Journal of Collective Bargaining in the Academy

Volume 0 *National Center Proceedings 2015* Article 30

April 2015

Electronic Privacy in Higher Education (CLE)

Jason Walta
NEA

Recommended Citation

Walta, Jason (2015) "Electronic Privacy in Higher Education (CLE)," *Journal of Collective Bargaining in the Academy*: Vol. 0, Article 30.
DOI: https://doi.org/10.58188/1941-8043.1491
Available at: https://thekeep.eiu.edu/jcba/vol0/iss10/30

TOPICS IN EMPLOYEE ELECTRONIC PRIVACY: THE CONSTITUTION, COLLECTIVE BARGAINING, AND SUNSHINE LAWS

For the Panel on "Electronic Privacy in Higher Education"
Monday, April 20, 2015

42nd Annual Conference
National Center for the Study of Collective Bargaining in Higher Education and the Professions
Hunter College, City University of New York

Jason Walta
Senior Counsel
National Education Association
jwalta@nea.org

I. Introduction

Neither federal nor state laws provide comprehensive protections for the electronic privacy of faculty —or employees generally — in the private or public sector. Instead, there is patchwork of federal and state laws, as well as workplace contracts and policies, that provide a complex and ultimately incomplete set of protections and remedies.

This paper will focus on a selection of issues dealing with employee privacy. In Part II, it will briefly survey the justifications for electronic monitoring of employees and the kinds of monitoring that employers use routinely.

In Part III, this paper will examine some of the protections provided by the federal and state constitutions. This will include constitutional protections, not only against an employer's invasion of an employee's privacy, but also the constitutional protections against discharge or discipline an employee may invoke once the employer has discovered the content of online or other electronic communications.

In Part IV, this paper examines some of the protections that both federal and state labor law offer for electronic privacy and online speech. Some of these protections apply to employees regardless of whether they are in a unionized workplace, while others are specific to the collective bargaining process.

Finally, in Part VI, this paper briefly surveys some of the decisions applying state Sunshine or Public Record laws to employees' electronic records and communications.

II. Employee Electronic Monitoring

A. Justifications for employee monitoring

1. Legitimate justifications

- Ensuring productivity.
- Uncovering or investigating workplace harassment, discrimination, violence, and unlawful or tortious conduct.
- Uncovering or investigating misuse of employer's resources, such as using computers to view pornography.
- Preventing the transmission of trade secrets or other confidential information.

2. Dodgy justifications

- Personal prying

https://thekeep.eiu.edu/jcba/vol0/iss10/30
DOI: 10.58188/1941-8043.1491

- Engaging in workplace harassment or discrimination
- Surveilling or punishing union activity

B. Varieties of electronic monitoring

- *Access Panels:* Electronic devices programmed to control entry into a doorway, stairwell, elevator, parking garage, or other restricted area. Typical panels require employees to enter a code or swipe an identification card. Authorized credentials are logged into a system. Such systems can be used to monitor employee attendance behavior, even how often employees use restroom or break-room doors.

- *Computer-Monitoring Programs:* These include programs can record commands and keystrokes sent to the computer by a user, translate these signals into data, and transmit this information to the employer. Some programs can record and copy, in real time, the activities that occur on an employee's computer, including tracking which software applications are open and for how long, logging the order in which applications are utilized, tracking passwords and usernames, taking screenshots, and tracking all windows open. Other monitoring techniques include internet-use audits that can track an employee's Web activity (including mouse-clicks).

- *E-Mail and Text Message Monitoring.* Programs that can track the content, timing, volume, and recipients of sent and received e-mail.

- *Filters and Firewalls:* Programs that restrict employees' internet access. These programs typically block access to sites associate with "adult" content, gaming, social networking, entertainment, shopping, and sports.

- *GPS and Radio Frequency Identification (RFID):* Provides precise location information for objects or individuals, on a real-time basis, by triangulating satellite signals. These devices can monitor employee cell phones, laptops, PDAs and Smartcards, or other forms of employer property.

- *Social Network and Search Engine Monitoring:* Searching sites such as Facebook or Twitter for information posted to an employee's profile. Or using internet search engines like Google.com to search for the employee's name. Employers may also rely on outside "big data" firms that can compile data from various online sources to create profiles for employer decisions such as hiring and promotion.

- *Telephone and Voicemail Monitoring:* Tracking the amount of time spent on calls, phone numbers dialed, breaks between receiving calls, and so forth. Voicemail

monitoring allows employers to review employee voicemail using programs that turns voicemail into audio files and e-mail text.

- *Video Surveillance:* Taping of employees within workplace facilities or outside of the workplace conducting work activities. Some employers place hidden cameras throughout the workplace, while others are purposefully overt.

III. Constitutional Protections for Employee Privacy and Online Activity

A. Federal constitution

The U.S. Constitution generally does *not* constrain a *private-sector* employer in its ability to conduct electronic surveillance or monitoring on its employees. Rather, to the extent the U.S. Constitution imposes any limits on employer surveillance, those limits apply only in *public-sector* employment, such as public universities.

