GPS AND CELL PHONE TRACKING OF EMPLOYEES

Marc Chase McAllister[*]

Abstract

This Article examines employee location tracking through smart phone apps and GPS devices attached to or embedded within an employee's personal or company vehicle. For each form of tracking, this Article provides separate frameworks for employers to follow when conducting individual employee misconduct investigations and when tracking an entire group of employees for non-investigatory purposes. Beginning with GPS tracking for individual misconduct investigations, this Article contends that such tracking should be used only as a means to corroborate evidence that an employee has committed a terminable offense, that an employer may resort to this technique only after alternative investigative methods fail to generate enough evidence to warrant disciplinary action, and that the tracking must cease once the alleged wrongdoing has been corroborated. Turning to non-investigatory forms of GPS tracking, such as the monitoring of an employer's entire fleet of taxi-cab or rideshare drivers, this Article proposes that such tracking should be performed only for legitimate business purposes and only if employees consent to the tracking in advance. Whether performed for investigatory or non-investigatory purposes, this Article further proposes that employers should avoid collecting GPS tracking data while employees are off-duty. Finally, this Article addresses employee tracking through smart phone apps, including employer-owned apps and apps designed for time-keeping purposes. Because employees who use such apps typically consent to the monitoring of their phone's location, this Article concludes that employees tracked in this manner cannot reasonably expect privacy in such monitoring. As a result, this Article predicts that app-based employee tracking will not trigger Fourth Amendment protection, nor will it be sufficient to sustain a privacy-related tort claim, such that employers will typically not face civil liability for tracking employees through smart phone apps.

* Marc McAllister is an Assistant Professor of Business Law in the Department of Finance and Economics at Texas State University. His articles have been published in prestigious journals such as the *Boston College Law Review* (forthcoming), *Alabama Law Review* (forthcoming), *Washington and Lee Law Review*, and *George Mason Law Review*.

INTRODUCTION

This Article examines modern forms of location tracking by employers, including the tracking of employees through GPS devices and smartphone apps.

The starting point to this Article's analysis is the established law governing GPS tracking by law enforcement. In that context, the United States Supreme Court recently ruled that the Fourth Amendment applies when police attach a GPS tracking device to a criminal suspect's vehicle and use the device to monitor the vehicle's movements.[1] In effect, this ruling established that when GPS tracking is conducted as part of a criminal investigation, the procedure must be authorized by a warrant or warrant exception.[2]

Like law enforcement officials, public employers must abide by the Fourth Amendment,[3] and private employers may be liable in tort for invading an employee's reasonable expectation of privacy, a concept borrowed from Fourth Amendment jurisprudence.[4] Yet the Fourth Amendment framework that governs employers differs somewhat from

1. United States v. Jones, 565 U.S. 400, 404 (2012).

2. Katz v. United States, 389 U.S. 347, 357 (1967) ("'Over and again this Court has emphasized that' . . . searches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions." (footnote omitted) (quoting United States v. Jeffers, 342 U.S. 48, 51 (1951))).

3. *See* O'Connor v. Ortega, 480 U.S. 709, 725 (1987).

4. *See infra* notes 102–04 and accompanying text.

that which governs law enforcement. In the employment context, employee investigations must generally be both reasonable at the inception and reasonable in scope,[5] which is the usual framework for cases that fall outside the criminal investigation context.[6]

Applying Fourth Amendment law as it pertains to employers, this Article considers both GPS tracking for purposes of investigating individual employee misconduct via a surreptitiously installed tracking device, and GPS tracking of an entire segment of employees via GPS devices that have been preinstalled in employer-owned vehicles.

Regarding individual misconduct investigations, this Article proposes that an employer may track an employee through a GPS device installed on the employee's personal or employer-owned vehicle only in very narrow circumstances. In particular, this Article proposes that this procedure be used only when the employer has reason to believe such tracking would corroborate evidence that an employee has committed a terminable offense, and only after alternative methods of investigation fail to generate enough evidence of wrongdoing to warrant disciplinary action. This Article further proposes that in these narrow circumstances, an employer should avoid collecting data as to purely private activity, unconnected to work obligations or alleged workplace misconduct, and may only track an employee's vehicle long enough to obtain the information it needs to corroborate a suspicion of wrongdoing. If GPS tracking continues beyond this point, the employer risks having any disciplinary action it takes against the employee overturned in court and may also risk civil liability for unduly invading the employee's privacy. Employing a corroboration framework similar to that of *Illinois v. Gates*[7] and *Alabama v. White*,[8] this Article thus presents a clear set of guidelines for investigating workplace misconduct by GPS, one that will allow employers to use this investigative technique in a reasonable manner while simultaneously respecting the rights of employees to be free from overly intrusive investigations into their private affairs.

Next, this Article considers GPS tracking for noninvestigatory work-related purposes.[9] Drawing upon a recent New York case,[10] this Article

5. *See O'Connor*, 480 U.S. at 725–26.

6. *See* New Jersey v. T.L.O., 469 U.S. 325, 341 (1985). *See generally* United States v. Kincade, 379 F.3d 813, 823–24 (9th Cir. 2004) (summarizing "special needs" cases, including those where the doctrine was deemed not to apply).

7. 462 U.S. 213 (1983).

8. 496 U.S. 325 (1990).

9. *See O'Connor*, 480 U.S. at 723 (adopting a framework for analyzing searches performed for "either a noninvestigatory work-related" purpose or to investigate "suspected work-related employee misfeasance").

10. Carniol v. N.Y.C. Taxi & Limousine Comm'n, 975 N.Y.S.2d 842, 849 (N.Y. Sup. Ct. 2013), *aff'd*, 2 N.Y.S.3d 337 (N.Y. App. Div. 2015).

proposes that wholesale GPS tracking of an entire segment of employees, such as a group of taxi-cab or Uber drivers, should be performed only for legitimate business purposes and only if employees consent to such monitoring in advance. This Article further proposes that to remain reasonable in scope, employers should avoid collecting GPS data while its employees are off duty.[11]

Finally, this Article addresses location tracking by employers through smartphone apps, including apps designed for employee timekeeping purposes. Because employees who use such apps typically consent to the monitoring of their phone's location and voluntarily convey evidence of their location to their employers, this Article concludes that this form of location tracking is simply not a Fourth Amendment "search," either under the physical trespass test or under the *Katz* test, such that it is generally not an invasion of privacy. As a result, this Article predicts that employer use of such apps will grow exponentially in the coming years given the more relaxed privacy laws—flowing from the Fourth Amendment concepts of consent and assumption of risk—that govern this form of location tracking.[12]

Part I of this Article summarizes the general privacy rights of both public and private employees. Part II examines the law governing GPS tracking by law enforcement and how it impacts the emerging law of GPS tracking by employers, an issue addressed in Part III. Finally, Part IV examines the tracking of an employee's movements via GPS-enabled smartphone.

I. EMPLOYEE PRIVACY PROTECTIONS

American workers, whether employed by public or private employers, are entitled to privacy protections in the workplace.[13] Along with the protections afforded by various statutes, employees may be protected

11. *See infra* notes 292–318 and accompanying text.

12. *See generally* Cunningham v. N.Y. State Dep't of Labor, 997 N.E.2d 468, 477 (N.Y. 2013) (Abdus-Salaam, J., concurring) ("Given the majority's imprimatur of warrantless GPS tracking, less intrusive methods for investigating government employees will almost certainly be replaced with electronic surveillance."); David K. Isom, *Location Based Electronic Discovery in Criminal and Civil Litigation - Part 1*, UTAH B.J. 28, 32 (2011) ("With hundreds of thousands of apps now available, and thousands of geo-apps, and more on the way, apps-engendered location metadata will continue to increase in volume and importance."); Scott McCartney, *A New Level of Security on Your Business Trip*, WALL ST. J. (May 30, 2018, 9:11 A.M.), https://www.wsj.com/articles/a-new-level-of-security-on-your-business-trip-1527685866 [https://perma.cc/C9RH-D23L] (reporting that U.S. companies are tracking employees through their smartphones much more frequently than in the past).

13. *See O'Connor*, 480 U.S. at 715 (establishing that employees of public employers enjoy Fourth Amendment protections in the workplace).

from employer intrusions by constitutional provisions and tort law.[14] Because the rules governing public and private employers differ in some respects, one must first determine the type of employer at issue in a given case to properly analyze a workplace privacy claim. This section summarizes the usual privacy claims brought against both types of employers.

A. *Employees of Public Employers*

When an employee of a public employer believes her privacy rights have been violated, she will generally sue her employer under 42 U.S.C. § 1983, alleging a violation of her constitutional right to be free from "unreasonable searches and seizures" under the Fourth Amendment.[15]

Although the Fourth Amendment is often applied to law enforcement in the context of criminal investigations, the Supreme Court has applied the Fourth Amendment to other types of government officials, including public school officials,[16] building inspectors,[17] and health and safety inspectors.[18] However, because such actors are usually not engaged in criminal investigations, their actions are judged according to a general "reasonableness" standard; the criminal law standard, by contrast, involves a more specific reasonableness analysis of whether the police should have obtained a warrant or acted pursuant to some warrant exception.[19] Searches and investigations by public employers are likewise subject to the general reasonableness approach, such that a public employer's workspace intrusion is judged by the reasonableness of the employer's actions under the circumstances of each case.[20]

To fully comprehend the law with respect to employee tracking, it is necessary to understand the broader contours of Fourth Amendment analysis. Generally speaking, the Fourth Amendment prohibits "unreasonable searches and seizures" by government officials.[21] At its

14. *See infra* notes 101–08 (discussing various privacy-related torts and statutes).

15. U.S. CONST. amend. IV; *see, e.g.*, *O'Connor*, 480 U.S. at 714 (noting that the plaintiff in the case, Dr. Ortega, brought suit against his employer under 42 U.S.C. § 1983, "alleging that the search of his office violated the Fourth Amendment"); *see also* West v. Atkins, 487 U.S. 42, 48 (1988) ("To state a claim under § 1983, a plaintiff must allege the violation of a right secured by the Constitution and laws of the United States, and must show that the alleged deprivation was committed by a person acting under color of state law.").

16. *See* New Jersey v. T.L.O., 469 U.S. 325, 334 (1985).

17. *See* Camara v. Mun. Court, 387 U.S. 523, 528, 540 (1967).

18. *See* Marshall v. Barlow's, Inc., 436 U.S. 307, 312–13, 324 (1978).

19. *See T.L.O.*, 469 U.S. at 341.

20. *See O'Connor*, 480 U.S. at 718.

21. U.S. CONST. amend. IV; *see also* Pennsylvania v. Mimms, 434 U.S. 106, 108–09 (1977) ("The touchstone of our analysis under the Fourth Amendment is always 'the reasonableness in

most basic level, there are three steps to Fourth Amendment analysis. In the first step, courts consider the threshold question of whether a "search"[22] or "seizure"[23] has occurred, without which the Fourth Amendment does not apply.[24] To determine whether a Fourth Amendment search has occurred, courts generally employ the "reasonable expectation of privacy" test derived from *Katz v. United States*.[25] Under the *Katz* test, a search occurs only when the government violates a person's expectation of privacy that society recognizes as legitimate or reasonable.[26] Under this test, the reasonableness of any asserted expectation of privacy is context-specific,[27] and will depend on various factors, such as the intrusiveness of an investigative technique,[28]

---

all the circumstances of the particular governmental invasion of a citizen's personal security.'" (quoting Terry v. Ohio, 392 U.S. 1, 19 (1968))).

22. The term "search" is a legal term of art distinct from its ordinary dictionary definition. *See* Kyllo v. United States, 533 U.S. 27, 32 n.1 (2001) (contrasting the Fourth Amendment definition of "search" with the dictionary definition of "search"). Indeed, many routine forms of police surveillance are not considered Fourth Amendment "searches," such as a dog sniff at an airport, even where the obvious purpose of the activity is to uncover evidence of a crime. *See* United States v. Place, 462 U.S. 696, 707 (1983).

23. Fourth Amendment claims may involve seizures of persons and seizures of property. Under Fourth Amendment precedent, "[a] 'seizure' of property occurs when there is some meaningful interference with an individual's possessory interests in that property." United States v. Jacobsen, 466 U.S. 109, 113 (1984). Seizures of persons include both investigative detentions of limited scope and duration, which must be supported by a reasonable suspicion of criminal activity as well as arrests, which are more intrusive than investigative detentions and therefore require the existence of probable cause to be reasonable. United States v. Davis, 94 F.3d 1465, 1467–68 (10th Cir. 1996).

24. *See* 19 WILLIAM A. KNOX, MISSOURI PRACTICE SERIES: CRIMINAL PRACTICE AND PROCEDURE § 4:1 (3d ed. 2017) ("If no 'search' or 'seizure' takes place, then the Fourth Amendment inquiry may be terminated because when there is no search or seizure, there is no need to obtain a warrant or even to consider whether the search or seizure was 'reasonable.'").

