"EYE IN THE SKY": EMPLOYEE SURVEILLANCE IN THE PUBLIC SECTOR[1]

*Stuart S. Waxman**
*Frank G. Barile***

Developments in modern technology, such as digital video, GPS, and email and computer monitoring software, have made it exponentially easier for employers to monitor and investigate employees, safeguard company property, and increase employee productivity.[2] However, as these forms of surveillance technology become more readily accessible to a majority of employers, more and more employers are at an increased risk of infringing upon employee rights. This is especially true in the public sector, where, in New York, employers are bound by the strictures of the Taylor Law,[3] which governs the rights of unions for public employers in New York, as well as the limitations on warrantless searches and seizures pursuant to the Fourth Amendment of the United States Constitution.[4] In addition, public employers must be wary of the multitude of state and federal statutes designed to protect employee privacy.[5]

The widespread use of such surveillance by employers in recent years has been well-documented:

- a 2007 survey[6] conducted by the American

[1] Reprinted with permission from the Labor & Employment Law Section Annual Meeting Book, Copyright 2015, published by New York State Bar Association; www.nysba.org.

* Partner at Thomas, Drohan, Waxman, Petigrow & Mayle, LLP

** Associate at Thomas, Drohan, Waxman, Petigrow & Mayle, LLP

[2] *See* Charles E. Frayer, *Employee Privacy and Internet Monitoring: Balancing Workers' Rights and Dignity with Legitimate Management Interests*, 57 BUS. L. 857, 858–59 (2002); John Soma et al., *Bit-Wise but Privacy Foolish: Smarter E-Messaging Technologies Call for a Return to Core Privacy Principles*, 20 ALB. L.J. SCI. & TECH. 487, 491–92 (2010).

[3] N.Y. CIV. SERV. LAW §§ 200–214 (McKinney 2015); William A. Herbert, *Card Check Labor Certification: Lessons from New York*, 74 ALB. L. REV. 93, 97 n.8 (2011).

[4] U.S. CONST. amend. IV; CIV. SERV. §§ 200–214.

[5] *See infra* Part III.

[6] AM. MGMT. ASS'N. & EPOLICY INST., 2007 ELECTRONIC MONITORING & SURVEILLANCE SURVEY 1 (2007), http://www.plattgroupllc.com/jun08/2007ElectronicMonitoringSurveillance Survey.pdf.

Management Association ("AMA") and the ePolicy Institute found that, among the companies surveyed:
    - 66 percent monitor employee Internet activity;[7]
    - nearly half (48 percent) use video monitoring to counter theft, violence, and sabotage, while 7 percent use video surveillance to track employees' on-the-job performance;[8]
    - 45 percent monitor time spent and numbers called from office phones, while another 16 percent record phone conversations;[9]
- two studies by Aberdeen Group in 2012 found that 62 percent of employers with field employees use GPS to track staff, as reported by Workforce Magazine; and[10]
- a 2013 poll found that 37 percent of the hiring managers and human resources professionals surveyed use social networking sites to prescreen candidates for employment.[11]

This article will summarize and analyze the cases and statutes that define the legal framework within which New York public employers, including school districts, must operate when implementing particular forms of employee surveillance, such as video surveillance, email monitoring, and GPS tracking. Part I will examine a public employer's duty to negotiate when it comes to employee surveillance, and includes summaries of the pertinent decisions of the New York Public Employment Relations Board ("PERB") and discusses what these decisions mean for public employers. Part II will synopsize the pertinent case law interpreting the Fourth Amendment of the United States Constitution, as it applies to searches in the employment context, including the monitoring of employee text messages on employer-issued cell phones, and the installation of GPS on private employee vehicles to track employee whereabouts. Finally, Part III will briefly summarize the state and federal statutes that apply to the different forms of

[7] *Id.*

[8] *Id.* at 3.

[9] *Id.*

[10] Caren Chesler, *Turn Here: GPS Tracking Gaining Acceptance*, WORKFORCE (Mar. 7, 2013), http://www.workforce.com/articles/turn-here-gps-tracking-gaining-acceptance.

[11] *Thirty-Seven Percent of Companies Use Social Networks to Research Potential Job Candidates, According to New CareerBuilder Survey*, CAREERBUILDER (Apr. 18, 2012), http://www.careerbuilder.com/share/aboutus/pressreleasesdetail.aspx?id=pr691&sd=4%2F18%2F2012&ed=4%2F18%2F2099.

employee surveillance conducted by public employers in New York State.

