasoned that this would create an unfairness because it would only produce evidence that was supportive of the user's claims and would not divulge information inconsistent with the user's claims.[131] But, in *Mailhoit v. Home Depot USA, Inc*., the Court was more critical of a broad request for social media communications relating to "any emotion, feeling, or mental state of Plaintiff, as well as communications by or from Plaintiff that reveal, refer, or relate to events that could reasonably be expected to produce a significant emotion, feeling, or mental state." [132] The Court held that the request failed to sufficiently put the responding party on notice of what constitutes responsive material, and thus the requesting party could not obtain the requested information.[133]

F. Tips for Employers

Social media presents a ripe opportunity for lawyers to obtain information that could greatly impact the outcome of a case. In light of the current state of eDiscovery law as applied to social media evidence, there are some key takeaways for employers that can enhance the usefulness of social media.

First, employers should review the social media privacy laws in the states in which they operate. If the laws differ, employers should consider whether developing a state-specific policy is necessary. Second, employers should keep up with technology as it develops.[134] By keeping up with technology, employers can ensure that discovery requests cover the possible social media platforms that could contain relevant information.[135] The rate at which technology develops makes it more likely that evidence could be found across a wider range of platforms than previously thought.[136]

Third, before drafting discovery requests, employers should first gather what information is publicly available.[137] This includes taking screen-shots of the relevant information in case it is later deleted or the user's privacy settings are changed.[138] Sending preservation letters to opposing counsel can also ensure that social media evidence is preserved and to avoid any issues of spoliation.[139] Having some idea as to what information is out there can help convince a court that further discovery should be compelled.[140] This can be furthered by asking deposition questions as to the plaintiff's social media use. The more enlightened the requesting party is, the more likely it is that their request will be found relevant to the claims or defenses in the case.

---

[130] *EEOC v. Simply Storage Mgmt., LLC*, 270 F.R.D. 430, 435-36 (S.D. Ind. 2010).
[131] *Id.*
[132] *Mailhoit v. Home Depot U.S.A., Inc*., 285 F.R.D. 566, 571-72 (C.D. Cal. 2012).
[133] *Id.*
[134] Abigail Rubenstein, *7 Tips for Employers on Social Media Discovery,* LAW360 (July 25, 2013, 8:39 PM), http://www.law360.com/articles/460045/7-tips-for-employers-on-social-media-discovery.
[135] *Id.*
[136] *Id.*
[137] *Id.*
[138] *Id.*
[139] *Id.*
[140] *Id.*

Fourth, employers should take care to access the information in a legal way, so as to avoid any invasion of privacy claims.[141] It is important to remember that the opposing party can request an employer's social media information as well.[142] Employers should have clear guidelines on social media appropriateness, and also include social media accounts in litigation holds so as to avoid spoliation.[143]

[141] *Id.*
[142] *Id.*
[143] *Id.*