1. Fourth Amendment

Public sector employees are protected against certain "unreasonable" searches by their employers:

> [P]ublic employer intrusions on the constitutionally protected privacy interests of government employees for noninvestigatory, work-related purposes, as well as for investigations of work-related misconduct, should be judged by the standard of reasonableness under all the circumstances. Under this reasonableness standard, both the inception and the scope of the intrusion must be reasonable ....

O'Connor v. Ortega, 480 U.S. 709, 725-26 (1987).

In *City of Ontario v. Quon*, 560 U.S. 746 (2010), the Court upheld a police department's review of transcripts of a police officer's text messages (including a number of sexually explicit messages) sent and received on his city-issued pager. The Court noted that the officer had a diminished expectation of privacy in the content of his messages sent from a city-issued because the employer had announced that the messages were subject to auditing. Furthermore, the Court found that the search was justified by a work-related need (to assess why the officer had repeatedly exceeded the monthly data limit on texting) and was reasonable in all other respects.

Thus, when it comes to electronic monitoring, the factors that determine "reasonableness" tend to favor the public employer so long the employee receives advance notice or possible monitoring and the search is performed for a legitimate purpose. *See, e.g., Biby v. Bd. of Regents of the Univ. of Nebraska*, 419 F.3d 845 (8th Cir. 2005) (rejecting university professor's Fourth Amendment claim on the ground that the professor did not have a

https://thekeep.eiu.edu/jcba/vol0/iss10/30
DOI: 10.58188/1941-8043.1491

legitimate expectation of privacy his computer files). *But see Cunningham v. N.Y Dep't of Labor*, 997 N.E.2d 468 (N.Y. 2013) (employer's GPS search of employee's location was unreasonable because employer made no effort to avoid tracking an employee outside of business hours).

2. First Amendment

For public employees, the First Amendment does not protect against an employer's actual invasion of the employee's electronic privacy—such as searching or monitoring the employees' emails or internet activity. But it may prevent the employer from taking adverse action against the employee based on speech or communications the employer uncovered during such monitoring.

a. What kind of speech is protected?

(i) Speech as a "citizen": To receive the protection of the First Amendment, a public employee must be speaking as a "citizen"; statements made pursuant to an employee's official duties are not protected. *See Garcetti v. Ceballos*, 547 U.S. 410, 421 (2006) ("[W]hen public employees make statements pursuant to their official duties, the employees are not speaking as citizens for First Amendment purposes, and the Constitution does not insulate their communications from employer discipline.").

However, there is a growing case law holding that this requirement — that the public employee speak as a "citizen" rather than pursuant to her official duties — does not apply where there are concerns about academic freedom. Under these decisions, academic speech related to scholarship or teaching is protected regardless of whether it was made as part of an instructor's duties. *See Demers v. Austin*, 746 F.3d 402 (9th Cir. 2014); *Adams v. Trs. of the Univ. of N.C.–Wilmington*, 640 F.3d 550 (4th Cir. 2011).

(ii) Speech on a matter of "public concern": In order to receive First Amendment protection, public employee speech must deal with matters of "public concern." Matters of purely provide concern—such as personal gripes about internal office matters—are not protected. *See Connick v. Myers*, 461 U.S. 138 (1983). Speech involves matters of public concern "when it can be fairly considered as relating to any matter of political, social, or other concern to the community, or when it is a subject of legitimate news interest; that is, a subject of general interest and of value and concern to the public." *Lane v. Franks*, 134 S. Ct. 2369, 2380 (2014).

Internet and social media activity—including Facebook "likes"—may deal with matters of public concern. *See Bland v. Roberts*, 730 F.3d 368 (4th Cir. 2013) (holding that sheriff's deputy's "like" of the Facebook page of the sheriff's campaign opponent was speech on a matter of public concern because "liking a political candidate's campaign page communicates the user's approval of the candidate and supports the campaign by associating the user with it" and was "the Internet equivalent of displaying a political sign in one's front yard"). *See also Mattingly v. Milligan*, No. 4:11CV00215, 2011 WL 5184283 (E.D. Ark. Nov. 1, 2011) (finding that that two off-duty posts made by a county clerk employee on her Facebook wall about the firing of four colleagues touched upon a matter of public concern because the terminations received wide publicity and information about the discharges generated angry responses from county residents who were Facebook friends of the employee).

However, personal activity — particularly if it involves pornography or controversial social behavior — is generally not protected. *See San Diego v. Roe*, 543 U.S. 77 (2004) (in a claim by a police officer who was fired displaying homemade pornography on the internet, the Court had "no difficulty in concluding that [such] expression does not qualify as a matter of public concern under any view of the public concern test"). *See also Snyder v. Millersville Univ.*, No. 07-1660, 2008 WL 5093140, at *16 (E.D. Pa. Dec. 3, 2008) (holding that a student teacher's internet posting of a photograph of herself wearing a pirate's hat and holding a cup with a caption that read "drunken pirate" was not protected).

b. Even when public-employee speech receives some protection, it is far from absolute.

