"UNFRIENDING": EMPLOYMENT DECISIONS IN THE AGE OF SOCIAL MEDIA AND CELLPHONES

BY
DOUG KERTSCHER AND TRAVIS CASHBAUGH
HILL, KERTSCHER & WHARTON, LLP
WWW.HKW-LAW.COM
ATLANTA, GA

Located at the intersection of employment law and social media, there exist issues of protected activities, free speech, privacy, and rights of employees and employers. Through a sample of recent national case law, this article examines the risks associated with making employment decisions in the age of social media.

As federal and state laws evolve in these areas to provide guidance for a society with an ever-increasing desire to blend personal and professional lives online through social platforms, both employers and employees will need to carefully assess what is permissible and private (and what is not) with these relatively new, yet already ubiquitous, technologies.

I. EMPLOYMENT DECISIONS INVOLVING SOCIAL MEDIA ACTIVITY

Social media can provide a vast range of information about an employee that is useful to the employer. Notwithstanding the upside to monitoring an employee's social media content, employers can walk a tight line between lawful and unlawful policies when employment decisions are based upon social media activity. Potential consequences for the employer include running afoul of Section 8(a)(1) of the National Labor Relations Act ("NLRA"), the Stored Communications Act ("SCA"), violations of First Amendment protections, Title VII of the Civil Rights Act of 1964, and common law privacy rights.

A. NLRA Actions

Section 8(a)(1) of the NLRA makes it an unfair labor practice for an employer to interfere with, restrain, or coerce employees in the exercise of their rights to self-organize, form, join, or assist labor organizations . . . or engage in any other concerted activity for the purpose of collective bargaining or other mutual aid or protection.[1] In recent years the National Labor Relations Board has issued numerous rulings which indicate a strict stance for employers taking adverse action against employees who take to social media to discuss matters affecting their employment.[2]

In *Hispanics United of Buffalo, Inc.*[3] an employee (Cruz) texted a co-worker (Rivera)

[1] 29 U.S.C. § 158.

[2] *See* NLRB Office of the General Counsel Division of Operations-Management, *Report of the Acting General Counsel Concerning Social Media*, Memorandum OM 11-74, Aug. 18, 2011 (discussing 14 cases decided by the NLRB and providing general guidance in accordance with those rulings in the context of the NLRA as it relates to issues of today's social media and the workplace).

[3] *Hispanics United of Buffalo, Inc.*, 359 NLRB No. 37 (2012).

stating that she intended to discuss her concerns regarding Rivera's performance at work with their manager. This text message prompted Rivera to post on Facebook a message which stated that Cruz did not think employees of the company helped their clients enough. The message ended with Rivera asking how other co-workers felt about Cruz's comments. Four off-duty co-workers responded to this posting[4], generally objecting to the assertion that their job performance was substandard. Both the initial Facebook message and subsequent responses were posted from the employees' personal computers while off duty. The first work day after the postings, all five employees were discharged on the grounds that the Facebook postings constituted harassment and bullying in violation of employer's "zero tolerance policy."

At issue was whether the employees' Facebook comments constituted "concerted activity," and if so, whether that activity is protected by the NLRA.[5] The NLRB Administrative Law Judge (ALJ) concluded there should be no question that the activities engaged in by the five employees was concerted, and that Facebook comments fall within the protection of the Act. The AJL reasoned that activity engage in by these employees was concerted for the purpose of mutual aid or protection, in that, such communication was for the purpose of preparing a group defense to another co-worker's complaints. Additionally, as these comments concerned employee discussions of job performance, the ALJ concluded they were within the Act's protection. This decision provided a wakeup call[6] to employers hastily responding to employee social media communications that could be considered protected concerted activity.

B. Stored Communications Act

Even when employees' social media communications are not afforded protection under the NLRA, additional legal consequences exist for an employer that bases termination or disciplinary decisions on social media posts. In *Ehling v. Monmouth-Ocean Hospital Service Corp.*[7], the Plaintiff, a nurse, was terminated, in part[8], for comments made on her private Facebook page. Plaintiff's Facebook comments criticized Washington, D.C. paramedics in their response to a museum shooting. The Plaintiff's privacy setting on Facebook were adjusted so that only her Facebook friends could see her posts. While Plaintiff was Facebook friends with many of her co-workers, she was not Facebook friends with any of her managers at the hospital. Unbeknownst to Plaintiff, a co-worker had been taking screenshots of her Facebook posts, printing them out, and delivering them to the hospital managers.

Upon receipt of the printed out Facebook posts, management decided to suspend Plaintiff

---

[4] Cruz herself responded to the post, demanding the five co-workers to stop lying about her.

