Workplace Monitoring in an Age of Endless Innovation

Matthew Helland, Nichols Kaster, PLLP
Nicky Jatana, Jackson Lewis, PC
Michelle Hackim, Jackson Lewis, PC
Danielle Lucido, Engineers and Scientists of California Local 20, IFPTE, AFL-CIO & CLC

I. Introduction

As more employers use monitoring technology to track employee behavior and movement in the workplace, more labor and employment practitioners are learning, and sometimes influencing, the legal principals of monitoring in the workplace and how information obtained from monitoring can and cannot be used. Technologies used for monitoring include, but are not limited to, global positioning system ("GPS") devices, cell phone metadata, social media platforms, biometrics and multiple forms of "wearable" tracking devices—from identification cards to "smart" hard hats. The authors have focused this paper on the legal implications of just two technologies (1) GPS devices and similar location tracking devices and (2) biometrics.

GPS devices rely on satellites that orbit the earth and send signals to receivers on the ground. They can provide location information for objects on a real time basis by triangulating these satellite signals.[1] GPS technology can be found in cars, cell phones and laptops. No state or federal law expressly prohibits the use of GPS technology, though limits on its use in the workplace has been, and continues to be, established through case law. While GPS devices are now commonly used by employers to monitor employees, as discussed below, the information collected through GPS and other location devices can also be used to assist with claims against employers as well as in defending those claims.

Similarly, biometrics can be used both by employers and by plaintiffs in litigation. The word biometrics can refer to both a characteristic and a process. We use the term to refer to a process, specifically automated methods of recognizing an individual based on measurable biological and behavioral characteristics.[2] Examples of these methods include fingerprint recognition, iris recognition and voice recognition. *Id.*

Below, each of the authors discusses how these technologies come up in our respective practices and the legal principles that govern their use in the workplace.

---

[1] April A. Otterberg, *GPS Tracking Technology the Case for Revisiting Knotts and Shifting the Supreme Court's Theory of Public Space Under the Fourth Amendment*, 46 B.C.L. Rev. 661, 663, 665 (2005).
[2] Nat'l Science and Technology Council, Subcomittee on Biometrics, *Biometrics Overview*, August 7, 2006, http://www.biometrics.gov/Documents/BioOverview.pdf [as of March 10, 2015]

II. The Use of Employer Monitoring by Plaintiffs in Employment Litigation

For plaintiffs bringing wage and hour claims against employers, increased employee monitoring results in discoverable information that could prove useful to plaintiffs in the litigation. For example, plaintiffs seeking unpaid wages are always in search of time-stamped data to support their claims of unpaid work. Fingerprint scans and GPS tracking can provide that information. Likewise, facial recognition software and GPS tracking can prove useful to plaintiffs facing an outside sales defense in an overtime case. Onerous employer monitoring can also be powerful evidence that a worker is under the control of the employer, and therefore properly classified as an employee instead of an independent contractor. However, this section of the paper examines two defenses in wage and hour cases which may be affected in more subtle ways by increased employer monitoring: the de minimis defense and the argument that the employer had no actual or constructive knowledge of any unpaid overtime.

A. The De Minimis Defense

Employers often invoke the de minimis defense when employees seek payment for relatively small periods of pre-shift or post-shift time. In determining whether the time at issue is de minimis, courts review "(1) the practical administrative difficulty of recording the additional time; (2) the aggregate amount of compensable time; and (3) the regularity of the additional work." *Lindow v. United States*, 738 F.2d 1057, 1063 (9th Cir.1984); see also *Rutti v. Lojack Corp., Inc.*, 596 F.3d 1046, 1056–57 (9th Cir.2010). The de minimis doctrine was first announced by the United States Supreme Court in the 1946 case of *Anderson v. Mt. Clemens Pottery Co.*, 328 U.S. 680. See 29 C.F.R. § 785.47.