Even when a public employee's speech is entitled to some degree of protection, the government employer will still prevail if it shows that its interest, "as an employer, in promoting the efficiency of the public services it performs through its employees" outweighs the employee's interest "in commenting upon matters of public concern." *Pickering v. Bd. of Educ.*, 391 U.S. 563, 568 (1968). In conducting this so-called "*Pickering* balancing," the Supreme Court has observed that, "[w]hen close working relationships are essential to fulfilling public responsibilities, a wide degree of deference to the employer's judgment is appropriate." *Connick*, 461 U.S. at 151-52. For example:

- *Richerson v. Beckon*, No. C07-5590, 2008 WL 833076 (W.D. Wash. Mar. 27, 2008), *aff'd*, 337 F. App'x 637 (9th Cir. 2009): A teacher was assigned a new position requiring her to coach and mentor less experienced teachers. The teacher posted

https://thekeep.eiu.edu/jcba/vol0/iss10/30
DOI: 10.58188/1941-8043.1491

several blog posting that criticized teachers and said of the teachers' union's chief negotiator: "What I wouldn't give to draw a little Hitler mustache on the chief negotiator." The school received complaints from other teachers, including at least one who refused to be mentored by the teacher. The Ninth Circuit upheld a lower court's conclusion that this was sufficiently disruptive to tip the *Pickering* balance in favor of the employer.

- *Curran v. Cousins*, 509 F.3d 36 (1st Cir. 2007): A correction officer made various postings on the discussion board of a password-protected union website referring to the sheriff (who is African-American) as Hitler, urging administrators to engage in insubordination, and comparing correction officers to the victims of the Shoah. The First Circuit concluded that the statements were unprotected under the First Amendment because they "directly went to impairing discipline by superiors, disrupting harmony and creating friction in working relationships, undermining confidence in the administration, invoking oppositional personal loyalties, and interfering with the regular operation of the enterprise."

- *Gresham v. City of Atlanta*, 542 F. App'x 817 (11th Cir. 2013): A police officer was disciplined after posting on Facebook an accusation that another police officer in her department unethically interfered with an investigation. The court held that the plaintiff's speech failed the *Pickering* balancing test, reasoning that the government had a superior interest in maintaining discipline and good working relationships among employees, and noting that comments concerning officer performance and integrity can impact confidentiality and a department's efficient operation.

- *Graziosi v. City of Greenville*, 775 F.3d 731 (5th Cir. 2015): A police officer was terminated after publically criticizing the city's police chief on the mayor's public Facebook page. In addition to finding that the posting was not a matter of public concern, the Court said her statements caused a disruption by changing the attitudes of some of the officers who reported to the police chief.

- *Shepherd v. McGee*, 986 F. Supp. 2d 1211 (D. Or. 2013): A Department of Human Services case worker posted negative comments on her Facebook page about the recipients of public assistance. The court found that the employee's statements had

harmed her ability to perform her job duties in that her credibility was damaged—for example, she would not be an effective witness where testifying in juvenile court hearings was part of her job duties. The court found that the government's interests outweighed any First Amendment right the employee would have in posting her Facebook comments.

- *Stengle v. Office of Dispute Resolution*, 631 F. Supp. 2d 564 (M.D. Pa. 2009): The court held that a hearing officer's blog entries were not constitutionally protected because the employer's interests in efficiency and maintaining the appearance impartiality were sufficient to justify the adverse action. In reaching this conclusion, the court emphasized that the government can restrict employee speech based on its potential to disrupt, not only actual disruptiveness.

3. "Informational privacy"

In *NASA v. Nelson*, 562 U.S. 134 (2011), the Supreme Court rejected a claim advanced by a NASA contract employee that the agency's requirement that contractors undergo a background check violated any constitutional right of information privacy. The Court assumed, without deciding, that such a right may exist, but concluded that the inquiries — which included questions about treatment or counseling for recent illegal-drug use — were reasonable under the circumstances and therefore constitutional.

The *Nelson* Court's skeptical treatment of the plaintiff's constitutional right to informational privacy claims strongly suggests that are few, if any circumstances, in which the Court would recognize protections that are any broader than those already established under the Fourth Amendment.

B. State constitution

For the most part, state constitutions operate like the U.S Constitution and do not protect private sector employees from invasions of privacy by their employers.

One notable exception is the California Constitution, which by its terms protects broadly against both public and private intrusions on privacy. *See* Cal. Const. art. I, §1 ("All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy.").

However, these protections are fairly mild, for they guard only against unreasonable intrusions on privacy and where the employer's interests do not outweigh those of the employees. *See Hernandez v. Hillsides, Inc.*, 47 Cal.4th 272 (2009) (holding that employer's use of secret surveillance camera in two employees' offices did not

https://thekeep.eiu.edu/jcba/vol0/iss10/30
DOI: 10.58188/1941-8043.1491

violate the constitution because intrusion upon employees' reasonable privacy expectations was not sufficiently offensive or serious in light of the employer's need to detect activity that threatened the facility's wholesome environment for the children in its care); *see also TBG Ins. Servs. Corp. v. Superior Court*, 96 Cal. App. 4th 443 (2002) (concluding that private sector employee's constitutional claim failed because the employer gave notice that use of company computer at home could be monitored and use of computers in employment context carries with it social norms that effectively diminish employee's reasonable expectation of privacy).