I. NEGOTIABILITY OF EMPLOYEE SURVEILLANCE

An employer choosing to unilaterally carry out a method of employee surveillance must, in the first instance, ensure that such surveillance does not interfere with the right of its employees to negotiate the terms and conditions of their employment.[12] It can be difficult, however, for management to balance its obligation to supervise its employees, and maintain security of the workplace and its property, with its duty to negotiate.[13] This typically becomes an issue where a particular method of surveillance implicates employee job security, intrudes upon an employee's personal belongings or private information, or interferes with an employee's off-duty time.[14] Improper practice charges relating to employee surveillance can arise in varying contexts, depending on the type and location of the surveillance, the level of involvement required of the employees, and the purpose of the surveillance.[15]

A. Video Surveillance: Investigatory Use

A public employer's right to implement video surveillance in the workplace has been significantly curtailed by the Taylor Law and, as a result, it can be a particularly risky endeavor, even for legitimate investigatory purposes, as illustrated by *Civil Service Employees Ass'n and Nanuet Union Free School District*.[16] In *Nanuet*, PERB ruled that, in general, the decision by a school district to engage in videotape surveillance of a workplace for monitoring and investigating its employees is mandatorily negotiable under the

[12] *See* 29 U.S.C. § 158(d) (2013) (obligating employers to bargain with their employees' collective bargaining representative before changing employees' "wages, hours, and other terms and conditions of employment"); N.Y. CIV. SERV. LAW § 203 (McKinney 2015) ("Public employees shall have the right to be represented by employee organizations, to negotiate collectively with their public employers in the determination of their terms and conditions of employment, and the administration of grievances arising thereunder.").

[13] *See* ROBERT H. LAVITT, MONITORING EMPLOYEE WHEREABOUTS: COLLECTIVE BARGAINING IMPLICATIONS OF RFID AND GPS TECHNOLOGIES IN THE WORKPLACE 1–2 (2011), http://www.americanbar.org/content/dam/aba/administrative/labor_law/meetings/2011/ac2011/155.authcheckdam.pdf.

[14] *See* Civil Serv. Emps. Ass'n, Local 1000, 45 N.Y. P.E.R.B. ¶ 3007 (2011) [hereinafter *Nanuet*].

[15] *See id.*

[16] *See generally id.* (discussing the balance between the employer's mission and the employees' privacy).

Taylor Law.[17] This case dealt with two instances of investigatory video surveillance, both of which were deemed to affect the terms and conditions of employment: in the first instance, the District decided to conduct camera surveillance in hallways and other public locations, the footage from which could be used in the pursuit of disciplinary charges against unit employees; secondly, the District separately informed the union that it was "probable" that a camera would be placed in a common area outside the custodial room of one of the District's schools, in order to investigate how much time a particular custodian was spending off-task.[18] In the case of the surveillance of the custodian, the subject camera captured him (and another unit employee) entering and leaving the custodial room on thirty-nine occasions over the course of approximately six months.[19]

In its decision, PERB distinguished the present case from *Custodian Ass'n of Elmont*,[20] where, in response to parental complaints about a bus driver's unsafe driving practices, a school district hired a private investigator to follow and videotape the driver over the course of two days.[21] In that case, the administrative law judge ("ALJ") ruled that the school district had no duty to bargain because the district's use of video surveillance was "investigatory and preliminary to the disciplinary action eventually pursued."[22] In *Nanuet*, PERB noted that "the length and scope of the surveillance was far-broader and more intrusive upon employee interests than the limited surveillance conducted in *Elmont*."[23]

Ultimately, because the union's charge was untimely, PERB did not decide whether the District's use of video surveillance in *Nanuet* violated the Taylor Law.[24] However, the *Nanuet* decision is noteworthy for employers because it means that, in the school setting, where videotape surveillance is not integral to the employer's mission (as it would be, for example, in a correctional facility), a District's decision to implement extensive video surveillance is likely to result in the filing of an improper practice charge against the District.[25] Such a charge would require an ALJ to conduct a "fact-specific examination of employer and employee interests" in order to

[17] *See id.*
[18] *Id.*
[19] *Id.*
[20] Custodian Ass'n of Elmont, 28 N.Y. P.E.R.B. ¶ 4693 (1995).
[21] *Id.*
[22] *Id.*
[23] *Nanuet*, 45 N.Y. P.E.R.B. ¶ 3007.
[24] *Id.*
[25] *See id.*

determine "whether the videotaping significantly or unnecessarily intrudes upon the protected interests of unit employees."[26]

In reconciling *Nanuet* and *Elmont*, an important takeaway is that investigatory surveillance, if conducted over an unnecessarily long period of time, can impact working conditions in violation of the Taylor Law.[27] At this point, it is uncertain as to where PERB might eventually draw the line as to what is an acceptable period of time to record, given the current precedent of the two-day stakeout in *Elmont* and the six-month video investigation in *Nanuet*.

Still, even if an employer's particular installation or use of video surveillance is a non-mandatory subject of bargaining, the employer's decision to use the tapes in disciplinary proceedings may still be subject to impact bargaining as it affects disciplinary procedures, which are mandatorily negotiable.[28] In *Amalgamated Transit Union*,[29] a public employer refused the union's demand to bargain the impact of using video footage from bus surveillance cameras in disciplinary proceedings.[30] PERB, in affirming the ALJ's finding, held that the employer violated its bargaining obligation when it refused to bargain the impact of using the video footage.[31]

B. Video Surveillance: Non-Investigatory Use

A pair of conflicting PERB decisions has called into question the propriety of using video cameras for the purpose of supervising employees or ensuring the security of the employer's premises.