The de minimis defense arises in a host of different work settings, including warehouses, call centers, meat processing plants, remote technicians or installers, and retail. See, e.g., *Cervantez v. Celestica Corp.*, 618 F.Supp.2d 1208, 1217–19 (C.D.Cal. 2009) (employees claiming unpaid wages for time spent in warehouse security screening); *Gillings v. Time Warner Cable LLC*, 583 Fed.Appx. 712 (9th Cir. 2014) (call center employees seeking pay for pre-shift time spent booting up their computers and logging into software programs); *Jones v. C & D Technologies*, Inc., 8 F.Supp.3d 1054, 1065 (S.D.Ind. 2014) (employees at battery manufacturing plant seeking pay for time spent donning and doffing safety gear), *Rutti*, 596 F.3d 1046, 1057 (repair technicians seeking pay for time spent "receiving, mapping, and prioritizing jobs and routes for assignment" prior to their shift); *Troester v. Starbucks Corp*., 2014 WL 1004098 (C.D. Cal. 2014) (shift supervisor seeking pay for time spent closing the store at the end of his shift).

Relying on the "administrative difficulty" prong of the de minimis defense, plaintiffs have increasingly argued that advances in modern technology render the defense obsolete. While the de minimis defense may have made sense in 1946, when there was little technology available for creating precise and accurate time records, technological advances allow companies to capture an employee's activities down to the fraction of a second. Some of these technologies

are not cutting-edge. For example, electronic time clocks have been accurate to the minute for years. Employees' computers and telephones record the moment an employee first accesses certain software. Offsite employees upload job-site data to a company's servers, creating an electronic record of the moment a task is complete. These technologies create problems for employers asserting the de minimis defense. See, e.g., *Jones*, 8 F.Supp.3d at 1065 (manufacturing employer who paid employees based solely on shift time was not entitled to the de minimis defense because its time keeping system was capable of tracking the time at issue); *Kasten v. Saint-Gobain Performance Plastics Corp.* 556 F.Supp.2d 941, 954 (W.D. Wis. 2008) ("[w]ith today's technology, one could argue that all time can be recorded to the minute"); *Gillings*, 583 Fed.Appx. 712 (employer denied summary judgment on the de minimis defense because it did not show it would be difficult to monitor the time its call center employees logged into their computer software prior to their shift).

Defendants have succeeded on the "administrative difficulty" prong of the de minimis defense when they have shown an inability to track the time employees spend on the tasks at issue. For example, in the *Troester* case, Starbucks argued it was unable to track the various activities the closing shift supervisor (who was classified as non-exempt) performed after clocking out of the point of sale system. The court found:

> it would be impracticable for Defendant to capture the tasks that Plaintiff performed after completing the close store procedure. He could not set the alarm prior to clocking out because the alarm became activated within one minute and would be triggered if the employees did not immediately exit the store. Similarly, the minimal time that Plaintiff spent walking out of the door, locking the door, walking co-workers to their cars, and letting co-workers back in the store necessarily occurred after he clocked out, and is not practical to record.

Troester, 2014 WL 1004098, *4. However, one can expect that increased employer monitoring would further erode the de minimis defense in wage and hour cases. Imagine, that Starbucks implemented heightened security measures at its stores, including remote video monitoring with facial recognition software. And imagine that Starbucks, concerned that closing shift supervisors were not closing on time or were lingering in the store after closing, used that remote video monitoring and facial recognition software to track and time closing managers' movements at the end of each shift. Or imagine that Starbucks installed fingerprint technology to set the store alarm and lock the doors. Suddenly, Starbucks has implemented the technology necessary to determine precisely how much time its closing shift supervisors worked after clocking out of the POS system. Armed with this knowledge and the ability to track the time, Starbucks would be ill-equipped to defend an off-the-clock case using the de minimis defense.

B. The "Knew or Should Have Known" Requirement

Similar concerns arise with respect to another common defense argument in off-the-clock cases – that the employee cannot show the employer "knew or should have known" about the overtime at issue. "[W]here an employer has no knowledge that an employee is engaging in overtime work and that employee fails to notify the employer or deliberately prevents the employer from acquiring knowledge of the overtime work, the employer's failure to pay for the overtime hours is not a violation" of the Fair Labor Standards Act. *Forrester v. Roth's I. G. A. Foodliner, Inc.*, 646 F.2d 413, 414 (9th Cir. 1981). "Knowledge may be actual or constructive, and, thus, an employer is liable for its employees' unpaid overtime work if the employer 'knew or should have known that they were working overtime.'" *Brennan v. Qwest Communications Intern., Inc.*, 727 F.Supp.2d 751, 755 (D. Minn. 2010) (quoting *Hertz v. Woodbury County, Iowa*, 566 F.3d 775, 781 (8th Cir.2009)). However, "[a]ccess to records indicating that employees were working overtime . . . is not necessarily sufficient to establish constructive knowledge." Hertz, 566 F.3d at 781–82. The FLSA's standard for constructive knowledge in the overtime context is whether the employer "should have known," not whether it could have known. *Id.* at 782 (emphasis added).