IV. Labor Law Protections for Employee Privacy and Online Activity

A. National Labor Relations Act

The National Labor Relations Act (NLRA) provides an integrated scheme of rights, protections, and prohibitions governing the conduct of employees, employers, and unions during private-sector union organizing campaigns and representation elections. Two of the NLRA's provisions have significant implications for employee privacy.

The first, Section 7 of the NLRA, provides that private sector employees have the right to "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 . . . mutual aid or protection." 29 U.S.C. § 157.

The second, Section 8(a)(5) of the NLRA, 29 U.S.C. § 158(a)(5), requires a unionized employer in the private sector to negotiate with the union representing its employees before making changes to certain terms and conditions of employers.

1. Threshold issues

a. Are faculty "employees"?

The protections of the NLRA generally extend only to "employees," and not to "managers." *See NLRB v. Bell Aerospace Co.*, 416 U.S. 267 (1974) (explaining that "managers" exempt from the NLRA's protections are those "formulate and effectuate managerial policies by expressing and making operative the decisions of their employer")

In *NLRB v. Yeshiva Univ.*, 444 U.S. 672 (1980), the Supreme Court held that the faculty Yeshiva University could not be considered "employees" for purposes of the NLRA because they exercised authority that, in any other context, would be considered managerial. The Court explained:

> Their authority in academic matters is absolute. They decide what courses will be offered, when they will be scheduled, and

> to whom they will be taught. They debate and determine teaching methods, grading policies, and matriculation standards. They effectively decide which students will be admitted, retained, and graduated. On occasion their views have determined the size of the student body, the tuition to be charged, and the location of a school. When one considers the function of a university, it is difficult to imagine decisions more managerial than these. To the extent the industrial analogy applies, the faculty determines within each school the product to be produced, the terms upon which it will be offered, and the customers who will be served.

Id. at 686.

In the wake of the Court's decision in *Yeshiva*, lower courts have routinely found that university faculty are exempt from the NLRA's protections. *See*, *e.g.*, *Boston Univ. Chapter, AAUP v. NLRB*., 835 F.2d 399 (1st Cir. 1987) (faculty at Boston University are not "employees" for purposes of the NLRA); *Point Park Univ. v. NLRB*, 457 F.3d 42 (D.C. Cir. 2006) (same with regard to faculty of Point Park University).

However, in *Pacific Lutheran Univ.*, 361 NLRB No. 157 (2014), the National Labor Relations Board — recognizing the significant changes that have occurred in higher education in the 30+ years since the *Yeshiva* decision — articulated a new test for whether faculty should be considered "managers" for purposes of the NLRA. The NLRB held that, to be excluded from the Act's coverage as managerial employees, faculty must have a significant breadth and depth of decision-making authority. Noting that universities are now increasingly run by administrators, the NLRB concluded that it will examine the following areas to determine the faculty's degree of managerial participation: academic programs, enrollment management, finances, academic policy, and personnel policies and decisions. It also said that it will give greater weight to the first three factors, which the NLRB referred to as the "primary areas of decision-making." In the case before it, the NLRB concluded that the university failed to prove that its full-time contingent faculty members exercised managerial authority on the university's behalf. The record did not show that these faculty members actually controlled or made effective recommendations in the primary or secondary areas of decision-making. Furthermore, even in those areas in which the full-time contingent faculty members had some involvement in decision-making, the university failed to show that their involvement rose to the level of actual or effective control.

b. Are schools "employers"?

https://thekeep.eiu.edu/jcba/vol0/iss10/30
DOI: 10.58188/1941-8043.1491

The NLRA does not specifically exempt religious schools and institutions from coverage as "employers." However, in *NLRB v. Catholic Bishop*, 440 U.S. 490 (1979), the Supreme Court held that such an exemption was necessary to avoid concerns that the NLRA's jurisdiction would interfere with the practices of religious institutions protected by the Free Exercise Clause of the First Amendment.

Since the Court's decision in *Catholic Bishop*, lower courts have frequently held that the NLRB lacks jurisdiction over religiously affiliated colleges and universities. *See*, *e.g.*, *Univ. of Great Falls v. NLRB*, 278 F.3d 1335 (D.C. Cir. 2002); *Carroll Coll., Inc. v. NLRB*, 558 F.3d 568 (D.C. Cir. 2009)

However, in *Pacific Lutheran University, supra*, the NLRB held that asserting jurisdiction is permitted unless the university or college can satisfy a two-part test. First, as a threshold matter, the college or university must show "that it holds itself out as providing a religious educational environment." Evidence that a university or college holds itself out as providing such an environment includes handbooks, mission statements, corporate documents, course catalogs, and documents published on the school's website.

Second, the college or university must also show that "it holds out the . . . faculty members as performing a specific role in creating or maintaining the school's religious educational environment." In this inquiry, the focus is on the faculty members themselves, and looks at whether they are "held out as performing a specific religious function." If the faculty members cannot be distinguished from faculty members at nonreligious universities, they should not be excluded from the NLRA's coverage.