25. 389 U.S. 347, 360 (1967) (Harlan, J., concurring).

26. *Id.* at 360–61 ("[T]here is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"); *see also Kyllo*, 533 U.S. at 32–33 (discussing this framework); United States v. Simons, 206 F.3d 392, 398 (4th Cir. 2000) (speaking in terms of a "legitimate expectation of privacy," or "one that society is prepared to accept as objectively reasonable").

27. *See* O'Connor v. Ortega, 480 U.S. 709, 715 (1987) ("[T]he reasonableness of an expectation of privacy, as well as the appropriate standard for a search, is understood to differ according to context."). *Compare* Leventhal v. Knapek, 266 F.3d 64, 73 (2d Cir. 2001) (finding, based on the particular facts of the case, that employee had a reasonable expectation of privacy in the contents of his office computer), *with* United States v. Barrows, 481 F.3d 1246, 1248–49 (10th Cir. 2007) (finding employee had no reasonable expectation of privacy in the contents of a personal computer he "voluntarily transferred . . . to a public place for work-related use").

28. A custodial arrest, for example, requires a greater degree of suspicion to be reasonable than does a suspect's brief, noncustodial detention. *Compare* New York v. Harris, 495 U.S. 14, 18 (1990) (noting the "long . . . settled" rule that "a warrantless arrest in a public place [is]

the suspect's status,[29] the location of the search,[30] and the precise manner of investigation—including whether sophisticated technology was employed.[31] In the employment context, expectations of privacy also largely depend on whether an employee has been notified of, and has consented to, the monitoring at issue.[32] Courts also consider the

---

permissible as long as the arresting officer had probable cause"), *with* Terry v. Ohio, 392 U.S. 1, 20–22 (1968) (authorizing a brief, temporary seizure of a person suspected of committing a crime on the basis of reasonable suspicion rather than probable cause). Likewise, a strip search requires a greater degree of suspicion than a search of a person's backpack or outer clothing. *See* Safford Unified Sch. Dist. No. 1 v. Redding, 557 U.S. 364, 373–77 (2009) (permitting search of a teenage girl's backpack and outer clothing but striking down a search of her underwear and bra which was a "quantum leap from outer clothes and backpacks").

29. For example, K–12 students and arrestees enjoy less Fourth Amendment protection than ordinary adult citizens. As one specific example, adult citizens enjoy full Fourth Amendment protection in their closed containers, which require either a warrant or an applicable warrant exception to search. United States v. Chadwick, 433 U.S. 1, 15–16 (1977), *abrogated by* California v. Acevedo, 500 U.S. 565 (1991). In the K–12 context, however, warrantless searches of lockers, purses, backpacks, cars, and clothing have all been upheld as reasonable based on a mere "reasonable suspicion" that the student violated either the law or school rules. *See* Bernard James, T.L.O. *and Cell Phones: Student Privacy and Smart Devices After* Riley v. California, 101 IOWA L. REV. 343, 350–51 (2015).

30. For example, the Supreme Court has ruled that dog sniffs do not constitute Fourth Amendment "searches," given that the asserted expectation of privacy is unreasonable when the dog sniff occurs in the airport (involving a passenger's luggage), or on a public road (where a dog is employed to sniff around a car). Illinois v. Caballes, 543 U.S. 405, 410 (2005); United States v. Place, 462 U.S. 696, 707 (1983). On the other hand, the Court ruled in 2013 that police deployment of a drug-sniffing dog on the front porch of a home was a "search" for Fourth Amendment purposes. Florida v. Jardines, 569 U.S. 1, 11–12 (2013).

31. For example, a suspect's location may typically be determined, without judicial approval, via cell tower records, but may not be obtained without a warrant through a GPS device that police attach to the same suspect's vehicle. *See* Marc McAllister, *GPS and Cell Phone Tracking: A Constitutional and Empirical Analysis*, 82 U. CIN. L. REV. 207, 221–29 (2013) (comparing cases); *see also Kyllo*, 533 U.S. at 34–36 (striking down warrantless police use of a thermal imaging device to scan the outside of a suspect's home, and recognizing that searches conducted via sophisticated technologies are fundamentally distinct from those that are not); United States v. Jones, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring) ("I do not regard as dispositive the fact that the government might obtain the fruits of GPS monitoring through lawful conventional surveillance techniques.").

32. *See* United States v. Simons, 206 F.3d 392, 398 (4th Cir. 2000) ("Government employees may have a legitimate expectation of privacy in their offices . . . . However, office practices, procedures, or regulations may reduce legitimate privacy expectations."); *id.* (on the merits, finding that search of employee's computer did not violate his Fourth Amendment rights because company's Internet policy allowed it to "'audit, inspect, and/or monitor' employees' use of the Internet, including all file transfers, all websites visited, and all e-mail messages," such that the employee could not reasonably expect privacy in files downloaded from the Internet); *see also* United States v. Yudong Zhu, 23 F. Supp. 3d 234, 240–42 (S.D.N.Y. 2014) (upholding computer search over Fourth Amendment challenge in part because employee gave written consent to inspection when he began his employment); United States v. Hamilton, 778 F. Supp. 2d 651, 654 (E.D. Va. 2011) (finding public school employee could not reasonably expect privacy in e-mails

ownership of the property subject to intrusion, as employees generally enjoy fewer expectations of privacy in property owned by their employers, particularly where an employer policy authorizes searches and inspections of the property.[33]

In deciding whether a Fourth Amendment search has occurred, courts alternatively apply the physical trespass-based test,[34] which became more prominent in search analysis as a result of the United States Supreme Court's 2012 decision in *United States v. Jones*.[35] Under this test, courts consider whether the government "obtain[ed] information by physically intruding" on a person, house, paper, or effect,[36] in which case a Fourth Amendment search occurred, regardless of whether it would be reasonable to expect privacy in the case.[37] In *Jones*, the Court held that a Fourth Amendment search occurred when police obtained location information by trespassorily attaching a GPS tracking device to a criminal suspect's vehicle, an "effect" under the Fourth Amendment, and using that device to monitor the vehicle's movements.[38] As a result, the *Jones*

---

with his wife that were stored on his work computer because he was on notice that contents of his computer were subject to inspection, which he acknowledged); Hill v. Nat'l Collegiate Athletic Ass'n, 865 P.2d 633, 655 (Cal. 1994) ("[T]he presence or absence of opportunities to consent voluntarily to activities impacting privacy interests obviously affects the expectations of the participant.").

33. *See, e.g.*, *Simons*, 206 F.3d at 398; *Hamilton*, 778 F. Supp. 2d at 654; *cf.* Riley v. California, 134 S. Ct. 2473, 2488–91 (2014) (examining the substantial privacy rights in modern cell phones, and declaring that "a cell phone search would typically expose to the government far *more* than the most exhaustive search of a house" because a phone contains not only "many sensitive records previously found in the home," but also "a broad array of private information never found in a home in any form").

34. *See* Free Speech Coal., Inc. v. Attorney Gen. of U.S., 677 F.3d 519, 543 (3d Cir. 2012) ("There are two ways in which the government's conduct may constitute a 'search' implicating the Fourth Amendment.").

35. 565 U.S. 400, 405–06 (2012); *see also* United States v. Cowan, 674 F.3d 947, 955 (8th Cir. 2012) ("An individual may challenge a search under the Fourth Amendment if it violates the individual's 'reasonable expectation of privacy,' or involves an unreasonable 'physical intrusion of a constitutionally protected area.'" (citations omitted) (quoting *Jones*, 565 U.S. at 414)); United States v. Johnson, 871 F. Supp. 2d 539, 546 (W.D. La. 2012) ("*Jones* established, or perhaps reiterated, that there are two ways to analyze [whether a Fourth Amendment 'search' has occurred]: a traditional common-law property rights test and the *Katz*/reasonable-expectation-of-privacy test.").

36. *See* U.S. CONST. amend. IV (establishing, in pertinent part, "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures").

37. Florida v. Jardines, 569 U.S. 1, 5 (2013) (quoting *Jones*, 565 U.S. at 406–07 n.3).

38. *Jones*, 565 U.S. at 404 ("We hold that the Government's installation of a GPS device on a target's vehicle, and its use of that device to monitor the vehicle's movements, constitutes a 'search.'" (footnote omitted)).

majority did not consider whether a search would have occurred under the alternative reasonable expectation of privacy test.[39]

Once a court determines that a Fourth Amendment search or seizure has occurred in a given case, the court must then determine whether the government's conduct was "reasonable."[40] In the context of criminal investigations, a warrant or some warrant exception is generally required for a search or seizure to be reasonable.[41] In addition searches or seizures ordinarily require a finding of probable cause, whether before the search, in the case of warrants, or afterwards, in the case of many of the numerous search warrant exceptions.[42]

Outside the criminal context, courts determine whether a particular search was reasonable by balancing the government's interests against the plaintiff's interests to arrive at a framework for assessing reasonableness, then applying that framework to the case at hand.[43] As

---

39. *See id.* at 406.

40. *See, e.g.*, Katz v. United States, 389 U.S. 347, 353–54 (1967) (turning to "[t]he question remaining for decision [of] whether the search and seizure conducted in this case complied with constitutional standards" after finding that a "search" had occurred in the case); *cf.* Smith v. Maryland, 442 U.S. 735, 745–46 (1979) ("The installation and use of a pen register . . . was not a 'search,' and no warrant was required.").

41. *See Katz*, 389 U.S. at 357 ("'Over and again this Court has emphasized that' . . . searches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions." (footnote omitted) (quoting United States v. Jeffers, 342 U.S. 48, 51 (1951))); United States v. Kincade, 379 F.3d 813, 822 (9th Cir. 2004) (recognizing that in the criminal context, either a warrant or an applicant warrant exception may satisfy the Fourth Amendment); Tracey Maclin, *When the Cure for the Fourth Amendment is Worse than the Disease*, 68 S. CAL. L. REV. 1, 5, 7 (1994) (arguing that the purpose of the Fourth Amendment is to control executive power and that it does so via a strong preference for searches and seizures conducted pursuant to warrants); *cf.* Terry v. Ohio, 392 U.S. 1, 20 (1968) (explaining why a specific type of police conduct, the *Terry* "stop and frisk," is not subject to the ordinary requirements of a warrant and probable cause).

42. Many warrant exceptions require probable cause. Under the automobile exception to the warrant requirement, for example, police may search a vehicle without a warrant if they have probable cause to believe the vehicle contains evidence of a crime and the vehicle is "readily mobile." *See* Pennsylvania v. Labron, 518 U.S. 938, 940 (1996). Also, under the search incident to arrest exception, police must have probable cause to arrest a suspect before they may search the arrestee as an incident to the arrest. United States v. Robinson, 414 U.S. 218, 235 (1973) ("A custodial arrest of a suspect based on probable cause is a reasonable intrusion under the Fourth Amendment; that intrusion being lawful, a search incident to the arrest requires no additional justification. . . . [Thus,] in the case of a lawful custodial arrest a full search of the person is not only an exception to the warrant requirement of the Fourth Amendment, but is also a 'reasonable' search under that Amendment."). The plain view exception to the warrant requirement likewise requires a showing of probable cause. Arizona v. Hicks, 480 U.S. 321, 326 (1987) (holding that probable cause is required to seize an item under the plain view exception).

43. *See, e.g.*, New Jersey v. T.L.O., 469 U.S. 325, 337–41 (1985) (explaining, in one special needs scenario, why the warrant and probable cause requirements are particularly unsuited to the

this law has developed, the Supreme Court has often held that such "special needs" searches must be both reasonable at their inception and reasonable in scope,[44] but the Court has generally refused to require either warrants or probable cause, opting instead for a less rigorous level of suspicion.[45]

Finally, once a court determines that a search or seizure has occurred (under step 1), and if such action was deemed unreasonable (under step 2), the court must determine the remedy for the Fourth Amendment violation.[46] In the criminal prosecution context, the usual remedy is exclusion of any evidence obtained as a result of the violation,[47] without which a criminal prosecution will often fail.[48] The exclusionary rule also applies in certain employee disciplinary proceedings.[49] Nevertheless, in the employment context—such as in a 42 U.S.C. § 1983 civil suit alleging a Fourth Amendment violation—the usual remedy is money damages for the employee whose Fourth Amendment rights were violated.[50]

O'Connor v. Ortega,[51] which involved an alleged Fourth Amendment violation by a public employer, illustrates the first and second steps

---

K–12 school environment and adopting a general reasonableness standard for assessing the legality of a student search).

44. *See, e.g.*, *id.* at 341–42 (applying this framework to K–12 school searches).

45. *See* O'Connor v. Ortega, 480 U.S. 709, 720–22 (1987) (rejecting the warrant and probable cause requirements in the employment context). In one special needs scenario, the Court found that "[t]he warrant requirement . . . is unsuited to the [K–12] school environment [because] requiring a teacher to obtain a warrant before searching a child suspected of an infraction of school rules (or of the criminal law) would unduly interfere with the maintenance of the swift and informal disciplinary procedures needed in the schools." *T.L.O.*, 469 U.S. at 340. For similar reasons, the *T.L.O.* Court found the probable cause requirement inapplicable as well. *See id.* at 341.