The "knew or should have known" standard can be a powerful barrier to recovery in off-the-clock cases. For example, defendants have been successful in meal period "auto-deduct" cases, especially where the employer provides a method for reversing automated meal period time deductions. See *White v. Baptist Memorial Health Care Corp.*, 699 F.3d 869, 876 (6th Cir. 2012) (nurse failed to show that employer knew or should have known that she worked through her meal periods, where she failed to use the employer's missed-meal reporting system). The mere requirement that employees accurately self-report the time may be enough for a defendant to avoid constructive knowledge, in the absence of proof the employer had reason to doubt the records. See *Forrester*, 646 F.2d at 414; *Hertz*, 566 F.3d at 782; *Newton v. City of Henderson*, 47 F.3d 746, 749 (5th Cir. 1995) ("If we were to hold that the City had constructive knowledge that Newton was working overtime because Freeman had the ability to investigate whether or not Newton was truthfully filling out the City's payroll forms, we would essentially be stating that the City did not have the right to require an employee to adhere to its procedures for claiming overtime.")

Importantly, however, "[a]n employer who is armed with . . . knowledge [of overtime worked] cannot stand idly by and allow an employee to perform overtime work without proper compensation, even if the employee does not make a claim for the overtime compensation." *Forrester*, 646 F.2d at 414. Thus, the more knowledge an employer acquires about its employees' work activities – especially as to potential off-the-clock work – the greater the employer's obligation to inquire as to the extent of the work. With increased employee monitoring, information the employer merely could have known might become information the employer should have known. "An employer is said to have constructive knowledge of its employee's overtime work when it has reason to believe that its employee is working beyond his

shift. 29 C.F.R. § 785.11. The employer's knowledge is measured in accordance with his duty . . . to inquire into the conditions prevailing in his business." *Allen v. Board of Public Educ. for Bibb County* 495 F.3d 1306, 1319 (11th Cir. 2007).

A recent case from the Middle District of Florida highlights the role employer monitoring plays in the fine line between "could have known" and "should have known." The plaintiff was a field service technician for a company that provided point of sale systems to retailers. *Frew v. Tolt Technologies Service Group*, LLC, 2010 WL 557940, at *1 (M.D. Fla., Feb. 11, 2010). The plaintiff traveled to customers' stores for service calls and to perform preventative maintenance on the employer's products. *Id*. He claimed unpaid overtime for off-the-clock service calls taken on his company cell phone, work during lunch periods, and other unrecorded hours. *Id*. at *3. In denying the defendant's motion for summary judgment, the court reasoned:

> It is undisputed that Frew was responsible for entering the hours he worked into his computer time sheet and that he did not notify Tolt directly of the hours he took service calls other than those he entered into his computer time sheet. [] However, evidence that Tolt frequently verified Frew's reported hours through his company cell phone records creates a genuine issue of material fact as to whether Tolt knew or should have known about Frew's off-the-clock service calls taken on his company cell phone. [] The frequency by which Tolt viewed Frew's cell phone records is significant. Tolt's ability to view Frew's cell phone records, without more, does not permit the inference that Tolt knew or should have known of Frew's off-the-clock service calls because an employer generally may rely upon the accuracy of an employee's self-reported work hours. [] But because there is evidence that Tolt frequently viewed Frew's company cell phone records to verify the hours he reported, it may be inferred that Tolt was actually aware or should have been aware of both over- and under-reporting of time spent working.

Frew v. Tolt Technologies Service Group, LLC, 2010 WL 557940, at *6 (M.D. Fla., Feb. 11, 2010) (internal citations omitted).

The Frew court's logic would apply to any employer monitoring its employees through GPS and other location tracking technology. The implications are especially great for employees in the field bringing off-the-clock claims. See *Brennan*, 727 F.Supp.2d 751 (defendant arguing lack of knowledge in an off-the-clock case brought by field network technicians). Seeking higher productivity and quicker customer interactions, an employer might use GPS and other technology to track employees' whereabouts throughout the day. While the employer may succeed in increasing productivity, any knowledge that employer gains through the employee monitoring may be used against it in an off-the-clock case. And, even if the employer used the technology on a limited basis and with a limited segment of its workforce, constructive knowledge could be imputed across the entire work force. If an employer monitors

its employees to increase production and reduce employee down-time, the employer should be prepared to pay for any off-the-clock work it discovers during that monitoring.