2. Protections for concerted activities

As noted above, Section 7 of the NLRA, provides that private sector employees have the right to "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 . . . mutual aid or protection." 29 U.S.C. § 157. This provision not only protects employees who engage in particular online activities, but it prohibits the employer from promulgating and enforcing certain overbroad restriction on employees' online activity. It is important to note that employees need not be unionized in order to enjoy the protections of Section 7; it applies generally to the concerted activities of private sector employees.

In *Hispanics United of Buffalo*, Inc. 359 NLRB No. 37 (2012), several employees made off-duty social media posts related to criticisms about the quality of their work. The NLRB held that the employer's fired them for these activities violated the employees' Section 7 rights.

In *Bettie Page Clothing*, 361 NLRB No. 79 (2014), the NLRB held that Facebook posts by employees of a clothing store were protected concerted activity for three reasons: first, the posts were a continuation of their complaints to the employer concerning working late in an unsafe area; second, they "were complaints among employees about the conduct of their supervisor as it related to their terms and conditions of employment and about management's refusal to address the employees' concerns"; and, third, the posts discussed consulting a book on California workplace rights.

In *Three D, LLC*, 361 NLRB No. 31 (2014), the NLRB found that the employer violated the Section 7 rights of two employees by discharging them for participating in a Facebook discussion about perceived errors in the employer's tax withholding calculations. The Board also found that the employer's "Internet/Blogging" policy in its employee handbook was unlawful under Section 7 because its prohibition of inappropriate discussions on the internet was vague and that employees would reasonably read it to prohibit discussions relating to their terms and conditions of employment.

In *Purple Communications*, 361 NLRB No. 126 (2014), the NLRB held that "employee use of email for statutorily protected communications on nonworking time must presumptively be permitted by employers who have chosen to give employees access to their email systems." The NLRB arrived at that conclusion by balancing the employees' rights to self-organization on the one hand and employers' rights to maintain business production and discipline on the other. The NLRB noted that e-mail has become a mainstay in business operations and therefore virtually indispensable for concerted activity. Furthermore, the NLRB concluded that there is less operational impact in allowing union-related communications on employer e-mail systems than on traditional employer "equipment" such as telephones and bulletin boards.

The *Purple Communications* rule has several important caveats. First, it applies only to employers that have already granted employees access to their e-mail systems; employers are not forced to give business e-mail access to employees who typically don't have such access. Second, employees can use business e-mails for union purposes only on "nonworking" time. Third, employers may still control their e-mail systems to the extent necessary to "maintain production and discipline." That includes monitoring e-mails to ensure informational security or even implementing an absolute ban on non-work use of e-mail if "special circumstances" so warrant. Fourth, the decision

https://thekeep.eiu.edu/jcba/vol0/iss10/30
DOI: 10.58188/1941-8043.1491

doesn't create any rights for nonemployees (such as "managers" or outside union representatives) to access business e-mail systems and doesn't address other types of electronic communications systems (such as social media accounts).

3. Protections for collective bargaining

Under Section 8(a)(5) of the NLRA, a unionized employer in the private sector cannot unilaterally change certain terms and conditions of employment — called "mandatory" subjects of bargaining — without first negotiating with the union.

Although there are few decisions dealing with employer computer monitoring, there are good reasons to believe that the NLRB and courts would agree that such monitoring — particularly when it might be used to discover and punish employee misconduct — would qualify as a mandatory subject of bargaining. As such, the employer could not unilaterally implement new policies without bargaining.

First, several decisions have already held that an employer's use of hidden surveillance cameras are a mandatory subject of bargaining. These courts have reasoned that such devices can be used to expose misconduct, and their use can have a significant impact on job security. *See National Steel Corp. v. NLRB*, 324 F.3d 928 (7th Cir. 2003); *Brewers & Maltsters, Local Union No. 6 v. NLRB*, 414 F.3d 36 (D.C. Cir. 2005)

Second, the NLRB has found on a number of occasions that unilaterally changes policies relating to employees' access to the use of our computers are a mandatory subject because they affect the manner in which the employee performs the job and violations of such restrictions may result in discipline. *See Associated Servs. for the Blind*, 299 NLRB 1150 (1990) (employer's computer access and use policy is a mandatory subject); *California Newspapers Partnership*, 350 NLRB 1175 (2007) (e-mail use policy).

B. Public-sector collective-bargaining laws

Many public-sector collective-bargaining laws are patterned, to some degree, on the NLRA. As a result, many state labor boards look to decisions interpreting the NLRA for guidance in construing their own public-sector laws. However, there is also a wide degree of variation among these laws — including limitations on striking and other such concerted activities, as well as restrictions on the subjects of bargaining.