[5] The NLRB analyzed this case under the four elements in *Meyers I*, however, only the issues of elements (i) and (iii) were disputed of the four element test, which states that an employer violates Section 8(a)(1) if (i) the activity the employee engages in is concerted (ii) the employer knew of the concerted activity (iii) the concerted activity was protected under the Act and (iv) the discipline or discharge was motivated by the employee's protected, concerted activity.

[6] Such a decision should not have been a complete surprise as warning signs of the NLRB's intent to closely monitor disciplinary actions based upon employees' social media activity were clearly visible in a 2010 complaint filed in *American Medical Response of Connecticut, Inc*., (Case No. 34-CA-12576).

[7] *Ehling v. Monmouth-Ocean Hospital Service Corp*., 961 F. Supp. 2d (D.N.J. 2013).

[8] Initially suspended with pay for the Facebook post, Plaintiff ultimately was terminated once she failed to return to work after exhausting her FMLA time and thereafter failing to fill out reasonable accommodation forms provided by her employer.

with pay and sent her a memo that her "D.C. paramedic" comments reflected a deliberate disregard for public safety.[9] After her termination, Plaintiff brought suit, alleging, among other violations[10], the hospital violated the Federal Stored Communications Act ("SCA"), 18 U.S.C. §§ 2701-11, by improperly accessed her Facebook post about the museum shooting.

Plaintiff argued that her Facebook posts were covered by the SCA because she selected privacy settings limiting access to only to her Facebook friends. Although hospital management never solicited[11] or had direct access to Plaintiff's Facebook posts, the Court ruled that the posts were covered under the FCA. Specifically, the Court ruled that Facebook wall posts, configured to be private are protected under the SCA. However, the SCA also provides two exceptions: (1) conduct authorized by the person or entity providing an electronic communications service or (2) by a user of that service with respect to a communication of or intended for that user.[12] The Court concluded the second exception to the SCA applied. Access to Plaintiff's Facebook post was authorized by a Facebook user (the co-worker who provided management with the posts) with respect to a communication that was intended for that user since Plaintiff's co-worker was a Facebook friend, and in accordance with Plaintiff's Facebook privacy settings, her posts were intended to be viewed by friends.[13] Accordingly, the hospital was not liable under the SCA.

A different result was reached in *Pietrylo v. Hillstone Restaurant Group*[14], when the district court upheld the jury's verdict finding the employer had violated the SCA. In *Pietrylo*, two employees created a password protected MySpace page, to which they invited other co-workers[15], allowing them to post criticisms about their employer and managers. After management learned of the site, they pressured an employee into providing her MySpace password so they could access the private, invitation-only chartroom. Ultimately the employee who created the MySpace page was terminated for damaging employee morale.

The terminated employee brought suit alleging, among other claims[16], that the managers had violated the SCA. The central issue the district court looked at was whether the managers' were *authorized* to access the website, thereby allowing them to fall within the second exception to the SCA.[17] Unlike the employer in *Ehling* who gained access unsolicited, here there was evidence that the employee who provided the password felt pressured to do so. The employer argued that the employee expressed no reservations to them about giving up the password, thus indicating they were *authorized* to access the website. However, the Court concluded that a reasonable jury could find that the defendants were not authorized based on the employee's

---

[9] *See Ehling*, 961 F. Supp. at 663.

[10] Plaintiff filed a six count Amended Complaint consisting of: (1) Violation of the Stored Communications Act (2) Violation of the Family and Medical Leave Act (3) Violations of New Jersey Law Against Discrimination (5) Violation of the Conscientious Employee Protection Act and (6) Invasion of Privacy.

[11] *But see Konop v. Hawaiian Airlines, Inc*., 302 F.3d 868 (9th Cir. 2002) for a discussion of SCA violation in relation to employer who intentionally solicits and has direct access to an employee's privately operated, secured website.

[12] 18 U.S.C. § 2701(c).

[13] *See Ehling*, 961 F. Supp. at 670-71.

[14] *Pietrylo v. Hillstone Rest. Grp.*, No. 06-575, 2009 WL 3128420 (D.N.J. Sept. 25, 2009).

[15] No managers were invited to join the MySpace page.

[16] Plaintiff also brought common law invasion of privacy claim, however, the jury determined that defendants did not invade plaintiff's privacy.