III. Employee Monitoring: Legal and Practical Considerations for Employers and Best Practices[3]

A. GPS

Some employers have experimented with GPS trackers in company vehicles, or even smart phones, to monitor their employees, leading to complaints about the intrusion into employee privacy. GPS not only monitors location, but through time and date stamps, can provide employers with information that could help employers allocate resources and track productivity. At the same time, such monitoring could become evidence of wage and hour violations and other employer compliance shortfalls.

1. Legal Issues

Few courts have addressed the issue of GPS tracking in the employment context, although, most have held that employers may use tracking devices on company-owned equipment, where the employee does not have a reasonable expectation of privacy in its use. Several states such as California, Minnesota, Tennessee, and Texas, have laws preventing the use of mobile tracking devices in order to track other individuals. Common exceptions to these laws include the consent of the owner of the device or vehicle to which a tracking device is attached.

In addition to notice and consent, employers should consider whether employees have a reasonable expectation of privacy when using the equipment on which the GPS device is to be attached or installed. A balance needs to be considered between the employee's expectation of privacy, the reasonableness of the intrusion upon that privacy (i.e., being tracked by the employer), and the employer's legitimate business purpose for utilizing the tracking device. These considerations are heightened when the device is attached to an employee's personal property or to company owned equipment that the employee uses or transports after work hours and the tracking system continues to record such after-hour usage.

Tracking employees during non-work hours can be an invasion of the employee's privacy, whether the tracking is done via employer-owned or employee-owned equipment. When the device tracks non-work time, such as during the evenings, weekends, and when the employee is on vacation, the employer may gain private information about an employee that would be considered an invasion into the employee's personal privacy. For example, an employer may find out that an employee travels each day after work to a dialysis center; that the employee has a

[3] Employer's Perspective was drafted by Nicky Jatana and Michelle T. Hackim, both attorneys with Jackson Lewis P.C. Michelle T. Hackim is an associate with the Cleveland, Ohio office of Jackson Lewis and a member of the firm's Privacy, e-Communication and Data Security practice group. Nicky Jatana is a Shareholder with the Los Angeles Office of Jackson Lewis and Co-Practice Group Leader of its Privacy, e-Communications and Data Security Practice Group.

pattern of visiting gambling facilities; the employee's travel habits; where and how often the employee shops; the amount of restroom breaks an employee takes during the day; the employee's eating habits; the employee's religious service attendance patterns or schedule; etc. Not only does obtaining and acting upon such information potentially lead to employee claims of an unreasonable invasion of privacy, it could also lead to claims of discrimination or wrongful termination based upon off-duty conduct (where such claims are permitted under state law, such as in New York.)

2. Best Practices

Information collected through GPS monitoring should be focused on an employee's job performance and disseminated only to employees who have a legitimate business reason for knowing the information. The tracking should be limited to the legitimate business purposes, conducted only during working hours, and provided the company has addressed the employee's expectation of privacy. Generally, policies should be carefully drafted to explain the legitimate business purpose, circumstances under which monitoring will take place, notice of the company's right to monitor employee actions while using Company owned property, the GPS monitoring capabilities of the Company-issued property, and that employees should not have an expectation of privacy while using the same. For employee-owned equipment, employers should have a carefully drafted Bring Your Own Device policy that provides for, among other things, employee consent for use of the tracking device on the employee's equipment, the employer's ability to access business information for legitimate reasons, and appropriate limitations on monitoring while the employee is working.

B. Biometric Methods

Employers are increasingly turning to biometrics technology ("life measurements") such as facial and voice recognition, hand and iris scans, finger and palm prints, and other forms of identification for various security and business purposes. While the use of biometrics continues to emerge in the workplace, employers should take into account the legal and practical considerations when implementing the use of this technology. Some states have already implemented laws regulating the use of biometrics, and even more are considering such legislation as businesses increase the use of biometrics.

Employees also continue to express concerns about the capture and use of their personal data. Many employees view the technology as too invasive, while others express concern about the security of their personal data. Many workers do not like the fact that biometrics can be used to track and monitor their movements and behavior as companies attempt to cut down on fraud and misconduct.