1. Protected activity

Many states have some provision analogous to Section 7 of the NLRA. These provisions have been interpreted in a variety of ways when it comes to claims that particular employee's online or computer activities are legally protected:

- *City of Detroit (Police Dep't),* 19 MPER ¶ 15 (2006), *aff'd, City of Detroit v. Detroit Police Officers Ass'n*, 2007 WL 4248562 (Mich. Ct. App. 2007): The state labor board concluded that the employer violated the public-sector bargaining law when it ordered a police officer to discontinue operating an off-duty website that he, his fellow officers, and the public used to discuss police department affairs, and then suspended the officer for refusing to do so.

- *Mid-Michigan Community Coll.*, 26 MPER ¶ 4 (2012) (MI): The state labor board dismissed a charge that an adjunct professor was unlawfully fired for meeting with union representatives about an organizing drive and by sending emails to the adjunct faculty and the college president announcing the campaign's commencement. While the professor's union organizing efforts were clearly protected, the college was found to have not violated the law because its decision to discharge was motivated by the professor's inappropriate and unprofessional Facebook posts concerning a student.

- *City of Saginaw*, 23 MPER ¶ 106 (2010) (MI): Finding a violation when an employer disciplined a police officer for sending a group e-mail through the employer's computer system criticizing the employer for engaging in bad faith bargaining, and making a negative reference to the city manager's relationship with a public administrator's organization. The e-mail was found to be protected concerted activity because it discussed the employer's conduct during negotiations, and the reference to the city manager was in the context of the discussion concerning negotiations. Finally, the labor board found the discipline to be discriminatory because other employees were permitted to send non-work related emails through the system, and the union used the system to send e-mails to its members.

- *David Gee, Sheriff of Hillsborough County*, 35 FPER ¶ 191, 2009 WL 8157366 (2009), *aff'd, Sheriff of Hillsborough County v. Dickey*, 32 So. 3d 631 (Fla. Dist. Ct. App. 2010) (per curiam): The labor board concluded that a police union president engaged in protected concerted activity when his two articles were posted on the union's website discussing contract issues, which contained disparaging,

https://thekeep.eiu.edu/jcba/vol0/iss10/30
DOI: 10.58188/1941-8043.1491

belittling, and insubordinate statements about the sheriff's chief deputy.

- *Sheriff of Alachula County*, 36 FPER ¶ 16 (2010) (FL). Dismissing a charge of unlawful discipline stemming from an employee's e-mail urging other employees to vote against a pending labor agreement negotiated by an incumbent union and encouraging them to join his competing union. Although the employee was off duty (in fact, on vacation) when he sent the email, he sent it to other employees at their work addresses, thus violating a prohibition on distributing union-related literature during working hours in areas where work is performed.

- *In re State of New York (Division of Parole)*, 41 NYPERB ¶ 3033 (2008) (NY): Finding protected a shop steward's off-duty e-mail, which encouraged unit members to report to work on a holiday to test a contractual argument, was unprotected. The labor board concluded that the e-mail could not be reasonably construed as seeking to disrupt, confront, or to instigate an unprotected protest.

- *State of New York (Public Employees Federation)*, 33 NYPERB ¶ 3046 (2000), *aff'd sub nom. In re Benson v. Cuevas*, 293 A.D.2d 927 (N.Y. App. Div. 2002). Holding that an employer did not commit a violation by blocking a union activist's access to its e-mail system, because it was motivated by the activist's insubordination for refusing to stop sending controversial blast e-mails to union members relating to budgetary and collective bargaining issues.

- *Orange County Board of County Commissioners*, 38 FPER ¶ 131 (2011) (FL): Holding that portions of a county fire department's social media policy were overbroad and chilled the firefighters' right to engage in concerted activity for mutual aid and protection. The labor board found that prohibiting firefighters from using personal devices to access the internet constituted interference with their statutory rights to engage in off-duty electronic protected concerted activities. It also found the several rules in the policy — including one that firefighters "shall not criticize or ridicule or debase the reputation of the Department, its officers or other employees through speech, writing or other expression" and one that prohibits posts that "[t]ends to interfere with the maintenance of proper discipline . . [or] [d]amages or impairs the reputation and/or efficiency of the Department or its employees" — interfered with protected concerted activities. However, FPERC concluded that the policy's restriction on employee use of department property and resources to engage in social

networking did not facially or intentionally interfere, restrain, or coerce employees in exercising their rights.

- *Fla. Bd. of Educ.*, 29 FPER ¶ 89 (2003) (FL): Holding that state university's ban on solicitation and distribution at all times and in all work areas, including use of university's e-mail system, was overbroad and violated employee's rights to engage in protected activities.

2. Subjects of bargaining

Again, many states have public-sector bargaining laws that require employers to bargain over mandatory subjects before implementation. But variations in what qualifies as mandatory make it difficult to generalize about the protections that would apply if a state-run university unilaterally implemented electronic surveillance measures.

- *Univ. of Mich.*, 25 MPER ¶ 64 (2012) (MI): Finding no obligation to bargaining before installing a single hidden camera used to discover the identity of persons frequenting a room that had been surreptitiously constructed without the employer's knowledge or consent, and to discover the nature of the activities occurring in that room. The labor board, in distinguishing the NLRB cases dealing with hidden cameras, reasoned that the activities that took place in the hidden room were neither relevant nor connected to the employees' job responsibilities.