46. *See generally* Hudson v. Michigan, 547 U.S. 586, 590–91 (2006) (recognizing that although evidence obtained in violation of the Fourth Amendment is often excluded in a subsequent criminal prosecution, exclusion is not always required).

47. *See* Mapp v. Ohio, 367 U.S. 643, 655 (1961) (establishing the general rule that "all evidence obtained by searches and seizures in violation of the Constitution is . . . inadmissible in a state court"). There are, however, numerous exceptions to the exclusionary rule in the criminal context. *See, e.g.*, State v. Jackson, 464 S.W.3d 724, 734 (Tex. Crim. App. 2015) (refusing to exclude evidence obtained from an illegal instance of GPS tracking under the attenuation exception to the exclusionary rule).

48. Whether a criminal conviction may be obtained, despite the exclusion of a key piece of evidence, will of course depend on whether the prosecution has additional, legally-obtained evidence sufficient to support a conviction.

49. *See* Cunningham v. N.Y. State Dep't of Labor, N.Y.S.2d 432, 435 (N.Y. App. Div. 2011), *rev'd*, 997 N.E.2d 468 (N.Y. 2013) (involving application of the exclusionary rule in an employee disciplinary proceeding, rather than in an invasion of privacy suit against the employer).

50. *See, e.g.*, K-Mart Corp. Store No. 7441 v. Trotti, 677 S.W.2d 632, 638 (Tex. Ct. App. 1984) (noting that a plaintiff-employee was awarded $108,000 in damages for an invasion of privacy by her employer).

51. 480 U.S. 709 (1987).

outlined above, and is particularly significant in assessing the privacy rights of employees. [52]

O'Connor involved a search of the office of a state hospital employee, Dr. Magno Ortega. The search uncovered personal items later used in an administrative proceeding resulting in the employee's termination.[53] Applying the reasonable expectation of privacy test, the Court first clarified that a search or seizure of a government employee's property may be subject to Fourth Amendment restraints, thereby rejecting the employer's argument that public employees may never reasonably expect privacy at work.[54] Noting that Fourth Amendment protections are contextual,[55] the Court then declared that different workplaces generate different expectations of privacy depending on their unique "operational realities."[56] According to the Court, factors that may influence actual expectations of privacy in a particular workplace include "actual office practices and procedures,"[57] "the context of the employment relation,"[58] and "legitimate regulation" of the workspace.[59] The Court noted, for example, that some government offices may be so open to others that no expectation of privacy is reasonable.[60] In the employment context, other factors—including, most notably, notice and consent to the employer practice at issue[61]—have become critical as well.

Turning to the particular circumstances of Dr. Ortega's workplace, the Court determined that Dr. Ortega could indeed reasonably expect privacy in his office.[62] The Court emphasized that Dr. Ortega did not share his desk or file cabinets with other employees, that he had occupied his office for 17 years and had kept personal materials there, and that his expectation of privacy was not diminished by any hospital policy discouraging employees from storing personal items in desks or file cabinets.[63] As such, Dr. Ortega reasonably expected privacy "at least in his desk and file cabinets."[64]

Having determined that Dr. Ortega was indeed entitled to Fourth Amendment protection, the Court then sought to determine "the standard

52. *Id.* at 715 (plurality opinion).
53. *Id.* at 712–13.
54. *Id.* at 715, 717.
55. *Id.* at 715.
56. *Id.* at 717.
57. *Id.*
58. *Id.*
59. *Id.*
60. *Id.*
61. *See supra* note 32 and accompanying text.
62. *O'Connor*, 480 U.S. at 718 (plurality opinion).
63. *Id.* at 718–19.
64. *Id.* at 719.

of reasonableness applicable to [this] particular class of [workplace] searches."[65] As a special needs scenario involving a non-criminal investigation, the applicable reasonableness standard would be determined by balancing the nature of the intrusion into the employee's private affairs against the employer interests at stake, including "the government's need for supervision, control, and the efficient operation of the workplace."[66]

After weighing the competing interests, the Court determined that the warrant requirement should not apply in this scenario, as public employers "are hardly in the business of investigating the violation of criminal laws" and instead conduct "work-related searches [as a mere] incident to the primary business of the [employer]."[67] For similar reasons, the Court determined that probable cause should not be required.[68] As a result, the Court concluded that "public employer intrusions on the constitutionally protected privacy interests of government employees for [1] noninvestigatory, work-related purposes, as well as for [2] investigations of work-related misconduct, should be judged by the standard of reasonableness under all the circumstances."[69]

Regarding the noninvestigatory form of intrusion, the Court noted that the reasonableness inquiry would not be particularly rigorous, and that public employers should be afforded "wide latitude" to perform such intrusions[70] given that the employer's interest in efficient operation of the workplace is "substantial" vis-à-vis the relatively limited expectations of privacy enjoyed by employees, which "are far less than those found at home or in some other contexts."[71] The Court "[came] to a similar conclusion for searches conducted pursuant to an investigation of work-related employee misconduct,"[72] and further emphasized that a "reasonable suspicion" standard, as opposed to probable cause, would best serve the needs of such employers "in [promptly] correcting the employee misconduct."[73]

Finally, the Court declared that a public employer search—regardless of whether it is conducted for an investigatory or noninvestigatory

65. *Id.*

66. *Id.* at 719–20.

67. *Id.* at 722.

68. *See id.* at 722–25. The Court emphasized that its decision was limited to public employer searches that involve either a noninvestigatory work-related intrusion or an investigatory search for evidence of suspected work-related employee malfeasance. *See id.* at 725–26.

69. *Id.* at 725–26.

70. *Id.* at 723.

71. *Id.* at 725.

72. *Id.* at 724.

73. *Id.*

purpose—will be deemed "reasonable" only if reasonable at its inception and in its scope.[74] As to the first prong, the Court declared that a search of an employee's office will be "'justified at its inception' when there are reasonable grounds for suspecting that the search will turn up evidence that the employee is guilty of work-related misconduct, or that the search is necessary for a noninvestigatory work-related purpose such as to retrieve a needed file" from an employee's office.[75] Finally, the Court added that such a search will be reasonable in scope when "the measures adopted are reasonably related to the objectives of the search and not excessively intrusive in light of . . . the nature of the [misconduct]."[76]

O'Connor provides four significant takeaways for the question of whether employee tracking is lawful. First, *O'Connor* established that government employees may enjoy Fourth Amendment protections in a given workplace, depending on its unique circumstances.[77] Second, *O'Connor* ruled that the Fourth Amendment claim of a public employee will depend on whether the employer acted reasonably, both at inception and in scope.[78] Third, for a search to be reasonable at its inception, the employer conducting the search must have had "reasonable suspicion"[79] either that the search would turn up evidence of work-related misconduct, or that the search was necessary for a noninvestigatory work-related purpose, such as to retrieve a needed file from an employee's office.[80] Finally, to be reasonable in scope, the employer's search must not be "excessively intrusive in light of . . . the nature of the [misconduct]."[81]

---

74. *Id.* at 725–26.

75. *Id.* at 726.

76. *Id.* (alteration in original) (quoting New Jersey v. T.L.O., 469 U.S. 325, 342 (1985)).

77. *Id.* at 725–26.

78. *Id.* at 726.

79. *See id.* at 724 ("The delay in correcting the employee misconduct caused by the need for probable cause rather than *reasonable suspicion* will be translated into tangible and often irreparable damage to the agency's work, and ultimately to the public interest." (emphasis added)). Although at times the *O'Connor* Court used the phrase, "reasonable grounds for suspecting," this phrase has been repeatedly used by the Supreme Court in Fourth Amendment cases as a substitute for the familiar "reasonable suspicion" standard. *See* United States v. Vinton, 594 F.3d 14, 25 (D.C. Cir. 2010) (recognizing that, in the context of the search incident to arrest exception to the warrant requirement, the Court's use of the phrase "reasonable to believe" in *Arizona v. Gant*, 556 U.S. 332 (2009), "probably is akin to the 'reasonable suspicion' standard"). Moreover, courts have interpreted the *O'Connor* language itself as requiring a showing of "reasonable suspicion." *See* Cunningham v. N.Y. State Dep't of Labor, 997 N.E.2d 468, 473 (N.Y. 2013) ("Under *O'Connor*, a workplace search based on a reasonable suspicion of employee misconduct is 'justified at its inception.'" (quoting *O'Connor*, 480 U.S. at 726 (plurality opinion))).

80. *O'Connor*, 480 U.S. at 726 (plurality opinion).

81. *Id.* at 726 (alteration in original) (quoting New Jersey v. T.L.O., 469 U.S. 325, 342 (1985)).

Over twenty years after *O'Connor*, the Supreme Court applied the *O'Connor* framework in another public employer search case, *City of Ontario v. Quon*,[82] involving the city's review of text messages sent and received on Ontario police officer Jeff Quon's employer-issued pager.[83] Before acquiring the pagers, the city informed its officers that it had a right to review text messages sent and received using the pagers.[84] After Officer Quon and others had reimbursed the city multiple times for exceeding their monthly allowance of text messages, the city wished to determine whether the monthly text message character limit should be increased, requiring the city to determine whether officers like Quon were incurring overage fees for work-related or personal messages.[85] To that end, Quon's supervisors obtained two months of pager transcripts from provider Arch Wireless.[86] After redacting all messages Quon sent while off duty, officials learned that most of Quon's text messages sent during work hours were not work-related.[87] As a result, Quon was disciplined for pursuing personal matters while on duty.[88] Quon then sued the city, alleging that it violated his Fourth Amendment rights by reviewing his pager messages.[89] After the lower courts issued differing rulings on the issue, the United States Supreme Court granted certiorari to address the Fourth Amendment claim.[90]

During the Supreme Court proceedings, the parties agreed that the *O'Connor* framework would control.[91] Applying that framework, the Court assumed that Quon reasonably expected privacy in the contents of his text messages[92] and went on to address the overall reasonableness of the search by considering whether it was justified at its inception and reasonable in scope.[93]

Finding the search reasonable under both prongs, the Court first declared that the text message review was "justified at its inception because there were 'reasonable grounds for suspecting that the search [was] necessary for a noninvestigatory work-related purpose,'"[94] namely,

82. 560 U.S. 746 (2010).

83. *Id.* at 752.

84. *Id.* at 751–52.

85. *Id.* at 752.

86. *Id.*

87. *Id.* at 752–53.

88. *Id.* at 753. The Court says that "Quon was allegedly disciplined." *Id.*

89. *Id.* at 754. There were other plaintiffs and defendants in the case. *See id.* at 753. For simplicity, this Article limits its discussion to Quon's suit against the City.

90. *See id.* at 754–55 (describing the lower court rulings).

91. *Id.* at 757.

92. *Id.* at 760.

93. *Id.* at 760–61.

94. *Id.* at 761.

to ensure the city was paying only for work-related, rather than personal, communications.[95]

As for the search's scope, the Court emphasized the limited scope of the city's review, noting that although Quon had exceeded his monthly character limit several times, the city reviewed only two months of transcripts and redacted all messages Quon sent while off duty, which reduced the review's intrusiveness.[96] Finally, the Court noted that Quon had been informed his text messages could be reviewed and thus had "received no assurances of privacy," thereby "lessen[ing] the risk that the [city's] review would intrude on highly private details of Quon's life."[97] For these reasons, the Court found no Fourth Amendment violation.[98]

B. *Employees of Private Employers*

Given the lack of state action, private employers are typically not subject to Fourth Amendment constraints.[99] Nevertheless, private employers may face liability for alleged privacy invasions through tort law, including the torts of intrusion upon seclusion (intrusion),[100] public

95. *Id.* (quoting O'Connor v. Ortega, 480 U.S. 709, 726 (1987) (plurality opinion)).

96. *Id.* at 761–62.

97. *Id.* at 762–63.

98. *Id.* at 763–65.