In *City of Syracuse* (1981),[32] the ALJ dismissed the union's complaint regarding the City's decision to install video cameras in a police garage.[33] In a sweeping opinion, the ALJ reasoned that, as long as employees are not required to participate in the recording process, a public employer is privileged to install and use a camera system "[b]y virtue of its accountability for public funds . . . to supervise its employees, and to maintain the security of its property."[34]

However, thirty years later, in 2011, a different PERB ALJ

---

[26] *Id.*
[27] *Id.*
[28] Amalgamated Transit Union, Local 1342, 36 N.Y. P.E.R.B. ¶ 3036 (2003).
[29] *Id.*
[30] *Id.*
[31] *Id.*
[32] City of Syracuse, 14 N.Y. P.E.R.B. ¶ 4645 (1981).
[33] *Id.*
[34] *Id.*

declined to follow the management-leaning rule articulated in *City of Syracuse*.[35] In *Civil Service Employees Ass'n and Town of Clarkstown*,[36] the ALJ held that the Town's installation of video cameras in the work areas of its highway garage was "little more than an enhanced investigatory tool to ascertain employee misconduct."[37] After balancing the employer's stated interest of protecting its assets "against the constant video monitoring of employee work performance and behavior with discipline as a stated consequence of such monitoring," the ALJ deemed the Town in violation of the Taylor Law for failing to negotiate the installation and use of the cameras.[38]

Crucial to the outcome in *Town of Clarkstown* was the Town's statement that video footage could be used as evidence in a disciplinary proceeding if any employee was viewed on camera engaged in improper activity, since such a use would directly implicate employee job security.[39]

As a result of the *Town of Clarkstown* decision, the extent to which a public school district may use video surveillance for non-investigatory purposes is uncertain. Even if the district's stated purpose is safety or security, a decision to use video surveillance might still compromise employee job security or implicate employee privacy concerns (an issue that was not reached in *Town of Clarkstown*).[40] Such use of video surveillance could still, even if implemented in good faith, result in a Taylor Law violation requiring a balancing of interests.

C. GPS Technology in Employee Phones/ Cars

The question of whether a public employer is required to negotiate its use of global positioning system ("GPS") technology has been of increasing interest, given the proliferation of such technology in cell phones and automobiles in recent years.[41] On one hand, employers generally have a right to be aware of the location of their employees and property; on the other hand, unions have argued that the use of

[35] Civil Serv. Emps. Ass'n, Local 1000, 44 N.Y. P.E.R.B. ¶ 4625 (2011) [hereinafter *Town of Clarkstown*].

[36] *Id.*

[37] *Id.*

[38] *Id.*

[39] *Id.*

[40] *Id.*

[41] *See* Stewart F. Hancock, Jr., *New York State Constitutional Law—Today Unquestionably Accepted and Applied as a Vital and Essential Part of New York Jurisprudence*, 77 ALB. L. REV. 1331, 1339–40 (2014) (discussing the development of new, sophisticated electronics belonging to citizens that police and others can use to keep track of their movements).

GPS implicates employee privacy rights, interferes with off-duty time, and involves employee participation in record keeping and disciplinary matters.[42] One PERB ALJ had the opportunity to weigh in on this issue in two different cases.

In *Civil Service Employees Ass'n and County of Nassau*,[43] the ALJ held that the County was not obligated to negotiate its decision to require certain employees to carry cell phones containing an activated GPS.[44] This decision was based on the ALJ's finding that an employer's decision to use cell phones equipped with GPS "involves the manner and means by which an employer serves its constituency and hence is a management prerogative."[45]

The ALJ rejected the union's contention that employee privacy concerns outweighed the County's interest in the location of its employees on work time.[46] The ALJ stated that the employees' "privacy rights are no more compromised in this matter than if an employer assigned a supervisor to accompany an employee on a specific job assignment, a prerogative which an employer possesses."[47] In rejecting the union's argument that the GPS interferes with employees' off-duty time, the ALJ pointed out that the employees are permitted to turn their phones off at the beginning of lunch or breaks, and that, while the phone is off, employee' location is not tracked.[48]

In response to the union's argument that the use of GPS requires employee participation in record keeping and discipline, the ALJ pointed out that because employees were already required to keep logs of their workday activities, obligating employees to turn their phones off during lunch or breaks would not unilaterally increase employee participation in record-keeping, since "employees are doing nothing in addition to that which they had previously done."[49]

The ALJ reached a similar conclusion with regard to a village's installation of GPS in vehicles operated by public works department employees in *Civil Service Employees Ass'n and Village of Hempstead*.[50] As in *County of Nassau*, the ALJ held that the decision

---

[42] Civil Serv. Emps. Ass'n, Local 1000, 41 N.Y. P.E.R.B. ¶ 4553 (2008) [hereinafter *Cty. of Nassau*].

[43] *Id.*

[44] *Id.*

[45] *Id.* (quoting Police Ass'n of New Rochelle, 10 N.Y. P.E.R.B. ¶ 3042 (1977)).