- *City of Patterson*, 33 NJPER ¶ 50 (2007) (NJ): No duty to bargain over cameras that were placed overtly and that served primarily as a public safety measure.

- *Nanuet Union Free Sch. Dist.*, 45 PERB ¶ 3007 (2001) (NY): Finding a duty to bargain over the installation of hidden cameras because it "bears a direct and significant relationship to working conditions," and it intrudes upon employee interests including job security, privacy and personal reputation.

- *City of Hartford*, 2014 WL 7967508 (2014) (CT): Concluding that video and audio surveillance is a mandatory subject of bargaining.

- *Amalgamated Transit Union v.Tri-County Metro. Transp. Dist.*, 2014 WL 5808351 (2014) (OR): Concluding that "continuous electronic recording of bus operators" is a mandatory subject of bargaining.

https://thekeep.eiu.edu/jcba/vol0/iss10/30
DOI: 10.58188/1941-8043.1491

- *Ass'n of Eng'g Employees v. State of Oregon*, 2013 WL 3465251 (2013) (OR): Holding that state's "unilateral decision to prohibit the use of its e-mail system for Association-related communications" was a violation because it involved a mandatory subject of bargaining.

- *Department of Veterans Affairs*, 50 FLRA 220 (1995): Holding that an agency has the duty to provide an exclusive representative with prior notice and an opportunity to bargain over the impact and implementation of management's decision to install covert surveillance cameras as part of its internal security practices.

- *Vermont State Employees' Ass'n v. State of Vermont (Re: Electronic Communications Policy)*, 2009 WL 2487431 (2009) (VT): Concluding that employer's computer use policy is a mandatory subject since employees may be subject to discipline for electronic communications or transactions, such as email communications, in which they represent themselves as state employees even though they are not using or accessing state equipment. But finding no violation because new policy did not represent a material change from old policy.

- *Clay Educational Staff Professional Ass'n v. Clay County Sch. Dist.*, 34 FPER ¶ 139 (2008) (FL): Assuming without deciding that electronic surveillance of employees is a mandatory subject of bargaining.

- *Kansas State Troopers Ass'n v. Hwy. Patrol*, 1990 WL 10555579 (1990) (KS): Concluding that electronic surveillance is not a mandatory subject of bargaining because it is already regulated by criminal and civil statutes, as well by the Fourth Amendment of the U.S. Constitution.

- *In re State of Connecticut*, 2010 WL 11030258 (2010) (CT): Holding that the state did not unilaterally change policies or work rules because its Acceptable Use of State Systems Policy was a reasonable measure designed to enforce existing rules and conditions of employment.

- *City of Okmulgee*, 124 Lab. Arb. (BNA) 423 (2007) (OK). The union challenged a police departments unilateral establishment of the new policies that set standards for use of city property, including a "Computers and Internet" policy. The arbitrator found that these changes were not mandatory subjects of bargaining because they did not materially, substantially, or significantly affect the terms and conditions of employment.

C. "Just cause" and civil service protections

In the both the private and public sectors, many collective-bargaining agreements protect employees against discipline except for "just cause." Many civil service laws incorporate similar protections for public sector employees. These protections can guard against adverse action for an employee's online activities. The degree of such protection often depends on whether the conduct took place off-duty and whether there were circumstances that militate against imposing a harsh penalty:

- *Land v. L'Anse Creuse Pub. Sch. Bd. of Educ.*, No. 288612, 2010 WL 2135356 (Mich. Ct. App. 2010), *appeal denied*, 789 N.W.2d 458 (Mich. 2010). A teacher was terminated after photographs were posted on a website showing her engaged in oral sex with a male mannequin during an off-duty party. The photographs were taken during the party without the teacher's knowledge and posted on the website without her consent. Although the photographs were removed from the website at the teacher's insistence, the school district terminated her for engaging in lewd behavior that undermined her moral authority and professional responsibility. The State Tenure Commission reversed the discharge on the grounds the event took place at a private party two years earlier with no students present, the conduct was not illegal, it did not have any nexus to school activities, and it was not related to her pedagogical responsibilities. Despite the negative publicity caused by the posting of the photographs, the State Tenure Commission concluded that it was insufficient to demonstrate just and reasonable cause under Michigan's teacher tenure law.

- *Warren County Bd. of Educ.*, 124 Lab. Arb. Rep. (BNA) 532 (2007). An arbitrator upheld the discharge of an Ohio high school mathematics teacher under contractual just cause and progressive discipline provisions after the teacher's estranged wife posted obscene nude photographs of him on websites and on a popular social media page (so-called "revenge pornography"). The arbitrator reasoned that high school students could access the photographs, which undermined the teacher's role-model status and credibility. The arbitrator criticized the teacher for failing to secure the photographs, from failing to take appropriate legal action in response to his estranged wife's threats, and in failing to warn his principal of the potential release of the photographs.