Additionally, companies using fingerprint or other biometric data devices (not just for employees but, in the case of businesses such as amusement parks, gyms and tanning salons,

requiring customer biometrics for access) have found that the technology is not perfect. Often, for various reasons, the system can be down or the scan does not work. Individuals have also learned how to hack and fake biometric data. Employers should keep these issues in mind, investigate the technology, and consider all factors when contemplating the use of a biometric system.

1. Benefits

One of the most significant benefits that biometric technology can provide to employers is a more effective method of recording the number of hours an employee has worked. With the increase in cases where employees have coworkers clock them in or out of work ("buddy punching"), or fraudulently claim or record inflated or inaccurate hours worked, employers have turned to new technology to reduce such fraud. Additionally, employers desiring to avoid potential claims of failure to properly maintain accurate records of actual hours worked and pay compensation, including overtime, need more accurate and reliable ways to determine whether an employee was actually present in the workplace at any given time.

Biometric technology also offers a solution for those employers seeking better ways to provide for security and restrict access to specific areas in the workplace, and understand which individuals were present in specific locations at any given time. With improvements in technology providing secure "keyless" locks based on biometric data from individuals authorized to access a facility, employers can now track access and activity in other ways with more accuracy.

2. Security, Privacy and Related Issues When Using Biometrics

While biometric technology can enable employers to keep records of their employees' time more accurately, and increase security at their facilities, employees often express fears that their data could be compromised, stolen or misused. However, depending on the technology that is being used, most of these issues are speculative. Once the technology is properly explained and understood, in most cases employees will find that what is stored is only a comparison "model" from which their actual individual characteristics cannot be reproduced. Nevertheless, employers should be mindful of whether the specific biometric system used can be hacked or otherwise compromised.

Another issue that employers can face when implementing biometric technology is the refusal of their employees to allow the scanning, recording or collecting of the biometric data out of fear for the possible misuse of this data. Employees may also object to this technology because they view it as the ultimate invasion of their privacy. This then raises the question of how the employer should handle the situation.

The employment-at-will doctrine allows employers to terminate employment for any lawful reason (whether positive or negative). Absent legislation providing that an employee

cannot be fired for refusing to provide a fingerprint, iris scan, or other biometric data, an employer would certainly have the right to terminate the employment of any individual who refuses to provide their data for legitimate business reasons. But from an employee relations standpoint, an employer should carefully consider all facts before deciding how to deal with employees who refuse to provide biometric data.

This is even more important considering the recent trend by states to pass legislation aimed at addressing employers' invasion of employee privacy. For example, laws have recently been passed in response to the use of social security numbers by employers for identification badges or computer access purposes. Many states also now have laws imposing liability on employers who do not properly maintain the security and integrity of systems and processes containing employee personal information. Additionally, several states have enacted legislation prohibiting employers from collecting social media passwords and other such information from employees and applicants.

Finally, it is important to note that other countries, including Canada, require employers who use biometric data to ensure privacy. In the United States, Illinois and Texas are among the states with laws regulating the collection and use of biometric data, and New York has a law prohibiting employers from fingerprinting employees unless required by law. Legislative developments in this area will undoubtedly progress as employees seek ways to limit employer collection and use of biometric data.

3. Best Practices

In light of the foregoing, employers should consider the following best practices before implementing the use of biometric technology in the workplace:

1. Notify all employees, in writing, of the company's intent to use a biometric system–include the reasons, what safeguards will be provided, and what an employee should do if they have any questions or concerns about the system.

2. Check applicable privacy and other potentially relevant laws before implementing the system (laws in this area can quickly change, as can the interpretation of existing laws).

3. Implement strict security policies and procedures that will ensure all biometric data will be securely stored and safeguarded.

4. If your company is unionized, give the union sufficient notice of your intention to implement the system and verify your right under any collective bargaining agreements to implement such a system.

5. Be ready to consider accommodation or other requests from employees who may raise issues based on disability, religious beliefs, or other areas protected by law.