[46] *Id.*

[47] *Id.*

[48] *Id.*

[49] *Id.*

[50] Civil Serv. Emps. Ass'n, Local 1000, 41 N.Y. P.E.R.B. ¶ 4554 (2008) [hereinafter *Vill. of*

to install GPS in Village vehicles related to the "manner and means by which an employer is providing services to the public," and dismissed the case accordingly.[51] Here, the ALJ added that, with respect to employer-owned vehicles, "[t]he Village has the managerial right . . . to know the location of its property whether or not an employee is on duty."[52]

Based on these cases, school districts and other public employers in New York appear to have more latitude with regard to unilateral installation and use of GPS in employee phones and vehicles than they do with regard to video surveillance.[53] Consider, for example, that while PERB typically considers the duration of the video monitoring to be a crucial element in determining whether a particular instance of video surveillance necessitates employer bargaining, the duration of GPS activation was a virtual non-issue, so long as the GPS monitoring did not carry over into an employee's off-duty time.[54] Similarly, while PERB has stated that an employer's interest in "protecting its assets" would not justify unilateral installation of video surveillance,[55] it appears that such an interest could more readily be used to defend an employer's use of GPS in employer-owned vehicles, given the ALJ's statement that a public employer has a managerial right to know the location of its property.[56]

Although these cases appear to give employers a great deal of leeway to use GPS technology, it is important to interpret them based on the facts of each case. For example, the ALJ in *County of Nassau* concluded that requiring employees to turn off their cell phones before lunches and breaks in order to deactivate the GPS did not constitute a unilateral increase in employee participation in record keeping based on the fact that the employer already required employees to keep records of their off-site activities.[57] An obligation to bargain could arise, however, in the absence of a similar record-keeping requirement.

An employer's stated purpose for utilizing GPS may also affect the

Hempstead].

[51] *Id.*

[52] *Id.*

[53] *Compare supra* Parts I.A–B (explaining that employers are often required to negotiate the use of video surveillance with employees), *with supra* Part I.C (noting that public employers can unilaterally track employees using GPS).

[54] *See Cty. of Nassau*, 41 N.Y. P.E.R.B. ¶ 4553; *Nanuet*, 45 N.Y. P.E.R.B. ¶ 3007.

[55] *See Town of Clarkstown*, 44 N.Y. P.E.R.B. ¶ 4625.

[56] *Vill. of Hempstead*, 41 N.Y. P.E.R.B. ¶ 4554.

[57] *Cty. of Nassau*, 41 N.Y. P.E.R.B. ¶ 4553.

ultimate determination as to whether an employer breached its duty to negotiate. In a National Labor Relation Board ("NLRB") advice memorandum,[58] a duty to bargain was found where an oil company unilaterally installed and began to utilize vehicle data recorders (which track vehicle location through GPS technology) for the purpose of monitoring and investigating employee misuse of company vehicles.[59] Because the technology was used as an investigatory technique for monitoring employee misconduct, it affected employee discipline and job security, ultimately causing a substantial and significant change to the terms and conditions of employment.[60] Although this case arose outside of New York in the private sector, it is instructional in illustrating how an employer's purpose for implementing a particular mode of surveillance may ultimately alter its duty to bargain.

D. Monitoring and Blocking of Emails

As a general rule, employers are permitted to ban nonwork related uses of employer communications-related equipment, including emails, telephones, bulletin boards, copy machines, and public address systems.[61] An employer's right to do so is generally not a mandatory subject of collective bargaining.[62] However, these rights occasionally clash with the rights of employees to engage in protected union activities.[63] These conflicts often arise in the case of email and typically result in the filing of improper practice charges under the Taylor Law.[64]

In *Public Employees Federation*,[65] one such conflict developed when the State Education Department ("SED") discontinued and blocked

---

[58] U.S. Nat'l Labor Relations Bd., Advice Memorandum on BP Exploration of Alaska, Inc. (July 11, 2005).

[59] *Id.* at 1.

[60] *Id.* at 9, 10.

[61] Guard Publ'g Co., 351 N.L.R.B. 1110, 1114, 1135–36 (2007), *aff'd in part, rev'd in part, sub nom*. Guard Publ'g Co. v. NLRB, 571 F.3d 53 (D.C. Cir. 2009).

[62] *See id.* at 1137 n.11.

[63] *See id.* at 1127 (Liebman & Walsh, dissenting) (citing Vons Grocery Co., 320 N.L.R.B. 53, 55 (1995); Honeywell, Inc., 262 N.L.R.B. 1402, 1402 (1982); Union Carbide Corp.-Nuclear Div., 259 N.L.R.B. 974, 980 (1982)).

[64] Under the Taylor Law, it is "an improper practice for a public employer or its agents deliberately to interfere with, restrain or coerce public employees in the exercise of their rights guaranteed in section two hundred two of this article for the purpose of depriving them of such rights," as well as "to discriminate against any employee for the purpose of encouraging or discouraging membership in, or participation in the activities of, any employee organization." N.Y. CIV. SERV. LAW § 209-a(1)(a), (c) (McKinney 2015).