[17] *See Pietrylo*, 2009 WL 3128420, at *2.

testimony that she feared adverse action from her employer if she were to refuse to give up the password.[18]

C. Title VII Actions

While the above discussion shows that social media material is a potential exercise of rights under the NLRA and that, under certain circumstances, employer access to an employee's social media content can lead to violations of the SCA, courts have had no difficulty in concluding that an employer may discipline employees for violations of employer policies. In *Rodriquez v. Wal-Mart Stores*, Inc.[19], the Plaintiff was terminated after violating Wal-Mart's social media policy. The Plaintiff saw on Facebook a picture of two co-workers at a party that they called in sick to attend. Plaintiff commented on these Facebook pictures, essentially stating how she could not believe they called in sick, then attend a party, and be bold enough to post about it on Facebook.[20] The next day a co-worker complained to employer about Plaintiff's comment. The employer determined that such a comment violated their social media policy, which prohibited any conduct that adversely affects job performance or other associates.[21]

After her termination, the Plaintiff brought a discrimination and retaliation claim against Wal-Mart under state law.[22] The Court upheld the district court's grant of summary judgment to Wal-Mart, stating that Plaintiff had failed to prove that Wal-Mart's legitimate reason for her termination, namely, the social media policy violation, was a pretext for discrimination.[23]

Going farther, several courts have upheld an employer's decision to terminate based upon the mistaken belief that an employee authored a social media comment. In *Smizer v. Community Mennonite Early Learning Center*[24], the Plaintiff was a teaching aide at the Community Mennonite Early Leaning Center ("Center"). Shortly after a judge awarded custody of Plaintiff's nephew to his sister, a former co-worker, claiming to be the Plaintiff, sent an email to the nephew that strongly criticized those in Plaintiff's family that were opposed to his sister receiving custody. One family member that opposed, was Plaintiff's mother, who also happened to be his co-worker. Based on this email, Plaintiff's mother lobbied the Center to have him terminated, referencing the email and stating that Plaintiff posted on Facebook "about his damned family & that's what we get for f***ing with his sister and other horrible stuff."[25]

Several days later Plaintiff received a letter stating that he was being fired for insubordination and unprofessional conduct. When Plaintiff was handed this letter, the Center told him "the Facebook posting was the basis for his dismissal."[26] Plaintiff sued the Center under Title VII. The district court granted summary judgment for the Center, for which Plaintiff

---

[18] *Id*. at *3.
[19] *Rodriquez v. Wal-Mart Stores*, Inc., 540 F. App'x 322 (5th Cir. 2013).
[20] For Plaintiff's entire Facebook comment *see id*. at 324.
[21] *Id*.
[22] Plaintiff's state law claims are analogous to Title VII claims, in that Texas courts apply analogous federal law to suits under the Texas Commission on Human Rights Act; *See id*.
[23] *Id*. at 328.
[24] *Smizer v. Cmty. Mennonite Early Learning Ctr*., 538 F. App'x 711 (7th Cir. 2013).
[25] *Id*. at 712.
[26] *Id*. at 713.

appealed. The principal issue on appeal was whether Plaintiff had enough evidence to show pretext, which centered on the authorship and existence of the Facebook post. According to the Seventh Circuit, regardless of whether the Plaintiff actually authored the Facebook post, if the Center honestly believed he did, that alone is a legitimate reason for termination[27]. Accordingly, the Court affirmed summary judgment.

II. TERMINATION/DISCIPLINARY PROCEEDINGS AND EMPLOYER ISSUED DEVICES

A. Cell Phones/Pagers

Generally stated, employers can monitor and record on employer owned phones and phone systems. This includes cell phones, voicemails, and text messages. In the seminal case of *City of Ontario v. Quon*[28], the Supreme Court of the United States determined that an employee did not have a reasonable expectation of privacy with regards to records from his employer issued pager. Accordingly, the employer was allowed to review those records in order to determine whether or not subsequent disciplinary action was appropriate if they deemed the employee violated the pager use policy.

In *Quon*, the plaintiff was a police officer with the City of Ontario ("City"). The city issued pagers to all officers and made them sign computer usage, internet, and email policies. Additionally, the pagers had monthly character limits. After becoming concerned that Plaintiff repeatedly exceeded his character limit, the City obtained the text message transcripts to determine whether the overage was work-related or personal.[29] Upon determination that the overages were personal, the City took disciplinary action against the Plaintiff. Subsequently, the Plaintiff brought an action under 42 U.S.C. § 1983 against the City, alleging that the City's review of his text messages violated the Fourth Amendment. Avoiding the question of whether the Plaintiff had a legitimate expectation of privacy in the text messages, the Court found that the government employer acted reasonably in reviewing the pager transcripts to investigate work-related misconduct.[30] Notably, Plaintiff was not completely without relief. Although the Supreme Court determined no Fourth Amendment violation occurred, they did not review the ruling by the Ninth Circuit Court of Appeals that held the third-party vendor whom provided the records to the City, violated the Stored Communications Act.