99. *See* Skinner v. Ry. Labor Execs.' Ass'n, 489 U.S. 602, 613–14 (1989) ("The Amendment guarantees the privacy, dignity, and security of persons against certain arbitrary and invasive acts by officers of the Government or those acting at their direction."). Purely private action cannot form the basis for a 42 U.S.C. § 1983 civil suit based on an alleged Fourth Amendment violation. *See, e.g.*, English v. Univ. of Tulsa, No. 14-CV-0284-CVE-FHM, 2015 WL 4623942, at *4–5 (N.D. Okla. Aug. 3, 2015) (dismissing plaintiff's 42 U.S.C. § 1983 claim when campus security officers of the University of Tulsa, a private university, entered plaintiff's apartment without consent because the alleged Fourth Amendment violation by campus police was not committed by a person "acting under color of state law" (quoting West v. Atkins, 487 U.S. 42, 48 (1988))). However, in limited instances, a private employer could be subject to constitutional constraints, particularly where the private party acts as an instrument or agent of the Government. *See Skinner*, 489 U.S. at 614. Whether a private individual or entity should be deemed an agent of the government for Fourth Amendment purposes is determined by the totality of the circumstances. *Id.* Under this test, most courts consider two primary factors: (1) whether the government directed, or acquiesced in, the intrusive conduct; and (2) whether the party performing the search intended to assist law enforcement efforts or to further his own ends. Under this test, the greater the government involvement in the search, the less important the private searcher's intent. *See, e.g.*, Piazzola v. Watkins, 442 F.2d 284, 289 (5th Cir. 1971) (striking down a college dorm room search conducted by both local law enforcement officers and university officials, at the request and direction of the local police, and recognizing that a university regulation permitting administrative inspections of dorm rooms "cannot be construed or applied so as to give consent to a search for evidence for the primary purpose of a criminal prosecution").

100. *See* Koeppel v. Speirs, 808 N.W.2d 177, 180–81 (Iowa 2011) (describing the four invasion of privacy torts).

disclosure of truthful but private facts about an individual,[101] placing a person in a "false light" by unreasonable and highly objectionable publicity,[102] and appropriating the name or likeness of another for one's own commercial use or benefit.[103] These distinct forms of invasion each involve an interference with a person's "right to be left alone."[104] For workplace intrusions, private employers might also be governed by privacy statutes, including the federal Electronic Communications Privacy Act[105] and the Stored Communications Act,[106] either of which might restrain employers from intercepting or reviewing employee e-mail, telephone calls, and other electronic communications.[107] In addition, some state statutes specifically make it unlawful for employers to utilize GPS tracking as a means of investigating their employees, often with an exception based on employee consent.[108]

---

101. This tort involves publication of information that would be highly offensive to a reasonable person and not of legitimate public interest. RESTATEMENT (SECOND) OF TORTS § 652D (AM. LAW INST. 1977). In one case, for example, a plaintiff employee sued her former employer under this tort when the former employer posted an interoffice memo about the plaintiff's termination on a bulletin board visible to numerous employees. Payton v. City of Santa Clara, 183 Cal. Rptr. 17, 17 (Cal. Ct. App. 1982).

102. "To prevail on a claim of 'false light,' a plaintiff 'must show that a highly offensive false statement was publicized by [defendants] with knowledge or in reckless disregard of the falsity.'" Taha v. Bucks Cty., 9 F. Supp. 3d 490, 493 (E.D. Pa. 2014) (quoting Santillo v. Reedel, 634 A.2d 264, 266 (Pa. Super. Ct. 1993)), *aff'd*, 862 F.3d 292 (3d Cir. 2017); *see, e.g.*, *id.* at 491, 494 (finding sufficient "false light" claim against company based on plaintiff's allegations that company selectively published his expunged arrest record and mugshot on its website in order to falsely portray him as a criminal, thereby creating a false impression regarding his criminal history and character).

103. Under this cause of action, liability arises from the use of the name or likeness of a public figure absent consent. RESTATEMENT (SECOND) OF TORTS § 652C cmt. b.

104. *Koeppel*, 808 N.W.2d at 181 (citing RESTATEMENT (SECOND) OF TORTS § 652C cmt. b).

105. Pub. L. No. 90-351, 82 Stat. 212 (1968) (codified as amended at 18 U.S.C. §§ 2510–2511 (2012)).

106. Pub. L. No. 99-508, 100 Stat. 1860 (1986) (codified as amended at 18 U.S.C. §§ 2701–2712 (2012)).

107. *See* 18 U.S.C. § 2511(1)(a) (prohibiting the intentional interception of any electronic communication); Pure Power Boot Camp v. Warrior Fitness Boot Camp, 587 F. Supp. 2d 548, 557–58 (S.D.N.Y. 2008) (interpreting the ECPA, consistently with most courts' interpretation, to apply only to the simultaneous "interception" of e-mail as it is being sent and received; for e-mails that are in storage, the Stored Communications Act, 18 U.S.C. §§ 2701–2712 (2012) would apply).

108. *See, e.g.*, CONN. GEN. STAT. § 31-48d(b)(1) (2018) (requiring an employer to provide prior written notice to all employees informing them that they may be monitored electronically, as a general rule); 720 ILL. COMP. STAT. 5/21-2.5(b) (2018) (generally prohibiting persons in Illinois from using an electronic tracking device to determine the location or movement of a person, with an exception for consent, among others); Gerardi v. City of Bridgeport, 985 A.2d 328, 333–34 (Conn. 2010) (suggesting the Connecticut statute would apply to GPS tracking).

The tort of intrusion is the most common tort used to sue employers for privacy invasions in the workplace, and its requirements overlap with those of the Fourth Amendment. To prevail on an intrusion claim, a plaintiff must prove that "(1) her solitude, seclusion, or private affairs were intentionally infringed upon, and that (2) this infringement would highly offend a reasonable person."[109]

Courts considering intrusion claims usually also consider whether the plaintiff could reasonably expect privacy in the case at hand, because without such an expectation an intrusion claim would fail.[110] A recent District Court opinion denying a defendant's motion to dismiss involving Facebook posts, *Ehling v. Monmouth-Ocean Hospital Service Corp.*,[111] exemplifies this reasonable expectation of privacy approach.

According to the plaintiff's allegations in *Ehling*, plaintiff Deborah Ehling was a registered nurse and paramedic who worked for Monmouth-Ocean Hospital Service Corporation (MONOC), a nonprofit hospital service corporation in New Jersey.[112] In July 2008, Ehling became the acting president of a local union for professional emergency medical services personnel, and in that capacity she sought to protect the rights of union members by filing various complaints against MONOC.[113] According to Ehling, her union activities caused MONOC to retaliate against her, eventually leading to her termination in July 2011.[114]

---

109. Ehling v. Monmouth-Ocean Hosp. Serv. Corp., 872 F. Supp. 2d 369, 373 (D.N.J. 2012) (citing Bisbee v. John C. Conover Agency Inc., 452 A.2d 689 (N.J. Super. Ct. App. Div. 1982)) (applying New Jersey law); *see also* K-Mart Corp. Store No. 7441 v. Trotti, 677 S.W.2d 632, 636 (Tex. Ct. App. 1984) (citing Indus. Found. of the S. v. Tex. Indus. Accident Bd., 540 S.W.2d 668, 682 (Tex. 1975)) ("[I]n Texas, an actionable invasion of privacy by intrusion must consist of an unjustified intrusion of the plaintiff's solitude or seclusion of such magnitude as to cause an ordinary individual to feel severely offended, humiliated, or outraged.").

110. There appear to be two bases for considering whether a reasonable expectation of privacy exists, even though it is not usually thought of as a formal element of the tort of intrusion. According to some courts, the first element of the tort "requires an intentional intrusion into a matter the plaintiff has a right to expect privacy," making it necessary to consider the threshold question of reasonable expectation of privacy. *See, e.g.*, Koeppel v. Speirs, 808 N.W.2d 177, 181 (Iowa 2011). According to other courts, an infringement upon one's privacy cannot be highly offensive if there is no reasonable expectation of privacy in the first place. *See, e.g.*, Acosta v. Scott Labor LLC, 377 F. Supp. 2d 647, 649–52 (N.D. Ill. 2005) (analyzing a plaintiff–employee's intrusion upon seclusion claim by considering whether the employee could reasonably expect privacy in videotaping occurring at work and, upon finding he could not, stating that it need not address whether the alleged privacy intrusion was "highly offensive" to prove the tort of intrusion).

111. 872 F. Supp. 2d 369 (D.N.J. 2012).

112. *Id.* at 370.

113. *Id.*

114. *Id.*

From 2008 to 2009, Ehling maintained a private Facebook account with limited access to Ehling's "friends."[115] Ehling invited many coworkers, but no members of MONOC management, to be her Facebook friends.[116] In June 2009, MONOC officials gained access to Ehling's Facebook account when a supervisor summoned a MONOC employee, who was one of Ehling's Facebook friends, into an office and coerced him into accessing his Facebook account on a work computer in the supervisor's presence.[117] The supervisor then viewed and copied Ehling's Facebook postings, including one unusual comment Ehling had made regarding a shooting at the Holocaust Museum in Washington, D.C., wherein Ehling blamed the D.C. paramedics for the death of a museum guard.[118]

A few days later, MONOC officials informed the New Jersey Board of Nursing and the New Jersey Department of Health of Ehling's Facebook post, expressing its concern that Ehling's post "showed a disregard for patient safety."[119] According to Ehling, MONOC's letters placed her nursing license at risk and were intended to damage her reputation and employment opportunities.[120] As a result, Ehling sued MONOC and others for the tort of intrusion upon seclusion (common law invasion of privacy) due to the supervisor's unauthorized "accessing of her private Facebook postings."[121] Defendants then moved to dismiss the claim, arguing that Ehling could not reasonably expect privacy in her Facebook post because it was disclosed to potentially hundreds of people.[122] In response, Ehling argued that she could reasonably expect privacy in her post, at least insofar as the supervisor who accessed her page was concerned, because her comment was disclosed to a limited number of people whom she had personally invited to view a restricted access webpage.[123]

Denying Defendants' motion, the court noted that Ehling's case occupied a middle ground between cases finding no reasonable expectation of privacy for "material posted to an unprotected website that anyone can view," and those finding "a reasonable expectation of privacy for individual, password-protected online communications."[124] Because

115. *Id.*
116. *Id.*
117. *Id.*
118. *Id.*
119. *Id.* at 370–71.
120. *Id.* at 371.
121. *Id.* at 372.
122. *Id.* at 372, 374.
123. *Id.* at 374.
124. *Id.* at 373–74 (emphasis omitted) (citing United States v. Gines-Perez, 214 F. Supp. 2d 205, 225 (D.P.R. 2002), *rev'd on other grounds*, 90 F. App'x 3 (1st Cir. 2004); Stengart v. Loving

the matter was unclear, the court decided that Ehling's intrusion claim should not be dismissed, explaining that "reasonableness (and offensiveness) are highly fact-sensitive inquiries" that are "not properly resolved on a motion to dismiss."[125]

Although Ehling's case involved a suit against a private employer for the tort of intrusion, the court's entire analysis of Ehling's tortious intrusion claim at the motion to dismiss stage focused on whether Ehling could reasonably expect privacy in her Facebook post.[126] Numerous other cases involving private employers follow the same approach and emphasize that the reasonable expectation of privacy analysis under the tort of intrusion involves both a subjective and objective component, just as it does under the Fourth Amendment.[127]

Although the formal proof requirements of a Fourth Amendment claim (typically brought against a public employer) and an invasion of privacy tort claim (typically brought against a private employer) are distinct, a plaintiff suing either type of employer under either type of claim must ordinarily prove she could reasonably expect privacy in the case at hand.[128] Nevertheless, because the tort of intrusion requires proof that the defendant's invasion of a plaintiff's privacy would cause an individual "to feel severely offended, humiliated, or outraged,"[129] this tort is arguably more difficult to prove than a Fourth Amendment claim, which merely requires a plaintiff to prove the defendant's conduct was "unreasonable."[130] Thus, it makes sense to first examine instances of employee tracking through an expectation of privacy lens, and then to consider whether reasonableness (under the Fourth Amendment) or extreme offensiveness (under the tort of intrusion) might change the outcome in a given case. Before addressing the most common methods of employee tracking, this Article examines the law that governs GPS

Care Agency, Inc., 990 A.2d 650 (N.J. 2010)).

125. *Id.* at 374.

126. *See id.*

127. *See Stengart*, 990 A.2d at 660–61 (comparing the two claims); *see also, e.g.*, Acosta v. Scott Labor LLC, 377 F. Supp. 2d 647, 649–52 (N.D. Ill. 2005) (analyzing plaintiff-employee's intrusion upon seclusion claim by examining whether his asserted expectation of privacy at work was reasonable); *Stengart*, 990 A.2d at 663–64 (analyzing plaintiff's intrusion upon seclusion claim against a private employer by considering whether plaintiff could reasonably expect privacy in e-mails she retrieved on her work computer, examining both plaintiff's subjective expectation of privacy and whether her expectation was objectively reasonable).

128. *Cf. Stengart*, 990 A.2d at 660 ("[T]he reasonable-expectation-of-privacy standard used by the parties [in a suit against a private employer] derives from the common law and the Search and Seizure Clauses of both the Fourth Amendment and . . . the New Jersey Constitution. The [constitutional] sources do not apply in this case, which involves conduct by private parties only.").

129. K-Mart Corp. Store No. 7441 v. Trotti, 677 S.W.2d 632, 636 (Tex. App. 1984).

130. *See Stengart*, 990 A.2d at 660.

tracking by law enforcement, which necessarily impacts the related issue of GPS tracking by employers.