[65] Pub. Emps. Fed'n, 33 N.Y. P.E.R.B. ¶ 3046 (2000).

the use of its computer-generated email system by one of its employees when, despite SED's policy that its "employees may not use state equipment for any use other than departmental business," and despite several warnings to cease from nonwork related use of the email system, the employee continued to use SED's email system to communicate with union members on subjects beyond the parameters set forth in the policy.[66] In determining that SED's decision to remove the employee's email capability was not improperly motivated, PERB was persuaded that SED's decision was prompted by the employee's refusal to comply with SED's directive, and not by the protected content of emails themselves.[67]

Public Employees Federation reiterated the long-recognized notion that employers can effectively ban otherwise protected communications transmitted through their email systems by implementing company-wide policies prohibiting all nonwork use of their facilities, including their email systems.[68] Until recently, the private sector operated in largely the same fashion under the NLRB's decision in *Register-Guard* (2007).[69] That is, until December 11, 2014, when the NLRB, in *Purple Communications, Inc.*,[70] overturned *Registered-Guard* and 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."[71] The NLRB indicated that its decision is "limited" insofar as employers may still ban nonwork use of their email systems, "including Section 7 use on nonworking time, by demonstrating that special circumstances make the ban necessary to maintain production or discipline."[72]

This decision represents a significant shift in this area of the law, as well as uncertainty for many private sector employers, who must now confront difficult questions with regard to their email policies; for example, many employers will have to determine whether special circumstances are present that would justify a ban on nonwork use

---

[66] *Id.*

[67] *Id.*

[68] *See id.*

[69] Guard Publ'g Co., 351 N.L.R.B. 1110, 1110 (2007), *aff'd in part, rev'd in part sub nom*. Guard Publ'g Co. v. NLRB, 571 F.3d 53 (D.C. Cir. 2009) ("[E]mployees have no statutory right to use [an employer's] e-mail system for [personal] purposes.").

[70] Purple Commc'ns, Inc., No. 21-CA-095151, 2014 N.L.R.B. LEXIS 952 (N.L.R.B. Dec. 11, 2014).

[71] *Id.* at *2.

[72] *Id.* at *4.

of their email systems.[73] Given the influence that private sector decisions can often have on the laws and bodies governing public sector employers, *Purple Communications, Inc.* warrants particular attention by all employers, especially in the event it is appealed.

II. FOURTH AMENDMENT RIGHTS OF PUBLIC EMPLOYEES

In addition to recognizing and adhering to its obligation to ensure that a particular mode of surveillance does not run afoul of the Taylor Law, government employers, including public school districts, must also comply with the Fourth Amendment's prohibition on unreasonable and warrantless searches of the private property of their employees.[74]

In *O'Connor v. Ortega* (1987),[75] the United States Supreme Court announced the standard that applies to searches and seizures in the workplace context.[76] In *O'Connor*, state hospital officials searched the office of one of its employees, a physician and psychiatrist, and seized several personal items from his desk and file cabinets.[77] The items were subsequently used as evidence in an administrative disciplinary proceeding against him.[78]

The *O'Connor* Court first recognized a "workplace" exception to the warrant requirement.[79] The plurality opinion stated that:

> In our view, requiring an employer to obtain a warrant whenever the employer wished to enter an employee's office, desk, or file cabinets for a work-related purpose would seriously disrupt the routine conduct of business and would be unduly burdensome. Imposing unwieldy warrant procedures in such cases upon supervisors, who

---

[73] *Id.* at *20 ("We recognize that the types of circumstances that arise in the context of email systems may be different from those arising in the context of employees' conduct on their employer's real property. Thus, an assertion of special circumstances will require that the employer articulate the interest at issue and demonstrate how that interest supports the email use restrictions it has implemented.").

[74] U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."); Edwin C. Darden, *Search and Seizure, Due Process, and Public Schools*, CTR. FOR PUB. EDUC. (Apr. 5, 2006), http://www.centerforpubliceducation.org/Main-Menu/Public-education/The-law-and-its-influence-on-public-school-districts-An-overview/Search-and-seizure-due-process-and-public-schools.html.

[75] O'Connor v. Ortega, 480 U.S. 709 (1987).

[76] *Id.* at 725–26.

[77] *Id.* at 712, 713.

[78] *Id.* at 713.

[79] *Id.* at 721–22.

> would otherwise have no reason to be familiar with such procedures, is simply unreasonable.[80]

The four-Justice plurality of the Court then articulated a two-part test in order to determine whether the search itself was reasonable.[81] First, a court must address whether an employee has a reasonable expectation of privacy "on a case-by-case basis,"[82] considering "[t]he operational realities of the workplace."[83] This prong recognizes "the great variety of work environments in the public sector."[84] Second, if the employee is deemed to have a reasonable expectation of privacy in the area searched, the employer's search "should [then] be judged by the standard of reasonableness under all the circumstances," considering "both the inception and the scope of the intrusion."[85] After applying the test, the Court determined that the physician "had a reasonable expectation of privacy at least in his desk and file cabinets,"[86] which were not shared with any other employees, but remanded the case to the District Court to evaluate the reasonableness of the inception and scope of the search.[87]

O'Connor has remained the standard for determining the scope of an employee's Fourth Amendment rights.[88] The applicability of this test has since expanded to various other types of searches that go well beyond searches of an employee's physical workspace, as illustrated by the following cases.