VI. Employer Monitoring and its Limits in the Union Context

As the use of GPS and biometric technology has slowly increased over the past two decades, employers, Unions, administrative agencies, courts and arbitrators have had to wrestle with the extent to which the introduction of this technology must be bargained, how it can and cannot be used and whether the data it creates is reliable. A review of the administrative and arbitral decisions that address these issues reveal several points worth noting: (1) there continue to be concerns about the reliability of data derived from both GPS and biometric devices and corroborating evidence may be required where this data is used to place an employee at a particular place and time; (2) failure to give employees and/or unions prior notice of the implementation of either technology can lead to the exclusion of the information derived thereby as evidence; (3) if the use of either technology is non-routine and "out of the ordinary," there is a greater chance it will be deemed "unlawful surveillance." Based on all of the above, wise employers will notify unions of their intent to implement either GPS or biometric technology in the workplace and bargain regarding the limits on the use of data derived thereby, storage of that data and privacy protections.[4]

A. GPS Technology

For Unions, the use of GPS technology by employers arises both in the context of employee surveillance and in the context of an employer's obligation to bargain with a union over mandatory subjects of bargaining. The National Labor Relations Board has, via advice memoranda and Regional Director dismissals, addressed both surveillance and the employer's duty to bargain vis a vis GPS technology, though not at any length.

1. Employer Surveillance

The right of employees to engage in concerted activity comes from the National Labor Relations Act, 29 U.S.C. section 158(a)(1), which protects employees from interference with, restraint, or coercion in the exercise of rights guaranteed by Section 7 of the Act. Section 7 provides that:

> Employees shall have the right to self-organization, to form, join or assist labor organizations, to bargain collectively through representatives of their own choosing, and to engage in other concerted activities for the purpose of collective bargaining or

[4] This section of the paper does not address the law regarding employee privacy in the workplace, but unions and employers must be aware that potential privacy claims exist and should consider this when implementing new monitoring technology. For an extensive discussion on privacy protections in the workplace see William A. Herbert & Amelia K. Tuminaro, *The Impact of Emerging Technologies in the Workplace: Who's Watching the Man (Who's Watching Me)?* (2009) Hofstra Labor & Employment L.J., Vol. 25:355.

> other mutual aid or protections, and shall also have the right to refrain from any or all such activities except to the extent that such right might be affected by an agreement requiring membership in labor organization as a condition of employment as authorized in § 158(a)(3) of this title.

Under Board law, the "routine observation of employees engaged in open § 7 activity on company property does not constitute unlawful surveillance" but "an employer violates § 8(a)(1) when it surveils employees engaged in § 7 activity by observing them in a way that is 'out of the ordinary' and therefore coercive." *Aladdin Gaming, LLC*, 345 NLRB 585-86 (2005), *petition for review denied*, 515 F.3d 942 (9th Cir. 2008). No Board cases have discussed the use of GPS in this regard to date.

However, in an Advice Memorandum, the General Counsel agreed with Region 22 of the Board that an employer "interfered directly with employees' Section 7" rights when it installed GPS tracking units in the trucks of two employees during a union organizing campaign. *East Coast Mechanical Contractors*, 22-CA-25324, 2003 WL 26072140 (N.L.R.B.G.C. 2003). The employer in *East Coast Mechancial Contractors* installed GPS units in only 2 of 8 company trucks. The 2 trucks with GPS units were driven by the only two employees with any union affiliation. The employer attempted to explain its decision to track only 2 vehicles but the Division of Advice found the employer lacked a "legitimate business concern":

> It is well established that increased employer surveillance of employees does not violate the Act if instituted for, and justified by, legitimate employer concerns, even where such increased surveillance occurs during a union organizing drive. In contrast, where such increased surveillance, or the impression of increased surveillance, is not justified by legitimate business concerns and company officials "do something out of the ordinary" by increasing surveillance of employees during an organizing drive, the employer violates section 8(a)(1).

Id. (Citations omitted.)

Because this Advice Memorandum is in line with prior Board case law regarding employee surveillance, it seems likely that any Board case addressing the use of GPS technology by employers will also look to whether the employer did "something out of the ordinary" when determining whether there was a violation of Section 7 rights. If the surveillance is not justified by legitimate employer concerns and is "out of the ordinary," there is a good chance it will be found unlawful.

2. The Duty to Bargain Under the NLRA

Whether an employer is required to bargain prior to installing GPS technology has not yet been decided by the NLRB.[5] However, the Act imposes a general duty to bargain with a bargaining representative regarding wages, hours and other terms and conditions whenever there is a "material, substantial and [] significant change." See *NLRB v. Katz*, 369 U.S. 736 (1962), *Litton Financial Printing Division v. NLRB*, 501 U.S. 190, 198 (1991), *Rust Craft Broadcasting of New York*, 225 NLRB 327 (1976) (finding change from manual to mechanical procedure for timekeeping was not a "material, substantial and []significant change.). And, the General Counsel's Division of Advice has addressed the issue of GPS devices and the duty to bargain in two Advice Memoranda.