II. GPS TRACKING BY LAW ENFORCEMENT

Although there are few reported cases involving GPS tracking by employers, those cases must be viewed in light of the United States Supreme Court's decision in *United States v. Jones*,[131] which involved GPS tracking by law enforcement.[132]

A. *The Law of Electronic Tracking Before* United States v. Jones

Before *Jones* was decided in 2012, law enforcement routinely utilized GPS tracking devices, without having obtained a warrant authorizing them to do so, to monitor the movements of criminal suspects.[133] When criminal defendants challenged this form of investigation, most courts rejected those challenges by invoking the principle that no person can reasonably expect privacy in his or her movements in public.[134] This

131. 565 U.S. 400 (2012).

132. *Id.* at 403.

133. *See, e.g.*, United States v. Cuevas-Perez, 640 F.3d 272, 272–73 (7th Cir. 2011), *vacated*, 565 U.S. 1189 (2012) (describing an investigation in which Arizona police attached a GPS tracking device to the suspect's Jeep and then tracked the Jeep's movements into several states); United States v. Smith, 387 F. App'x. 918, 919 (11th Cir. 2010) (per curiam) (describing an investigation in Florida in which police installed a GPS device on the truck of a person suspected of trafficking marijuana); United States v. Marquez, 605 F.3d 604, 607 (8th Cir. 2010) (recounting how DEA and Iowa state police placed a GPS tracking device on a vehicle's bumper while it was parked in Iowa and used the device to monitor the vehicle's movements to Colorado); United States v. Pineda-Moreno, 591 F.3d 1212, 1213 (9th Cir. 2010) ("Over a four-month period, [DEA] agents [in Oregon] repeatedly monitored Pineda-Moreno's Jeep using various types of mobile tracking devices."), *vacated*, 565 U.S. 1189 (2010); United States v. Santiago, 560 F.3d 62, 64–65 (1st Cir. 2009) (detailing "a year-long investigation into a large-scale heroin distribution operation" in 2003 and 2004 in Massachusetts, in which agents tracked defendant's van with a GPS unit); United States v. Mayberry, 540 F.3d 506, 511 (6th Cir. 2008) (noting that in a robbery investigation, police in Michigan "secretly placed a GPS tracking device on the [defendant's] rental car" while it was parked at an apartment complex); United States v. Wilson, 484 F.3d 267, 281 (4th Cir. 2007) (detailing an extensive federal drug investigation in Maryland involving GPS trackers).

134. *See, e.g.*, *Marquez*, 605 F.3d at 610 ("[W]hen police have reasonable suspicion that a particular vehicle is transporting drugs, a warrant is not required when, while the vehicle is parked in a public place, they install a noninvasive GPS tracking device on it for a reasonable period of time."); *Pineda-Moreno*, 591 F.3d at 1216–17 (invoking *Knotts* and holding that the GPS tracking of an individual's movements in his vehicle over a prolonged period is not a search); United States v. Garcia, 474 F.3d 994, 996–97 (7th Cir. 2007) (relying on *Knotts* and holding that GPS tracking is not a search); *see also Cuevas-Perez*, 640 F.3d at 276 (Flaum, J., concurring) ("The practice of using [GPS tracking] devices to monitor movements on public roads falls squarely within the [Supreme] Court's consistent teaching that people do not have a legitimate expectation of privacy in that which they reveal to third parties or leave open to view by others.").

result is seemingly supported by two Supreme Court cases from the 1980s, each involving the tracking of a vehicle by electronic beeper.

In *United States v. Knotts*,[135] the Supreme Court upheld the warrantless use of a beeper to track a drum of chloroform along a 100-mile journey.[136] According to the Court in *Knotts*, the use of the beeper did not constitute a Fourth Amendment search because the beeper did not provide any information police could not have obtained through simple visual surveillance.[137] Just one year later, the Court in *United States v. Karo*[138] reached the opposite result in a similar case, primarily because the beeper in that case was used to track a can of ether inside a private residence.[139] Distinguishing *Knotts*, the Court reasoned that "[i]ndiscriminate monitoring of property that has been withdrawn from public view" must remain subject to Fourth Amendment oversight.[140]

Invoking *Knotts*, pre-*Jones* GPS tracking cases typically found that when a GPS tracking device is used to monitor a suspect's movements on public roads, no Fourth Amendment search occurs—because a suspect cannot reasonably expect privacy in those movements given that police could have simply trailed the suspicious vehicle to obtain the same information.[141] However, some pre-*Jones* courts refused to apply this rationale on the grounds that it fails to account for differences between trailing a vehicle for a few hours and using GPS technology to track that same vehicle for a substantially longer period of time, which is far more

135. 460 U.S. 276 (1983).

136. *Id.* at 276. Having suspected Knotts of manufacturing drugs, federal officers, without a warrant, had installed a beeper in a chemical drum they knew would be sold to Knotts. *Id.* at 278. With the beeper's assistance, officers followed Knotts's vehicle to where it stopped outside a certain cabin. *Id.* Based on this information, the police secured a warrant to search the cabin and uncovered incriminating evidence inside. *Id.* at 279.

137. According to the *Knotts* Court, "[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another," and the "use of the beeper to signal the presence of [the vehicle] . . . does not alter the situation." *Id.* at 281–82.

138. 468 U.S. 705 (1984).

139. *See id.* at 714.

140. *Id.* at 716. As the Court explained, "[*Karo*] is thus not like *Knotts*, for there the beeper told the authorities nothing about the interior of Knotts' cabin. . . . [H]ere, [by contrast] . . . the monitoring indicated that the beeper was inside the house, a fact that could not have been visually verified [by the police from outside the house]." *Id.* at 715.

141. *See, e.g.*, United States v. Pineda-Moreno, 591 F.3d 1212, 1216 (9th Cir. 2010) (invoking *Knotts* and holding that the GPS tracking of an individual's movements in his vehicle over a prolonged period is not a search), *vacated*, 565 U.S. 1189 (2012); United States v. Garcia, 474 F.3d 994, 997 (7th Cir. 2007) (same), *abrogated by* 776 F.3d 513 (2015).

invasive.[142] The Supreme Court granted certiorari in *Jones* to resolve the split.[143]

B. United States v. Jones

In *Jones*, all nine Justices of the United States Supreme Court struck down one instance of GPS tracking in which a suspect's vehicle was monitored on public streets for nearly a month.[144]

In *Jones*, officers surreptitiously installed a GPS tracking device on suspect Antoine Jones's Jeep, without a valid warrant,[145] and used the device to track the vehicle for twenty-eight days.[146] The resulting GPS data connected Jones to a structure that contained cash and cocaine, leading to criminal charges against him.[147] Before trial, Jones moved to suppress the evidence obtained through the GPS tracking device, but the trial court denied the motion by invoking the *Knotts* rationale that no person may reasonably expect privacy in his movements in public.[148]

---

142. *See, e.g.*, United States v. Maynard, 615 F.3d 544, 555–68 (D.C. Cir. 2010) (rejecting the Government's argument, based on an attempted extension of *Knotts*, that "[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another" even in such extended instances of GPS tracking); People v. Weaver, 909 N.E.2d 1195, 1198–1201 (N.Y. 2009) (distinguishing *Knotts*) ("At first blush, it would appear that *Knotts* does not bode well for Mr. Weaver, for in his case, as in *Knotts*, the surveillance technology was utilized for the purpose of tracking the progress of a vehicle over . . . predominantly public roads and, as in *Knotts*, these movements were at least in theory exposed to 'anyone who wanted to look.' This, however, is where the similarity ends." (quoting *Knotts*, 460 U.S. at 281)).

143. United States v. Jones, 564 U.S. 1036 (2011).

144. *See* United States v. Jones, 565 U.S. 400, 404 (2012) (holding that "the Government's installation of a GPS device on a target's vehicle, and its use of that device to monitor the vehicle's movements, constitutes a [Fourth Amendment] 'search,'" thereby presumptively requiring a warrant (footnote omitted)); *see also id.* at 430–31 (Alito, J., concurring) (concluding on behalf of Justices Alito, Ginsburg, Breyer, and Kagan that the lengthy GPS monitoring that occurred in that case constituted a Fourth Amendment "search," thereby presumptively requiring a warrant); *id.* at 413 (Sotomayor, J., concurring) (internal citations omitted) (agreeing with the majority that "a search within the meaning of the Fourth Amendment occurs, at a minimum, '[w]here, as here, the Government obtains information by physically intruding on a constitutionally protected area'" (alteration in original)).

145. Although the officers had obtained a warrant authorizing installation of the device, the device was installed after the warrant had expired and outside the jurisdiction specified in the warrant. *See id.* at 402–03 (majority opinion).

146. *Id.* at 403. The device relayed more than 2,000 pages of data regarding the vehicle's movements over the four-week period. *Id.*

147. *Id.* at 403–04.

148. United States v. Jones, 451 F. Supp. 2d 71, 87–88 (D.D.C. 2006) (citing *Knotts*, 460 U.S. at 281–82), *rev'd in part*, United States v. Maynard, 615 F.3d 549 (D.C. Cir. 2010). The District Court granted the motion in part, suppressing only the data obtained while the vehicle was parked in the garage adjoining Jones's residence. *Id.* at 88.

On appeal, a majority of the Supreme Court—consisting of Justices Scalia, Roberts, Kennedy, Thomas, and Sotomayor[149]—considered "whether the attachment of a Global-Positioning-System (GPS) tracking device to an individual's vehicle, and subsequent use of that device to monitor the vehicle's movements on public streets, constitutes a search or seizure within the meaning of the Fourth Amendment."[150] By phrasing the issue in this manner, the *Jones* majority effectively limited its analysis to the movements of Jones's vehicle "on public streets,"[151] rather than within private spaces,[152] potentially triggering the *Knotts* rationale that no person may reasonably expect privacy in his movements in public. Refusing to apply this rationale, the majority held that a search had occurred.[153] Since no warrant justified the search, the evidentiary fruits of that search had to be suppressed.[154]

While all nine Justices in *Jones* agreed that this particular instance of GPS tracking triggered the protections of the Fourth Amendment,[155] the Justices

149. *Jones*, 565 U.S. at 401.

150. *Id.* at 402.

151. *Id.*

152. In limiting the issue to the movements of Jones's vehicle "on public streets," the *Jones* majority seemingly accepted the District Court's suppression of the GPS tracking data obtained while the vehicle was parked in the garage adjoining Jones's residence. *See id.* at 402–03.

153. According to the majority, "the Government's installation of a GPS device on a target's vehicle, and its use of that device to monitor the vehicle's movements, constitutes a 'search.'" *Id.* at 404. In its brief in *Jones*, the Government argued that individuals have no reasonable expectation of privacy in information that is knowingly exposed to public view, and that Antoine Jones himself had no reasonable expectation of privacy in the movements of his vehicle on public streets because that information was exposed to public view. *See* Brief for the United States at 18, 38, *Jones*, 565 U.S. 400 (No. 10-1259). The Government argued that "[t]his case, like *Knotts*, involves movements of a vehicle on public streets," which is unprotected by the Fourth Amendment. *Id.* at 19, 22. By ruling for Jones, the majority effectively rejected the Government's *Knotts*-based argument. *See also* United States v. Garcia-Gonzalez, No. 14-10296-LTS, 2015 WL 5145537, at *7 (D. Mass. Sept. 1, 2015) ("The [*Jones*] majority opinion also impliedly rejects as unsupported, by *Knotts* or otherwise, the suggestion that an unconstitutional search is permissible if it produces only public information.").

154. *See Jones*, 565 U.S. at 413 (affirming the lower court's judgment that admission of the evidence obtained by use of the GPS device violated the Fourth Amendment and refusing to address the Government's argument that the warrantless "search" that occurred in this case was made reasonable, despite no valid warrant, by the reasonable suspicion or probable cause the officers had obtained before using the device).

155. *See id.* at 404 (holding that "the Government's installation of a GPS device on a target's vehicle, and its use of that device to monitor the vehicle's movements, constitutes a [Fourth Amendment] 'search,'" thereby presumptively requiring a warrant (footnote omitted)); *see also id.* at 430–31 (Alito, J., concurring) (concluding on behalf of Justices Alito, Ginsburg, Breyer, and Kagan that the lengthy GPS monitoring that occurred in that case constituted a Fourth Amendment "search," thereby presumptively requiring a warrant); *id.* at 413 (Sotomayor, J., concurring) (agreeing with the majority that "a search within the meaning of the Fourth

were split in their rationale on the question of whether a Fourth Amendment search had occurred. Five members of the Court applied the physical trespass doctrine and the remaining members of the Court—along with Justice Sotomayor, who endorsed both views—applied the *Katz* reasonable expectation of privacy test.[156] Applying the physical trespass test, the majority declared that "a vehicle is an 'effect' as that term is used in the [Fourth] Amendment"[157] and that in this case, the Government physically trespassed upon Jones's vehicle by attaching the device to the vehicle without consent.[158] According to the majority, "the Government's installation of a GPS device on a target's vehicle, and its use of that device to monitor the vehicle's movements, constitutes a 'search,'"[159] which is presumptively unreasonable in the absence of a valid warrant.[160]

Justice Alito's concurring opinion, joined by Justices Ginsburg, Breyer, and Kagan, employed the *Katz* test instead, framing the issue as "whether the use of GPS tracking in [this] particular case involved a degree of intrusion that a reasonable person would not have anticipated."[161] Emphasizing the length of surveillance as a critical factor under *Katz*, the concurring Justices declared that the majority's trespass-based analysis "largely disregards what is really important (the *use* of a GPS for the purpose of long-term tracking)," emphasizing instead the officers' seemingly insignificant act of trespassing upon Jones's vehicle.[162] In the view of these four Justices,

---

Amendment occurs, at a minimum, '[w]here, as here, the Government obtains information by physically intruding on a constitutionally protected area'" (alteration in original)).