A. Monitoring of Text Messages on Employer-Issued Cell Phones

The Supreme Court did not have occasion to "clarif[y]" the *O'Connor* standard until more than two decades later, when it applied *O'Connor* to searches of employee text messages on government-issued pagers in *City of Ontario v. Quon*.[89]

In *Quon*, the City of Ontario, California issued alphanumeric pagers to employees through a contract with a service provider, Arch

---

[80] *Id.* at 722; *see also id.* at 732 (Scalia, J., concurring) ("[Warrantless searches] to investigate violations of workplace rules . . . do not violate the Fourth Amendment.").

[81] *Id.* at 711, 719–20.

[82] *Id.* at 718.

[83] *Id.* at 717.

[84] *Id.* at 718.

[85] *Id.* at 725–26.

[86] *Id.* at 719 (citing Gillard v. Schmidt, 579 F.2d 825, 828–29 (3d Cir. 1978); United States v. Speights, 557 F.2d 362, 364 (3d Cir. 1977); United States v. Blok, 188 F.2d 1019, 1021 (D.C. Cir. 1951)).

[87] *O'Connor*, 480 U.S. at 718, 729.

[88] City of Ontario v. Quon, 560 U.S. 746, 757 (2010).

[89] *Id.* at 750, 757.

Wireless, which afforded the City a monthly limit on the number of characters each pager could send or receive.[90] When several employees exceeded their monthly character limits for several months straight, the City requested that Arch Wireless provide it with transcripts of the text messages sent and received by two of its employees, including the respondent, over the course of two months.[91] The transcripts revealed that many of respondent's text messages "were not work related, and [that] some were sexually explicit."[92] The respondent was disciplined on the basis of the text messages.[93]

The Supreme Court, fearful of the implications that a broad holding might have due to the developing nature of the technology, assumed without deciding that the respondent had a reasonable expectation of privacy in the text messages sent on the pager; it also operated under the assumption that the City's review of the transcript constituted a Fourth Amendment search.[94] The Court then applied the second prong of the *O'Connor* test and determined that the search was reasonable because it "was justified at its inception because there were 'reasonable grounds for suspecting that the search was necessary for a noninvestigatory work-related purpose,'" and that the scope of the search "was reasonable because it was an efficient and expedient way to determine whether [the respondent's] overages were the result of work-related messaging or personal use."[95]

This decision is yet another illustration of how courts treat Fourth Amendment questions (and surveillance cases, generally) based on the unique facts presented. For example, it would be impossible to assume that this case would have turned out similarly had the City read through twelve months of text message transcripts as opposed to the two months of transcripts it actually accessed, since this would have presented a closer call as to whether the review was "'excessively intrusive.'"[96] Similarly, had the City officials accessed and read the text message transcripts for the purpose of employee monitoring generally, rather than for the limited purpose of determining whether the specific character overages were the result of work-related messaging or personal use, this case could have

[90] *Id.* at 750–51.
[91] *Id.* at 752.
[92] *Id.* at 752–53.
[93] *Id.* at 753.
[94] *Id.* at 760.
[95] *Id.* at 761 (quoting O'Connor v. Ortega, 480 U.S. 709, 726 (1987)).
[96] *Quon*, 560 U.S. at 761–62 (quoting *O'Connor*, 480 U.S. at 726).

turned out much differently.

B. GPS Technology in Employee Vehicles

New York's highest court recently had the opportunity to apply *O'Connor* to a state employer's attachment of a GPS device to an employee's personal car. In *Cunningham v. New York State Department of Labor*,[97] as part of an investigation of a state employee for his alleged unauthorized absences from work and falsification of records concealing those absences, the Department attached a GPS to the worker's personal car, without his knowledge, while the car was parked in a lot near the state office.[98] The GPS, and its two subsequent replacements, tracked the employee's car for over a month, including evenings, weekends, and during one vacation.[99] The employee was ultimately terminated, in part, as a result of the information gathered from the GPS recordings.[100]

The New York Court of Appeals, relying on United States Supreme Court (as well as its own) precedent regarding use of GPS in the criminal context, explained that attachment of a GPS device to an automobile constituted a Fourth Amendment search.[101] The court then held that the "workplace" exception to the warrant requirement applies to GPS searches by employers, explaining that because the employee "was required to report his arrival and departure times to his employer," he had a diminished expectation of privacy regarding the location of his personal car during working hours.[102] In comparing this interest to the employee's expectation of privacy in the areas at issue in *O'Connor*, including the employee's desk and the employee bulletin board, the court explained that "[t]he location of a personal car used by the employee during working hours does not seem to us more private."[103]

Despite its determination that the search did not require a warrant, the court ultimately held that the search was "excessively intrusive," and, as a result, was unreasonable under *O'Connor*.[104] The court stressed the fact that the State tracked "much activity with

---

[97] Cunningham v. N.Y. State Dep't of Labor, 997 N.E.2d 468 (N.Y. 2013).

[98] *Id.* at 470.

[99] *Id.*

[100] *Id.* at 470–71.