In *BP Exploration of Alaska, Inc.*, the employer, without bargaining with the union, began installing vehicle data recorders or "VDRs", which utilized GPS technology, for the purpose of monitoring employee compliance with its driving safety rules. *BP Exploration of Alaska, Inc.*, 19-CA-29566, available at http://www.nlrb.gov/case/19-CA-029566. According to the General Counsel, the use of the VDRs was a mandatory subject and installation of the system "significantly affected terms and conditions of employment." *Id*. Prior to installation of the VDRs, employee driving had been monitored by two security guards "a very small percentage of the time they were driving." *Id.*

However, where an employer switched from a two-way radio system for monitoring truck drivers' work to GPS technology, the General Counsel found no violation of the Act. *Roadway Express, Inc.*, 13-CA-39940-1, 2002 WL 34680591(N.L.R.B.G.C. 2002). Because the type of information collected by the employer remained unchanged, the General Counsel found it did not result in a "significant and substantial change in employees' terms and conditions of employment" or in a "unilateral change[] in the degree of surveillance employees experienced." *Id*.

Based on these Advice Memoranda it seems probable that any future Board decision addressing the introduction of GPS technology in a unionized workplace will look to whether it results in a material, substantial and significant change in the conditions of employment. In a workplace where there has been little or no surveillance of employee movement, such a finding – and an accompanying duty to bargain – seems likely.

3. Arbitration Decisions

There are not enough arbitration decisions to date, to suggest whether an arbitrator will uphold discipline where employees' on duty behavior is discovered via surreptitious GPS

[5] Despite the lack of a definitive Board ruling that requires bargaining prior to implementing GPS technology, various employers and unions have bargained on this topic and reached agreements. See William A. Herbert & Amelia K. Tuminaro, *The Impact of Emerging Technologies in the Workplace: Who's Watching the Man (Who's Watching Me)?* (2009) Hofstra Labor & Employment L.J., Vol. 25:355, 377-378.

monitoring. However, the issue has been addressed. In *Beverage Mktg. Inc.*, an employee was terminated "for going home without permission on repeated occasions." *Beverage Mktg. Inc.*, 120 Lab. Arb. Rep. (BNA) 1388 (Fagan, Arb.), 2005 WL 6714466. The employer installed GPS technology in the employee's company vehicle without notice because it suspected he was spending time at home rather than on the road or at work locations. *Id*. The Arbitrator reduced the discipline to a sixty day suspension at least in part because the employer did not give employees notice that the GPS systems had been installed. *Id*.

A different outcome resulted where there was evidence that the Union may have known that GPS technology was installed on company vehicles, but there was no evidence of individual notice to employees. (Dixon, Arb.), 2013 WL 3974457 (AAA).[6] In that case, the arbitrator upheld a termination for time card falsification based on GPS data showing the employee was home for several hours during hours reported as work time on his time cards. *Id.*

B. Biometrics

1. The Duty to Bargain Under the NLRA

While no Board case has addressed employers' duty to bargain over the introduction of biometrics in the workplace, the Board has issued decisions regarding the duty to bargain over new and different time keeping systems. And, two NLRB administrative law judge decisions address the duty to bargain when a fingerprint based time keeping system is implemented. These decisions seem to suggest that an employer need not bargain with a union when the new fingerprint based time keeping system simply replaces a less technologically advanced but similar time keeping system.

In *Rust Craft Broadcasting of New York*, 225 NLRB 327 (1976), the Board found that the change from a manual to mechanical procedure (timeclocks) for timekeeping was not material, substantial or significant and did not have to be bargained over because the basic rule, that employees had to record their times of arrival and departure, remained the same.

But the Board reached a different outcome, in *Nathan Littauer Hospital Assn*., 229 NLRB 1122, (1977), where it held the employer unlawfully unilaterally implemented a requirement that nurses record their regular time using a timeclock where there had been no prior requirement to record time, by any means. The Board also found a duty to bargain and an unlawful change where the employer changed from the use of timeclocks to a system where supervisors recorded the employees' time on forms and employees' signed off on the forms each week. *Vincent Industrial Plastics, Inc.*, 328 NLRB 300 (1999), *aff'd in part, rev'd and remanded in part*, 209 F.3d 727 (D.C. Cir. 2000).