156. *See id.* at 405–06, 414, 419. According to the majority, *Katz* did not repudiate the understanding that the Fourth Amendment embodies a particular concern for government trespass upon the areas it enumerates. *See id.* at 406–07 (majority opinion). Rather, "the *Katz* reasonable-expectation-of-privacy test has been *added to*, not *substituted for*, the common-law trespassory test." *Id.* at 409. Thus, as the majority saw it, "Jones's Fourth Amendment rights do not rise or fall with the *Katz* formulation." *Id.* at 406. For future cases, however, the majority clarified that "[s]ituations involving merely the transmission of electronic signals without trespass would *remain* subject to *Katz* analysis." *Id.* at 411.

157. *Id.* at 404.

158. According to the majority, "[b]y attaching the device to the Jeep, officers encroached on a protected area." *Id.* at 410.

159. *Id.* at 404 (footnote omitted). In a similar passage, the majority declared: "The Government physically occupied private property [i.e., Jones's vehicle] for the purpose of obtaining information. We have no doubt that such a physical intrusion would have been considered a 'search' within the meaning of the Fourth Amendment when it was adopted." *Id.* at 404–05.

160. United States v. Karo, 468 U.S. 705, 717 (1984) ("Warrantless searches are presumptively unreasonable . . . .").

161. *Jones*, 565 U.S. at 430 (Alito, J., concurring).

162. *Id.* at 424–25; *see also id.* at 430–31 (emphasizing the length of surveillance as critical under the *Katz* test). Again emphasizing the length of surveillance, Justice Alito's concurrence

> the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy [because] [f]or such offenses, society's expectation has been that law enforcement agents and others would not . . . secretly monitor and catalogue every single movement of an individual's car for a very long period.[163]

For these reasons, the concurring Justices would have ruled that "the lengthy monitoring that occurred in this case [i.e., twenty-eight days] constituted a search" under the *Katz* test.[164]

Justice Sotomayor wrote separately to express agreement with both the majority and the concurrence.[165] According to Justice Sotomayor, the majority's trespass-based analysis was sufficient to resolve the case because "[t]he Government usurped Jones' property for the purpose of conducting surveillance on him, thereby invading privacy interests long afforded . . . Fourth Amendment protection."[166] Justice Sotomayor went on to declare, however, that the Fourth Amendment could be violated, "even in the absence of a trespass," under the *Katz* reasonable expectation of privacy framework.[167] Applying that framework, Justice Sotomayor agreed with the other four concurring Justices that "at the very least, 'longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.'"[168] Accordingly, at least five Justices in *Jones* rejected the notion that a person may never reasonably expect privacy in his movements in public and endorsed the view that GPS surveillance becomes more intrusive when conducted over a lengthy period of time, opinions that will likely impact the developing law of employer-initiated GPS tracking.[169]

---

described the issue as "whether respondent's reasonable expectations of privacy were violated by the long-term monitoring of the movements of the vehicle he drove." *Id.* at 419.

163. *Id.* at 430.

164. *Id.* at 430, 431. Notably, the concurring Justices did not attempt to determine "with precision the point at which the tracking of this vehicle became a search," *id.* at 430, but declared that "the line was surely crossed before the 4-week mark." *Id.*

165. *See id.* at 413–14 (Sotomayor, J., concurring).

166. *Id.* at 413–14.

167. *Id.* at 414 (quoting Kyllo v. United States, 533 U.S. 27, 33 (2001)).

168. *Id.* at 415.

169. *See* United States v. Garcia-Gonzalez, No. 14-10296-LTS, 2015 WL 5145537, at *7 (D. Mass. Sept. 1, 2015) (recognizing "the principle that a momentary observation is not a search," but noting that "the converse of that principle, that a lengthy sustained surveillance at some point becomes a search, is precisely the point made by Justice Alito's concurrence in the judgment [in *Jones*], in which four Justices joined and for which a fifth, Justice Sotomayor, expressed some support").

C. *How* Jones *Impacts Employers*

Jones impacts the legality of GPS tracking by employers in a number of ways. First, in unanimously rejecting the GPS tracking decisions preceding *Jones*, in which most courts had refused to extend Fourth Amendment protection to this investigative technique,[170] the *Jones* ruling revealed a Court concerned by the potential for mass surveillance inherent in this form of investigation, with an acute concern for longer term monitoring of a person's otherwise private affairs.[171] Although *Jones* dealt with the tracking of a single suspected drug dealer,[172] the Court's concerns regarding mass surveillance centered on the potential to track ordinary, law-abiding citizens on no suspicion of wrongdoing. Several Justices voiced this concern during oral argument in *Jones*. For example, Chief Justice Roberts inquired: "You think there would also not be a search [i.e., the Fourth Amendment would not apply] if you put a GPS device on all of our cars, monitored our movements for a month? You think you're entitled to do that under your theory?"[173] Expressing a similar concern, Justice Ginsburg inquired:

> [T]he government's position would mean that any of us could be monitored whenever we leave our homes. So, the only thing secure is the home. Is—I mean, that is—that is the end point of [the Government's] argument, that an electronic device, as long as it's not used inside the house, is okay.[174]

This overall sentiment, especially considering that no member of the Court sided with the Government in *Jones*, reveals that the current Court might not look favorably upon any instance of mass surveillance, particularly where the surveillance involves the GPS monitoring of numerous individuals in the absence of individualized suspicion of wrongdoing. This would likely be true in the employment context as well unless, as outlined below, an employer conducts such surveillance for a legitimate business reason unique to that employer.[175]

---

170. *See Jones*, 565 U.S. at 408–10.

171. *See id.* at 430–31 (Alito, J., concurring); *see also id.* at 415 (Sotomayor, J., concurring).

172. *See id.* at 402 (majority opinion) (describing the suspect as someone who the police suspected was "trafficking in narcotics").

173. Transcript of Oral Argument at 9, *Jones*, 565 U.S. 400 (No. 10-1259), http://www.supremecourt.gov/oral_arguments/argument_transcripts/2011/10-1259.pdf [https://perma.cc/WS8K-TAT7].

174. *Id.* at 12.

175. Recall that *O'Connor v. Ortega* requires that any search or seizure by a public employer be both reasonable at its inception and reasonable in scope. 480 U.S. 709, 725–26 (1987). Moreover, to be reasonable at its inception, *O'Connor* requires an employer to have "reasonable grounds for suspecting" that the employer's search will turn up evidence that the employee is

Second, and relatedly, it is doubtful that the employment context would alter the Court's analysis with respect to the threshold question of whether a Fourth Amendment search had occurred. As noted, a majority of Justices in *Jones* agreed that the placement of a GPS tracking device on a suspect's vehicle and use of that device to monitor the vehicle's movements constitutes a Fourth Amendment search under the physical trespass test,[176] and for that reason courts reviewing instances of GPS tracking by employers have had no difficulty finding that a search occurs upon a similar trespassory invasion of a public employee's vehicle.[177] Accordingly, any instance of GPS tracking carried out by a public employer by means of trespass would almost certainly constitute a Fourth Amendment "search" and would thus turn on the reasonableness of that action under the reasonableness test espoused in *O'Connor*.

Third, when GPS tracking is accomplished in the absence of a trespass, *Jones* clearly indicates that the *Katz* reasonable expectation of privacy test controls,[178] and there is no reason to believe this test would not apply for non-trespassory forms of location tracking in the employment context, where the *Katz* test has been applied often.[179] Thus, the question becomes whether, and under what exact circumstances, a reasonable expectation of privacy would exist in the event an employee's

---

guilty of work-related misconduct, or that the search is necessary for a noninvestigatory work-related purpose. *Id.* at 726. Although public employers should be afforded "wide latitude" to conduct such searches for "work-related, noninvestigatory reasons," *id.* at 723, the employer must still be able to point to "reasonable grounds for suspecting" the search is necessary in a given case, even where the search is conducted for a noninvestigatory work-related purpose, *see id.* at 725–26, which is the most likely instance in which mass surveillance would be used by an employer. *See infra* note 318 and accompanying text.

176. *See Jones*, 565 U.S. at 404.

177. *See, e.g.*, Cunningham v. N.Y. State Dep't of Labor, 997 N.E.2d 468, 471–72 (N.Y. 2013) (applying the physical trespass test, as espoused in *Jones*, to find a "search" had occurred when a public employer attached a GPS device to an employee's vehicle and later used the device to monitor the vehicle's movements).

178. *See Jones*, 565 U.S. at 411 ("Situations involving merely the transmission of electronic signals without trespass would *remain* subject to *Katz* analysis."); *see also id.* at 415 (Sotomayor, J., concurring) ("But '[s]ituations involving merely the transmission of electronic signals without trespass would *remain* subject to *Katz* analysis.'" (alteration in original)); *id.* at 430–31 (Alito, J., concurring) (arguing that the *Jones* majority erred in reviving the trespass test and suggesting that all "search" questions should be governed exclusively by *Katz*).

179. *See, e.g.*, *O'Connor*, 480 U.S. at 715–19 (analyzing whether an employee of a public hospital could reasonably expect privacy in his office); United States v. Barrows, 481 F.3d 1246, 1247 (10th Cir. 2007) (analyzing whether the plaintiff–employee could reasonably expect privacy in a personal computer he used at work); United States v. Yudong Zhu, 23 F. Supp. 3d 234, 237 (S.D.N.Y. 2014) (considering whether an employee could reasonably expect privacy in his work computer); K-Mart Corp. Store No. 7441 v. Trotti, 677 S.W.2d 632, 635─36 (Tex. App. 1984) (analyzing whether a search had occurred under *Katz* by considering whether the employee-plaintiff could reasonably expect privacy in her workplace locker).

movements are tracked in the absence of a trespass[180]—most notably, where an employee's location is determined through a GPS-enabled cell phone[181] or smartphone app.[182] In *Jones*, five Justices expressed the view that "longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy."[183] Although the concurring Justices were speaking in terms of *criminal* "offenses," the Justices reached this result because "society's expectation has been that law enforcement agents *and others* would not . . . secretly monitor and catalogue every single movement of an individual's car for a very long period."[184] Although it is unclear who these "others" referenced in the above quote might include, it is at least plausible that the concurring Justices deliberately left room to rein in the actions of other government actors, such as public employers, with respect to GPS monitoring. Indeed, the Court has repeatedly deemed the Fourth Amendment applicable to all types of government actors, including employers.[185]

Finally, if the concurring opinions in *Jones* are a guide, then length of surveillance may become important in any *Katz*-based analysis of employee tracking, particularly as it pertains to the scope of that surveillance.[186] According to the five concurring Justices in *Jones*, tracking a person's vehicle via GPS for twenty-eight days constituted a search under the *Katz* test (and hence a Fourth Amendment violation due to the lack of a valid warrant or applicable warrant exception).[187] These

180. Some courts have described *Jones* as signaling "a particular concern for government trespass upon the areas ('persons, houses, papers, and effects') [the Fourth Amendment] enumerates." United States v. Figueroa-Cruz, 914 F. Supp. 2d 1250, 1260 (N.D. Ala. 2012) (alteration in original) (quoting *Jones*, 565 U.S. at 406).

181. *See, e.g.*, United States v. Skinner, 690 F.3d 772, 779–80 (6th Cir. 2012). In a case where law enforcement "pinged" a suspect's phone to determine its location, the court distinguished *Jones* on the grounds that "[n]o such physical intrusion [of the suspect's phone] occurred in [this] case. [The suspect] himself obtained the cell phone for the purpose of communication, and that phone included the GPS technology used to track the phone's whereabouts." *Id.*

182. *See infra* notes 346–49 and accompanying text.

183. *See Jones*, 565 U.S. at 430 (Alito, J., concurring); *see also id.* at 415 (Sotomayor, J., concurring).

184. *Id.* at 430 (Alito, J., concurring) (emphasis added).

185. *See supra* notes 15–18 and accompanying text.