[101] *Id.* at 471 (citing United States v. Jones, 132 S. Ct. 945, 949 (2012); People v. Weaver, 909 N.E.2d 1195, 1203 (2009)).

[102] *Cunningham*, 997 N.E. 2d at 472.

[103] *Id.*

[104] *Id.* at 473 (quoting O'Connor v. Ortega, 480 U.S. 709, 726 (1987)).

which the State had no legitimate concern—i.e., it tracked [him] on all evenings, on all weekends and on vacation."[105] The court recognized the inherent difficulty in limiting a GPS search of an employee's car to avoid all tracking of private activity, but nonetheless concluded that the State could have "stop[ped] short of seven-day, 24-hour surveillance for a full month," making specific note of the possibility that the State could have removed the GPS prior to the employee's departure for his annual vacation.[106]

Despite its ultimate holding suppressing the State's use of GPS evidence in this instance, this case actually recognizes a significant and expansive right of employers to use GPS as a tool in employee investigations by permitting employers to covertly attach GPS devices to private employee vehicles that are used during working hours.[107] As a practical matter, however, the court's warning against tracking private activity may end up dissuading many employers from attempting to use GPS as the primary means of investigation, since it may prove too burdensome for employers to remove such devices from employee vehicles daily or weekly.[108]

C. Computer Hard Drive Searches

United States v. Simons,[109] despite the fact that it is not controlling on New York employers, is important insofar as it illustrates the power that an official company policy can have on a public sector employer's right to access digital materials stored on its own computer systems, over employee objections of unconstitutionality.[110]

In *Simons*, during a routine inspection of the computer system's firewall, the Central Intelligence Agency's ("CIA") network manager noticed a large amount of activity outside the network.[111] The network manager, upon further investigation, discovered that over one thousand pornographic images had been downloaded by one of the agency's engineers onto his hard drive.[112] The CIA had a policy stipulating that employees could use the Internet for "official business use, incidental use, lawful use, and contractor

---

[105] *Id.*

[106] *Id.*

[107] *Id.* at 472, 473.

[108] *Id.* at 473.

[109] United States v. Simons, 206 F.3d 392 (4th Cir. 2000), *aff'g*, 29 F. Supp. 2d 324 (E.D. Va. 1998).

[110] *Id.* at 398.

[111] *Simons*, 29 F. Supp. 2d at 325, 326.

[112] *Id.* at 326.

communications" and that the agency would conduct electronic auditing of the computer network to "support identification, termination, and prosecution of unauthorized activity."[113]

The district court, after giving "significant weight to the portion of the policy stating that audits shall be implemented to support identification, termination and prosecution of unauthorized activity," found that the defendant had no reasonable expectation of privacy with respect to any of his Internet activity.[114] The court went on to explain that, even if it had determined that the defendant had a reasonable expectation of privacy, the CIA's search was reasonable both at its inception and in its scope.[115]

The importance of a clear and controlling policy on Internet use is made evident by *Simons*. Having a company policy that clearly and entirely divests any employee expectation of privacy in employee Internet activity or email communications can conclusively settle a case in favor of the government employer even before an *O'Connor* analysis is considered.[116]

III. LAWS RESTRICTING EMPLOYEE SURVEILLANCE

In addition to the numerous cases and administrative decisions interpreting the Taylor Law and the Fourth Amendment as they pertain to employee surveillance, there are also various state and federal statutes governing the rights of employees to be free from certain intrusions by their employers.[117] Several of these statutes are summarized as follows:

A. Fair Credit Reporting Acts

Both public and private sector employers wishing to screen job applicants' social media communications must be mindful of laws that place restrictions on such background checks.[118] Among those laws is the federal Fair Credit Reporting Act ("FCRA"),[119] which applies whenever an employer hires an outside party to conduct such screenings.[120] Under the FCRA, an employer may not obtain a

[113] *Id.* at 327.
[114] *Id.*
[115] *Id.* at 327, 328.
[116] *See id.* at 327.
[117] *See infra* notes 119, 124, 126–27, 137 and accompanying text.
[118] Eric D. Bentley, *The Pitfalls of Using Social Media Screening for Job Applicants*, 29 A.B.A. J. LAB. & EMP. L. 1, 8–9 (2013).
[119] Fair Credit Reporting Act, 15 U.S.C. §§ 1681–1681x (2014).
[120] 15 U.S.C. § 1681a(f). However, an employer can circumvent the requirements of the

"consumer report"[121] from such an outside party unless it gives written notice to the applicant that a background check will be conducted, obtains the permission of such applicant, and certifies to the reporting agency that the background check will be for a statutorily-defined "permissible purpose," including for "adverse action."[122] The FCRA also contains procedural requirements by which employers must abide prior to taking any adverse employment action.[123] New York also has its own Fair Credit Reporting Act ("NYFCRA"),[124] which closely tracks the federal FCRA, but which has several additional procedural requirements.[125]

B. New York State Labor Law Section 201-d – Employee Recreational Activities

Under Section 201-d of the Labor Law, public and private sector employers are barred from taking adverse employment action against an individual based on, among other things, that "individual's legal recreational activities outside work hours, off of the employer's premises and without use of the employer's equipment or other property."[126] Although this statute does not explicitly mention social networking, it seems conceivable, if not likely, that Section 201-d may soon be the basis of an action brought on behalf of a job applicant who is allegedly denied employment because of that individual's participation in a legal recreational activity that is deemed objectionable by the employer, that was pursuant to the employer's screening of the applicant's social networking activity.