[6] Party names omitted in Westlaw.

The administrative law judge ("ALJ") in *South Bronx Job Corps Center*, 2-CA-32700, 2001 WL 1598700 (N.L.R.B. Div. of Judges, June 8, 2001), cited *Rust Craft, supra*, 225 NLRB 327, to support his finding that the employer's change from one method of timekeeping – paper time sheets – to a different method of timekeeping – finger print scans – was not significant and did not violate the duty to bargain. The ALJ rejected the Union's argument that the "biometric system [wa]s extremely invasive because it g[ave] the [employer] full access to employees' fingerprints" which could be used in workplace or criminal investigations. *Id.* According to the ALJ, there was insufficient evidence to show the biometric system recorded the fingerprints in such a way that they could be accessed for use in conducting investigations. *Id.*

Conversely, in *Spartan College of Aeronautics and Technology*, 17-CA-24965, 2011 WL 2412622 (N.L.R.B. Div. of Judges, June 9, 2011), the ALJ distinguishes *Rust Craft, supra*, 225 NLRB 327, because implementation of the new biometric "hand-scan" timeclock was "more than a unilateral initiation of a more modern method of obtaining employees' time in and out." Prior to the hand-scan timeclock there was no requirement that employees record their time at all. *Id.*

2. The Duty to Bargain under the RLA

Though most of the case law regarding GPS devices and the duty to bargain arises under the NLRA, at least one court has addressed the issue in the context of a request for injunctive relief under the Railway Labor Act ("RLA"). *Brotherhood of Maintenance of Way Employees Div. of Intl. Brotherhood of Teamsters v. Union Pacific Railroad*, (N.D. Iowa 2007) 475 F.Supp.2d 819, 181 L.R.R.M. (BNA) 2639. The employer in that case planned to implement iris recognition technology to record the attendance of employees without bargaining with the union. The union claimed the issue was a "major dispute" under the RLA, and unsuccessfully sought to enjoin the implementation. *Id.* at 837 (citations omitted.) The federal court found the implementation of iris recognition technology was not a "major dispute," which seeks to create a contractual right, and was instead a "minor dispute," which concerns enforcement of existing contractual rights. *Id.* Because there was language in the parties' collective bargaining agreement that authorized the employer to make changes in work methods, and because the employer had in the past implemented changes in timekeeping, the issue was a "minor dispute" and the court held it lacked subject matter jurisdiction. *Id.* at 843.

3. Arbitration Decisions

To date, there are very few decisions that address the use of biometric data in just cause arbitrations. The two cases cited herein reflect two different views on the reliability of biometric time and attendance data as evidence in arbitration. In *Commonwealth of Pennsylvania*, (D'Eletto, Arb.) 2010 WL 8435395 (AAA), the arbitrator found there was no just cause for a 1 day suspension issued for alleged attendance infractions, one of which was substantiated only through a biometrics report. According to the report, the grievant was four minutes late on a

particular date. *Id.* The arbitrator rejected the biometrics report where there was no corroborating evidence that the grievant was late. The arbitrator found that "[r]eliance upon a biometric report or by an identification card swipe is not convincing evidence because such systems malfunction." *Id*.

In *Bridgeport Health Care Manor*, (Diaz, Arb.) 2011 WL 4537211, the arbitrator came to a different conclusion about the value of biometric evidence and upheld the termination of a nursing assistant based at least in part on that evidence. The nursing assistant was assigned to a unit she did not wish to work in and according to her finger print scan in and out of the unit, she spent just 26 minutes with two patients -- a purportedly insufficient amount of time. *Id*. Though the nursing assistant thought she had spent longer with the patients, the arbitrator found the biometric evidence "showed unmistaken and uncontroverted evidence that she clocked in at 7:04 a.m. and then that she punched out at 7:30 a.m." *Id*.

Given the newness of biometric data and the apparent lack of agreement on its usefulness to prove a person's whereabouts, it seems likely arbitrators will want to see corroborating evidence in discipline cases.[7]

[7] For a discussion of reliability issues with respect to biometric data, see Duncan, *Why Haven't Biometrics Replaced Passwords Yet?* (March 9, 2013) < http://www.digitaltrends.com/computing/can-biometrics-secure-our-digital-lives/> [as of March 3, 2015].