186. Many lower courts post-*Jones* have applied *Katz* in cases where no trespass has occurred. *See, e.g.*, State v. Jones, 903 N.W.2d 101, 109–10 (S.D. 2017) ("But this case does not concern a physical trespass; therefore, the *Katz* analysis controls [due to the opinions expressed in *Jones*]."). In addition, courts have recognized that length of surveillance is a critical factor in such a case. *Cf.* United States v. Patrick, 842 F.3d 540, 544 (7th Cir. 2016) ("If a cell-site simulator is like a GPS tracker, and if the approach of the concurring opinions in *Jones* is adopted, then it would be necessary to know how long the police used a simulator while searching for Patrick and just how accurate is the location information it provides.").

187. *See Jones*, 565 U.S. at 430 (Alito, J., concurring); *id.* at 415 (Sotomayor, J., concurring).

Justices did not identify the precise point at which the tracking became a search, but simply declared that "the line was surely crossed before the 4-week mark."[188] As a result, criminal suspects——and perhaps government employees as well——can arguably expect not to be tracked by GPS for such a lengthy period of time.[189] At the other end of the spectrum, the Court's prior holding in *United States v. Knotts*[190] suggests that a person traveling on public roads for just a few hours cannot reasonably expect privacy in those movements,[191] a decision *Jones* was careful not to overrule.[192] In the wake of *Jones*, the line between these two points remains unclear,[193] and, as explained below, is an issue that resurfaces in cases involving GPS tracking by employers—albeit under the separate question of whether an employer investigation is reasonable in scope.[194] With these principles in mind, this Article next examines instances of GPS tracking by employers.

III. GPS TRACKING BY EMPLOYERS

As noted, the Supreme Court in *O'Connor* adopted rules governing both investigations of work-related misconduct and searches conducted

188. *Id.* at 430 (Alito, J., concurring); *see also id.* at 415 (Sotomayor, J., concurring) (agreeing with the Alito concurrence that "at the very least, 'longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy'").

189. *See* United States v. Garcia-Gonzalez, No. 14-10296-LTS, 2015 WL 5145537, at *4 (D. Mass. Sept. 1, 2015) ("When considering the legality under the Fourth Amendment of long-term video surveillance of an individual's activities or home, unquestionably the various opinions issued by the Justices in *Jones* require serious and careful consideration.").

190. 460 U.S. 276 (1983).

191. *Id.* at 281–82, 285. In *Knotts*, the Court upheld the warrantless use of a beeper to track a drum of chloroform from the defendant's point of purchase to a cabin about 100 miles away. *Id.* at 285. According to the Court, the use of the beeper did not constitute a "search" because the beeper did not provide any information police could not have obtained through visual surveillance along the vehicle's route. *Id.* at 281–82. Just one year after *Knotts*, the Court in *United States v. Karo* examined a similar case and reached the opposite result as in *Knotts*, primarily because the beeper in that case was used to track a can of ether inside a private residence. United States v. Karo, 468 U.S. 705, 714–15 (1984).

192. *See Jones*, 565 U.S. at 409 (distinguishing *Knotts* as a case where the Court's trespass concerns did not apply because "[t]he beeper had been placed in the container before it came into Knotts' possession, with the consent of the then-owner"); *see also* United States v. Figueroa-Cruz, 914 F. Supp. 2d 1250, 1268 (N.D. Ala. 2012) (noting that *Jones* did not overrule *Knotts*, but rather distinguished it based on "the ownership or exclusivity of use of the chattel" at issue).

193. *See* United States v. Skinner, 690 F.3d 772, 780 (6th Cir. 2012) ("Justice Alito's concurrence and the majority in *Jones* both recognized that there is little precedent for what constitutes a level of comprehensive tracking that would violate the Fourth Amendment.").

194. *See, e.g.*, Cunningham v. N.Y. Dep't of Labor, 997 N.E.2d 468, 473 (N.Y. 2013) (striking down an instance of GPS tracking by an employer due to its duration).

for noninvestigatory work-related purposes.[195] This section addresses employer use of GPS tracking in both scenarios.

A. *GPS Tracking on an Individualized Basis to Investigate Employee Wrongdoing*

Jones was decided in January 2012.[196] Two years later, the Court of Appeals of New York applied *Jones* to an instance of GPS tracking conducted by the State of New York in its capacity as an employer.[197] The opinion is significant because, although it applied the *Jones* majority's trespass-based test to the initial "search" question and found an obvious search on facts similar to *Jones*,[198] it ultimately declared the search unlawful due to its duration.[199]

The employee in the New York case, Michael Cunningham, became a state employee in 1980.[200] In 2008, suspecting that Cunningham was submitting false time sheets and taking unauthorized absences from work, the New York State Department of Labor (the Department) attached a GPS device to Cunningham's car, without his knowledge, while the car was parked in a lot near the Department's offices.[201] The device was then used to track the vehicle's movements for thirty days, including evenings, weekends, and several days when Cunningham was on vacation in another state.[202] GPS information showed that Cunningham's arrival and departure times from work were not consistent with the number of hours he claimed on his time sheets.[203] On the strength of this and other evidence,[204] the Department brought thirteen charges of misconduct against Cunningham,[205] eight of which were dependent on evidence obtained from the GPS device.[206] Cunningham then sought to suppress

195. *See* O'Connor v. Ortega, 480 U.S. 709, 723 (1987).

196. *Jones*, 565 U.S. at 400.

197. *Cunningham*, 997 N.E.2d at 470–71, 475.

198. *See id.* at 475.

199. *See id.* at 473.

200. *Id.* at 470 (stating that in 2008, the New York State Department of Labor conducted an initial investigation of Cunningham which resulted in a two-month suspension, and that during this investigation, Cunningham successfully eluded an investigator who was following his car, prompting the Department to contact the Office of the State Inspector General about the matter, which then conducted an independent investigation of Cunningham).

201. *Id.*

202. *Id.*

203. *Id.*

204. *Id.* (stating that as part of the investigation, the state Inspector General conducted surveillance of an apartment building Cunningham was suspected of visiting during working hours, obtained subpoenas for E-ZPass records, and interviewed Cunningham and his secretary).

205. Cunningham v. N.Y. Dep't of Labor, 933 N.Y.S.2d 432, 434 (N.Y. App. Div. 2011), *rev'd*, 997 N.E.2d 468 (N.Y. 2013).

206. *Cunningham*, 997 N.E.2d at 470.

the GPS evidence, but the Hearing Officer overseeing his administrative proceeding denied the motion.[207] The Hearing Officer then found enough proof to sustain eleven of the thirteen charges and recommended termination of Cunningham's employment, which occurred shortly thereafter.[208]

Cunningham appealed his termination in court, arguing that the GPS tracking of his vehicle violated the Fourth Amendment such that the data obtained from that surveillance should have been suppressed.[209] Applying *Jones*, the court first held that the GPS tracking of Cunningham's vehicle was a search under the Fourth Amendment.[210] However, the court declared (correctly) that *Jones* did not resolve the separate question of "when, if ever, a GPS search is permissible in the absence of a search warrant," recognizing further that the employment-specific framework set forth in *O'Connor v. Ortega* would govern.[211]

As in *O'Connor*, the court determined that the warrant requirement does not apply in the employment context, such that the failure to secure a warrant before attaching the GPS device to Cunningham's car was not dispositive.[212] Nevertheless, the court deemed the search unreasonable.[213] Applying the *O'Connor* framework, the court deemed the search justified at its inception because Cunningham's employer had "ample grounds to suspect him of submitting false time records."[214] However, the court deemed the search unreasonable in scope as it involved "excessively intrusive," round-the-clock surveillance of Cunningham's vehicle,[215] which encompassed "much activity with which the State had no legitimate concern—i.e., it tracked [Cunningham] on all evenings, on all weekends and on vacation[,]" capturing a great deal of purely private activity.[216]

In the most striking portion of the opinion, the court then addressed the fact that no evidence obtained from surveillance conducted *outside of business hours* was used against Cunningham in his disciplinary proceeding, and whether, in light of that fact, suppression of GPS data

207. *Cunningham*, 933 N.Y.S.2d at 434.

208. *Id.*

209. Brief for Petitioner at 10, *Cunningham*, 997 N.E.2d 468 (No. 2013-0123).

210. *Cunningham*, 997 N.E.2d at 471.

211. *Id.* (citing O'Connor v. Ortega, 480 U.S. 709, 722 (1987)) (finding that the New York Court of Appeals also applies the *O'Connor* test to analyze the constitutionality of searches conducted by public employers under the New York Constitution).

212. *Id.* at 472.

213. *Id.* at 473.

214. *Id.*

215. *Id.*

216. *Id.*

obtained *during business hours* was necessary.[217] On this point, the court reasoned:

> Ordinarily, when a search has exceeded its permissible scope, the suppression of items found during the permissible portion of the search is not required. But we hold that rule to be inapplicable to GPS searches like the present one, in light of the extraordinary capacity of a GPS device to permit "[c]onstant, relentless tracking of anything." Where an employer conducts a GPS search without making a reasonable effort to avoid tracking an employee outside of business hours, the search as a whole must be considered unreasonable. That conclusion concededly requires suppression of [all] GPS evidence here. . . .[218]

When read in light of *Quon* (the text message case described in Part I.A. above), the New York Court of Appeals' decision in *Cunningham* seems incorrect, but the decision becomes more defensible when viewed through the lens of the concurring opinions in *Jones*. Both *Quon* and *Cunningham* involved employer-initiated investigations of potential work misconduct by an employee.[219] In both cases, the employee was either deemed or assumed to have a legitimate expectation of privacy under the circumstances of the case, making the reasonableness of the employer's actions the controlling issue.[220] Moreover, the courts in both cases ruled that the employer's investigatory action was reasonable at its inception given the employer's reasonable suspicion that the search would uncover evidence of work misconduct.[221] The opinions thus differed only on the final step of the *O'Connor* analysis: whether the employer's investigatory conduct was reasonable in scope.[222]

In *Quon*, a Supreme Court opinion that should control Fourth Amendment employer-search cases like *Cunningham*, the Court deemed the review of the employee's text messages reasonable in scope because of the limited nature of the review, including the fact that evidence of the employee's activities while off duty was redacted from his disciplinary proceedings.[223] Arguably the same result should have been reached in *Cunningham*, as the data obtained from the times when Cunningham was

---

217. *Id.*

218. *Id.* at 473 (citations omitted) (citing United States v. Martell, 654 F.2d 1356, 1361 (9th Cir. 1981); United States v. Clark, 891 F.2d 501, 505 (4th Cir. 1989); Boyd v. Constantine, 613 N.E.2d 511, 511 (N.Y. 1993)).

219. City of Ontario v. Quon, 560 U.S. 746, 750 (2010); *Cunningham*, 997 N.E.2d at 470.

220. *Quon*, 560 U.S. at 750; *Cunningham*, 997 N.E.2d at 472.

221. *Quon*, 560 U.S. at 761; *Cunningham*, 997 N.E.2d at 473.

222. *Quon*, 560 U.S. at 761; *Cunningham*, 997 N.E.2d at 473.

223. *Quon*, 560 U.S. at 762.

off duty had been redacted from his disciplinary proceedings.[224] Yet, the *Cunningham* court did not follow *Quon* on this point, and instead deemed the search unreasonable in its entirety.[225] The *Cunningham* court's departure from *Quon* is likely due to the same underlying concerns with respect to GPS tracking that troubled the concurring Justices in *Jones*—namely, the potential for GPS tracking to unveil vast amounts of private information that realistically could not be obtained through traditional means of surveillance, such as trailing a vehicle turn-by-turn.[226] For employers, then, the obvious lesson from *Cunningham* is to limit their use of GPS tracking to investigations of employees that are based on a reasonable suspicion of wrongdoing, and to avoid collecting GPS data not truly necessary to corroborate that suspicion.

From an employer perspective, the most important issue with respect to GPS tracking of an employee concerns the permissible length of surveillance, as there is no doubt that in light of *Jones*, GPS tracking by way of surreptitiously installed GPS triggers Fourth Amendment protection.[227] As courts and commentators have recognized, the Supreme Court in *Jones* did not resolve the question of whether *long-term* GPS surveillance is unconstitutional, particularly in cases where GPS tracking is accomplished in the absence of a trespass.[228] In the employment

224. *Cunningham*, 997 N.E.2d at 473.

225. *Id.*

226. United States v. Jones, 565 U.S. 400, 415–16 (2012) (Sotomayor, J., concurring) ("GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations. . . . The government can store such records and efficiently mine them for information years into the future."); *see also Cunningham*, 997 N.E.2d at 474 (Abdus-Salaam, J., concurring) (recognizing that GPS is vastly more intrusive than simply following a car, and stating that "GPS is not a mere enhancement of human sensory capacity," given that it permits tracking and data capture over "a practically unlimited period," and that "[t]he potential for a similar capture of information or 'seeing' by law enforcement would require, at a minimum, millions of additional police officers and cameras on every street lamp" (quoting People v. Weaver, 909 N.E.2d 1195, 1199 (N.Y. 2009))).