- *NYC Sch. Dist. v. McGraham*, 958 N.E.2d 897 (N.Y. 2011). A teacher provided her student with her personal e-mail address, and frequently communicated electronically with him after school about cultural and personal issues. Moreover, their e-mail exchanges and her anonymous blog entries demonstrated feelings that went well beyond those appropriate for a teacher-student relationship. Despite the seriousness of her misconduct, the arbitrator concluded that termination was too serious a punishment and, instead, imposed a suspension without pay and reassignment to another school. In deciding that the discharge was inappropriate, the arbitrator considered the teacher's remorse

https://thekeep.eiu.edu/jcba/vol0/iss10/30
DOI: 10.58188/1941-8043.1491

when confronted with the allegations, her cessation of communications with the student, the abandonment of her personal blog, and the fact she obtained professional therapy to heal the emotional issues that led to her misconduct. The state's highest court found that the policy favoring protection of children did not constitute an absolute mandate requiring vacatur of an arbitral penalty short of discharge.

- *Rubino v. City of New York*, 950 N.Y.S.2d 494 (N.Y. Sup. Ct. 2012), *aff'd*, 965 N.Y.S.2d 47 (N.Y. App. Div. May 7, 2013): An intermediate appellate court affirmed the vacatur of the discharge of a New York City tenured teacher for making inappropriate off-duty Facebook posts after the drowning death of a school district student. (In one post, the teacher stated: "After today, I am thinking the beach sounds like a wonderful idea for my 5th graders! I HATE THEIR GUTS! They are the devils [sic] spawn!") The termination imposed by the arbitrator was set aside based upon the teacher's unblemished 15-year career, the posts were made off-duty following a difficult day at school, they were deleted three days after they were posted, students and parents were not on-line friends of the teacher, and the comments did not impact her ability to teach and did not harm her students.

- *In re Palleschi v. Cassano*, 102 A.D.3d 603 (N.Y. 2013): The state's highest court sustained the discharge of a Fire Department emergency medical services supervisor and lieutenant, who posted on his Facebook page a photograph of a computer screen containing the name, address, and confidential medical information of a female 911 caller, which was accessible to hundreds of his Facebook friends. At the time of the posting, the lieutenant knew that the disclosure of patient information violated departmental rules and was a breach of trust.

- *U.S. Steel Corp.*, 130 Lab. Arb. (BNA) 461 (2011): Employer lacked just cause to discharge employee on the basis of three off-duty Facebook messages sent to his mother-in-law during a contested divorce and child custody fight.

- *Baker Hughe*s, Inc. 128 Lab. Arb. (BNA) 37 (2010): Employer had just cause to discharge employee for his off-duty post referencing the plant manager as "German, green card terminator" and stating "I could have sworn that Hitler committed suicide." The national origin slur violated the employer's anti-harassment policy and the employee failure to show remorse or apologize for the content of his post.

- *A.E. Staley Mfg. Co*., 119 Lab. Arb. Rep. (BNA) 1371 (2004): Upholding termination where employees were "repeatedly advised against using the computer for personal business and especially not to use it to download or transmit pornography"

V. State Sunshine/Open Records Laws

One potential threat to employee privacy comes, not from snooping employers, but from members of the public or press who seek employee e-mails, cell-phone records, and other information under state sunshine or open records laws. As a general matter, these laws protect communications that are private in nature, but not those that deal with the performance of public functions:

- *Am. Tradition Inst. v. Rector & Visitors of Univ. of Va.*, 287 Va. 330 (2014): Professor's email correspondence were either personal (not a public record) or proprietary (exempt from state open records law).

- *Denver Pub. Co. v. Board of County Com'rs*, 121 P.3d 190 (Colo. 2005): "Public records" included only e-mail messages concerning performance of public functions or public funds, and not sexually explicit and romantic e-mails between employees.

- *Tribune-Review Pub. Co. v. Bodack*, 961 A.2d 110 (Pa. 2008): Privacy rights of city council members precluded disclosure of cell phone records under right-to-know law.

- *Associated Press v. Canterbury*, 688 S.E.2d 317 (W. Va. 2009): Personal e-mail by public official or employee, which does not relate to conduct of public's business are not a public record subject to disclosure.

- *Schill v. Wisconsin Rapids School Dist.*, 786 N.W.2d 177 (Wis. 2010): Teachers' personal e-mails sent on school district e-mail accounts and district-owned computers are not public records under Wisconsin law.

- *Easton Area Sch. Dist. v. Baxter*, 35 A.3d 1259 (Pa. Commw. Ct. 2012): Personal e-mails sent by or received from the e-mail addresses of school board members, school district superintendent, and the general school board address that did not document a transaction or activity of the school district were not records subject to disclosure under the Right to Know Law

- *Griffis v. Pinal County*, 156 P.3d 418 (Ariz. 2007): E-mails generated or maintained on a government-owned computer system are not automatically public records, and the government may withhold documents of a purely private or personal nature.

- *State v. City of Clearwater*, 863 So. 2d 149 (Fla. 2003): Public employees' personal e-mails did not fall within the definition of public records subject to disclosure by virtue of their placement on a government-owned computer system.

https://thekeep.eiu.edu/jcba/vol0/iss10/30
DOI: 10.58188/1941-8043.1491