C. Electronic Communications Privacy Act

The federal Electronic Communications Privacy Act of 1986

FCRA by conducting its own employee background screening.

[121] A "consumer report" is defined as "any . . . communication of any information by a consumer reporting agency bearing on a[n] [individual's] credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used . . . as a factor in establishing . . . eligibility for . . . employment purposes." *Id.* § 1681a(d)(1), (d)(1)(B).

[122] *Id.* §§ 1681b(b)(1)–(3). An adverse action includes "a denial of employment or any other decision for employment purposes that adversely affects any current or prospective employee." *Id.* § 1681a(k)(1)(B)(ii).

[123] *Id.* §§ 1681b(b)(3)(A), 1681m(a).

[124] N.Y. GEN. BUS. LAW §§ 380–380-v (McKinney 2015).

[125] *Compare* 15 U.S.C. §§ 1681d(a) (2014) (requiring only notice to a consumer), *with* N.Y. GEN. BUS. LAW §§ 380-c(a) (requiring notice to consumer and the consumer's consent).

[126] N.Y. LAB. LAW §201-d(2)(c) (McKinney 2015).

("ECPA")[127] is a comprehensive legislation that protects wire, oral, and electronic communications while those communications are being made, are in transit, and when they are stored digitally.[128] The ECPA contains prohibitions on the interception of wire or electronic communications, and on eavesdropping on the content of telephone calls.[129]

Public employers are not specifically exempted from the ECPA.[130] However, the ECPA contains several exceptions, one of which, the "consent" exception,[131] would generally allow an employer to avoid liability under the ECPA by obtaining a blanket consent from each employee (for example, in the employee's contract or a signed copy of company policy) to monitor all emails sent on the employer's email system and/or record all telephone calls made via office telephones.[132]

D. New York State Penal Law Sections 250.00 and 250.05 – Prohibition on Eavesdropping

New York also has a law on its books, similar to those provisions federal Electronic Communications Privacy Act dealing with wire and oral communications, which makes it a class E felony to record or eavesdrop on an in-person or telephonic conversation without the consent of at least one party.[133] This law applies to employers, who are prohibited from eavesdropping without permission on telephone calls between employees and outside persons.[134] However, this provision would allow an employer to record or intentionally overhear a conversation or phone call involving one of its employees if the employer is either a party to the conversation or if the employer obtains permission from one party to the conversation in advance.[135]

---

[127] Electronic Communications Privacy Act, 18 U.S.C. §§ 2510–22 (2013).

[128] John R. Forbush, *Regulating the Use and Sharing of Energy Consumption Data: Assessing California's SB 1476 Smart Meter Privacy Statute*, 75 ALB. L. REV. 341, 355 n.80 (2012).

[129] 18 U.S.C. § 2511(1).

[130] *See* Rebecca Ebert, *Mailer Daemon: Unable to Deliver Message Judicial Confusion in the Domain of E-Mail Monitoring in the Private Workplace*, 1 J. HIGH TECH. L. 63, 66 (2002).

[131] 18 U.S.C. § 2511(2)(c).

[132] *See id.* § 2511(2)(d).

[133] N.Y. PENAL LAW § 250.05 (McKinney 2015); *see* N.Y. PENAL LAW § 250.00(1) (McKinney 2015).

[134] *See* N.Y. Op. Att'y. Gen. 272, 274–75 (1957) (interpreting former N.Y. PENAL LAW § 738, predecessor to §§ 250.00, 250.05).

[135] 2 JONATHAN L. SULDS, NEW YORK EMPLOYMENT LAW § 18.03(2)(c) (2015).

E. New York State Labor Law Section 203-c – Prohibition on Videotaping

Although New York does not recognize a common law right of privacy, there exists a statutory remedy for employees who are the subjects of surreptitious videotaping by their employers. Under section 203-c of the Labor Law, employers are forbidden from videotaping their employees in restrooms, locker rooms, or any room designated by an employer for employees to change their clothes.[136] This provision provides for civil remedies, including damages and attorneys' fees, to employees prevailing in a civil action alleging a violation of this section.[137]

CONCLUSION

With perhaps the sole exception of criminal law, there is perhaps no other context in which the laws regarding government surveillance are more prominent and more controversial than they are with regard to the workplace. Of course, this distinction, along with the sharp and significant increases in the types and availability of surveillance and monitoring equipment, has resulted in an extensive list of rules and requirements that government employers must follow prior to the implementation of any new mode of employee surveillance. These rules, however, which define everything from the negotiation rights of unions to the privacy rights of employees, have truly and irreversibly shaped the modern workplace.

[136] N.Y. LAB. LAW § 203-c(1) (McKinney 2015). An exception exists for videotaping pursuant to a court order. *Id.*

[137] *Id.* § 203-c(3).