The existence, or lack thereof, of an employer policy stating that employees have no expectation of privacy in employer issued devices was a significant factor in the case of *Cunningham v. Terrebonne Parish Consol. Gov't*[31]. Similar to *Quon*, the Plaintiff was a police officer who brought suit under 42 U.S.C. § 1983, alleging the police department had violated the Fourth Amendment when they reviewed his phone records without permission. After suspecting the Plaintiff of violating department policy by contacting local media regarding an upcoming election within the police department, Plaintiff's supervisor obtained a subpoena and viewed his

---

[27] *Id*. at 714.
[28] *City of Ontario v. Quon*, 560 U.S. 746 (2010).
[29] *Id*. at 750-51.
[30] *Id*. at 760.
[31] *Cunningham v. Terrebonne Parish Consol. Gov't.*, No. CIV.A. 09-8046, 2011 WL 651997 (E.D. La. Feb. 11, 2011).

phone records. The department placed great emphasis on the recent *Quon* decision in their motion for summary judgment.[32] However, the facts of *Cunningham* differed from *Quon* in significant ways. First, the phone was Plaintiff's personal cell, although the department provided a monthly stipend for business use charges.[33] Most notably, the department had no computer or cell phone policy similar to *Quon*.[34] Although these facts contrasted with *Quon*, they did not prove fatal for the police department. The court, relying on *Quon's* cautious approach to the Fourth Amendment and technology, ultimately denied Plaintiff's motion for summary judgment, finding that there still existed a genuine question as to whether Plaintiff had a reasonable expectation of privacy in his cell phone records.[35]

It is unclear to this point the transformative effect *Quon* or *Cunningham* will have on technology and the law,[36] especially the private sector. However, *Quon* suggested in dicta that employer monitoring of employer issued cell phones would be permissible, provided the employer creates a reasonable expectation with employees of such a policy.[37] Additional guidance concerning workplace decisions relating to employer issued cell phones may come from case law on the issue of employer provided computers.[38]

B. Computers

Similar to employer issued cells phones, employers also have the ability to make termination or disciplinary decisions regarding an employee's use of employer provided computers. Most controversy in this area deals with employer access to personal email sent on company computers. Generally, an employer will be allowed to monitor personal email sent using a company network if there is a clear policy in place that the employee is aware of.[39] However, case law has differed concerning employee privacy and the use of personal web-based email on company computers.

In *Stengart v. Loving Care Agency*[40], the Plaintiff sent emails to her attorney from a company computer through her personal, password protected email account. The Plaintiff filed a discrimination suit against the company and the company's IT department discovered personal emails between the Plaintiff and her attorney. Plaintiff brought state privacy law claims against the company for accessing these emails. The company argued that there was a policy in place that notified the Plaintiff, along with other employees, that there should be no expectation of privacy in the use of company computers.[41] The court held in favor of the Plaintiff due to the

---

[32] *See id*. at *4-6

[33] *Id*. at 5.

[34] *Id*. at 4.

[35] *Id*. at 5.

[36] *See Quon*. at 759 (discussing the Court's hesitancy to elaborate too fully on the Fourth Amendment implications of emerging technology).

[37] *See id*. at 760.

[38] *See United States v. Wurie*, 728 F.3d 1, 8 (1st Cir. 2013) *cert. granted* (discussing how in reality a cell phone is a computer).

[39] *See Leor Exploration & Production LLC v. Aguiar*, 2009 WL 3097207 at *4 (S.D. Fla. 2009) (noting that employer policy that employees had no expectation of privacy in communications sent over employer systems supported denial of employees privacy claim).

[40] *Stengart v. Loving Care Agency, Inc*., 990 A.2d 650 (N.J. 2010).

[41] *Id*. at 664.

confusion of the employer's email policy, namely, that the policy created doubt about whether personal emails are company or private property.[42] \

The opposite result was reached in *Aventa Learning, Inc. v. K12, Inc.*[43], 830 F. Supp. 2d 1083, 1110 (W.D. Wash. 2011). Again, the issue of employee privacy on a company computer was decided in the context of attorney-client privilege, and employer access to communications sent from a personal web-based email system.[44] In ruling that Plaintiff enjoyed no expectation of privacy for personal emails on web-based systems stored on the employer's computer, the court highlighted the broadness of the employer's policy.[45] Therefore, unlike *Stengart*, whose policy was confusing as it related to personal email, Aventa's policy stated the employer had the right to "access, search, ... or disclose *any file or stored communication.*"[46] Accordingly, the court accepted the policy on its face, and refused to create any distinction, as other courts have, between the type of email system accessed on employer issued devices.

* * *

[42] *Id*.
[43] *Aventa Learning, Inc. v. K12, Inc.*, 830 F. Supp. 2d 1083, 1110 (W.D. Wash. 2011).
[44] *Id*. at 1107.
[45] *Id*. at 1110.
[46] *Id*.