227. *Jones*, 565 U.S. at 404.

228. *See id.* at 412 ("It may be that achieving the same result through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy, but the present case does not require us to answer that question."); *see also* United States v. Garcia-Gonzalez, No. 14-10296-LTS, 2015 WL 5145537, at *3 (D. Mass. Sept. 1, 2015) (recognizing that legality of longer-term video surveillance of an individual's home or activities was not resolved in *Jones*); United States v. Brooks, 911 F. Supp. 2d 836, 842 (D. Ariz. 2012) (recognizing that *Jones* left open for "some future case" the question whether the Supreme Court "is willing to accept the principle that Government surveillance can implicate an individual's reasonable expectation of privacy over time"); State v. Jones, 903 N.W.2d 101, 113 (S.D. 2017) ("[T]his case concerns long-term, remote surveillance, and there is no controlling law on that question."); Carniol v. N.Y.C. Taxi & Limousine Comm'n, 975 N.Y.S.2d 842, 849 (N.Y. Sup. Ct. 2013) ("[T]he Court [in *Jones*]

context, this same length-of-surveillance issue resurfaces in the question of what makes an instance of GPS tracking unreasonable in scope.[229]

Although the following proposals will be outlined more fully below, for instances in which employees are suspected of work-related misconduct, this Article proposes that the best approach for employers to follow—one that accounts for the concerns of the concurring Justices in *Jones* and of the entire *Cunningham* court—is to track an employee via GPS only as a means of corroborating an allegation of serious employee misconduct. Even then, an employer should utilize this technique only after exhausting alternative investigation methods, and only to the extent necessary to justify an adverse employment action against the offending employee. To further account for the concerns of the *Cunningham* court, which emphasized the need for an employer to "mak[e] a reasonable effort to avoid tracking an employee outside of business hours,"[230] an employer should seek to avoid uncovering purely private activity unconnected to work obligations by, for example, shutting off the GPS tracking device during nonworking hours. Finally, from a temporal standpoint, the employer should only track an employee's vehicle long enough to obtain the information necessary to corroborate a suspicion of wrongdoing.

Borrowed from the criminal context, this proposed framework finds support in the Supreme Court's framework for elevating an allegation of wrongdoing through corroboration of an informant's tip, one that if applied by employers, would minimize their potential liability by limiting the intrusiveness of this investigative device.

The Supreme Court's corroboration-based framework derives largely from its decision in *Illinois v. Gates*,[231] which the Court applied in the context of establishing probable cause[232] and expanded, in *Alabama v. White*,[233] to encompass circumstances where the lesser standard of reasonable suspicion is required to conduct a less intrusive search or seizure.[234] The investigations in both *Gates* and *White* began with a tip from an anonymous informant.[235] Because an anonymous informant's tip

---

merely determined that such GPS monitoring was a search but it did not address whether the search was reasonable."), *aff'd*, 2 N.Y.S.3d 337 (N.Y. App. Div. 2015).

229. *See Cunningham*, 997 N.E.2d at 473 (deeming an instance of GPS tracking by an employer unreasonable due to its duration).

230. *Id.*

231. 462 U.S. 213, 246 (1983).

232. *See id.* at 230.

233. 496 U.S. 325 (1990).

234. *See id.* at 328–29.

235. *Gates*, 462 U.S. at 225; *White*, 496 U.S. at 326–27.

is usually insufficient to establish probable cause,[236] police must typically corroborate certain aspects of the tip in order to conduct a more extensive search or seizure via warrant.[237]

Prior to *Gates* and *White*, Supreme Court precedent had been read to require police to ascertain both the tipster's "basis of knowledge"(typically consisting of details regarding exactly how the tipster obtained the provided information) as well as his or her "veracity" or "reliability"(usually established through evidence that the informant is credible or reliable).[238] Abandoning that so-called "two-pronged test," the Court in *Gates* ruled that probable cause could be established via an informant's tip through a "totality of the circumstances" approach,[239] one that accounts for the fact that "[i]nformants' tips . . . come in many shapes and sizes"[240] and ultimately recognizes that a deficiency in either the "reliability" or "basis of knowledge" prong may be compensated for by a strong showing as to the other, or even by some other indicia of reliability.[241] The Court noted, for example, that if a particular informant is known for the unusual reliability of his predictions of certain types of illegal activity, his failure to thoroughly explain the basis of his knowledge in a particular case should not serve as an absolute bar to a finding of probable cause based on the tip.[242]

The true significance of *Gates*, insofar as employers are concerned, is the Court's recognition of the vital role that independent corroboration of an allegation of wrongdoing plays in developing the suspicion necessary to conduct a Fourth Amendment search or seizure.[243] As the *Gates* Court recognized, ordinary persons "generally do not provide extensive recitations of the basis of their everyday observations," and "the veracity of persons supplying anonymous tips is by hypothesis largely unknown, and unknowable," yet many of those tips, "particularly when supplemented by independent police investigation," are necessary tools for solving "otherwise 'perfect crimes.'"[244] From there, the Court readily determined that independent corroboration of the details of an

236. *See Gates*, 462 U.S. at 227 (agreeing that standing alone, the anonymous letter sent to the police in that case would not provide the basis for a magistrate's determination that probable cause existed).

237. *See id.* at 241–46 (discussing the importance of corroboration).

238. *Id.* at 227–29 (discussing the Illinois Supreme Court's interpretation of the Court's prior precedent on this issue: Spinelli v. United States, 393 U.S. 410 (1969), *abrogated by Gates*, 462 U.S. 213; Aguilar v. Texas, 378 U.S. 108 (1964), *abrogated by Gates*, 462 U.S. 213).

239. *Gates*, 462 U.S. at 230, 238.

240. *Id.* at 232.

241. *Id.* at 214, 233.

242. *Id.* at 233.

243. *Id.* at 241.

244. *Id.* at 237–38.

informant's tip could elevate a facially deficient allegation of wrongdoing into one that rises to the level of probable cause.[245]

More relevant to the employment context, which dispenses with the requirement of probable cause, the *Gates* corroboration framework was later expanded to cases involving reasonable suspicion, a lesser standard of suspicion often applied in the employment context.[246] The Court considered this issue in *Alabama v. White*.[247]

In *White*, an anonymous informant called police and stated that a person named Vanessa White would be leaving a specific apartment (235-C) in a specific apartment building (235), at a specific time, in a brown Plymouth station wagon with a broken right taillight; the informant added that White would then drive to a certain motel in possession of an ounce of cocaine in a brown attaché case.[248] Officers went immediately to the apartment building and observed a station wagon that fit the informant's description.[249] Officers then saw a woman exit apartment building 235, but, they did not verify exactly which apartment unit the woman exited from.[250] Further, the officers did not observe a brown attaché case; the woman appeared empty-handed.[251] At this point, the woman entered the station wagon and began to drive in the direction of the motel specified by the informant.[252] Officers stopped the station wagon before it reached the motel and informed the driver, White, that she had been stopped because she was suspected of carrying cocaine in the vehicle.[253] Officers then obtained White's consent to search the vehicle, where they found a brown attaché case, which they opened with her consent.[254] Inside the case, officers discovered marijuana, prompting White's arrest on marijuana charges.[255]

In her ensuing prosecution, White argued that the brief investigatory stop of her vehicle was unsupported by reasonable suspicion, such that the marijuana found in her vehicle had to be suppressed.[256] When White's Fourth Amendment claim reached the Supreme Court, the Court addressed the issue of whether the corroborated tip "exhibited sufficient

245. *Id.* at 241–44.
246. *See supra* note 80 and accompanying text.
247. 496 U.S. 325, 328–29 (1990).
248. *Id.* at 327.
249. *Id.*
250. *See id.*
251. *Id.*
252. *Id.*
253. *Id.*
254. *Id.*
255. *Id.*
256. *See* White v. State, 550 So. 2d 1074, 1075, 1079 (Ala. Crim. App. 1989), *writ denied*, 550 So. 2d 1081 (Ala. 1989), *and rev'd*, 496 U.S. 325 (1990).

indicia of reliability to provide reasonable suspicion" to stop White's vehicle.[257] Although this particular investigatory stop required only reasonable suspicion, rather than probable cause,[258] the Court analyzed the issue using the same corroboration-based framework used in *Gates*.[259]

Similar to the tip in *Gates*, the Court noted that the tip in *White* provided virtually no information regarding the tipster's reliability, nor did it provide any indication of the basis for the tipster's knowledge regarding White's criminal activities.[260] As such, the tip alone would not have justified the *Terry* stop of White's vehicle.[261] Yet, as in *Gates*, police corroborated many aspects of the tip, including the fact that a vehicle fitting the tipster's description was parked outside the described apartment building; a woman fitting the tipster's description came out of the specified apartment building (rather than the particular apartment); the woman got into the car and drove in the direction of the motel, as the tipster had predicted; and this all occurred within the time frame specified by the informant.[262]

This corroboration of seemingly innocent details is significant, in the Court's words, "because [if] an informant is shown to be right about some things, he is probably right about other facts that he has alleged, including the claim that the object of the tip is engaged in criminal activity."[263] This corroboration, therefore, "imparted some degree of reliability to the other allegations made by the caller."[264] In addition, the Court noted that although the tip in *White* was not as detailed as the one in *Gates*, and although the corroboration was not as complete in *White* as in *Gates*, the required degree of suspicion in *White*—reasonable suspicion as opposed to probable cause—was also not as high.[265] Finally, the Court emphasized that, in *White*, as in *Gates*, the tip included details regarding the suspect's future actions not easily predicted by members of the general public who do not possess "inside information" about the suspect's future affairs. This information included the fact that White would shortly leave the apartment building, get in the car, and drive in the direction of the motel.[266] This accurate prediction of White's future activities thus made

257. *White*, 496 U.S. at 326–27.

258. *Id.* at 328 (citing Terry v. Ohio, 392 U.S. 1 (1968)).

259. *See id.* at 328–29.

260. *Id.* at 329.

261. *Id.* ("Simply put, a tip such as this one, standing alone, would not '"warrant a man of reasonable caution in the belief" that [a stop] was appropriate.'" (alteration in original) (quoting *Terry*, 392 U.S. at 22)).

262. *Id.* at 331.

263. *Id.* (citing Illinois v. Gates, 462 U.S. 213, 244 (1983)).

264. *Id.* at 332.

265. *Id.* at 329.

266. *Id.* at 332.

it "reasonable for police to believe that a person with access to such information is likely to also have access to reliable information about that individual's illegal activities."[267] In the end, such corroboration of an otherwise deficient tip gave police "reason to believe not only that the caller was honest but also that he was well informed, at least well enough to justify the stop."[268]

In the employment context, similar to cases like *Gates* and *White*, allegations of employee wrongdoing are often initiated by laypersons rather than professional investigators, and are then investigated further by company officials.[269] For relatively small employers, these complainants may be "known" to the investigating officials, and although this may not be the case may not be in larger corporations, in either event complainants' "reliability" and "basis of knowledge" will often be central to the investigation.[270] Such a scenario may arise, for example, in workplace harassment cases, and may also arise in other instances of alleged employee wrongdoing that might prompt an investigator to utilize methods of employee tracking, such as falsifying time sheets.[271]

Although an informant's reliability and basis of knowledge will not always be at issue in the employment context, the important point is that when an investigation is initiated based upon the report of an aggrieved coworker or customer, or even based upon an anonymous individual's complaint, the corroboration principles espoused in cases like *Gates* and *White* would serve as a useful guide to employers.

For investigations of alleged workplace misconduct, this Article proposes that to be reasonable at its inception, an employer should track an employee by surreptitiously installed GPS only if the employee under investigation has allegedly committed a terminable offense, and only if the employer has been unable to corroborate an allegation of employee wrongdoing through some other means. Finally, this Article proposes that

267. *Id.*

268. *Id.*

269. *See, e.g.*, Leventhal v. Knapek, 266 F.3d 64, 68 (2d Cir. 2001) (analyzing an employer search of an employee's workplace computer to investigate alleged workplace misconduct first reported by an anonymous informant); *see also* Smith v. White, 666 F. Supp. 1085, 1089–90 (E.D. Tenn. 1987), *aff'd*, 857 F.2d 1475 (6th Cir. 1988) (recognizing that in an employment context,"[r]easonable suspicion may be based on statements made by other employees and tips from informants").

270. *See, e.g.*, Benavidez v. City of Albuquerque, 101 F.3d 620, 625 (10th Cir. 1996) (discussing a challenge to a known informant's reliability in the context of establishing the reasonable suspicion necessary to perform employment-related drug tests); Reeves v. Singleton, 994 S.W.2d 586, 592 (Mo. Ct. App. 1999) (finding no reasonable suspicion based on an uncorroborated anonymous tip identifying plaintiff-employee as a drug user).

271. *See generally* Greer v. McCormick, No. 14-CV-13596, 2017 WL 1315718, at *15–20 (E.D. Mich. Apr. 10, 2017) (discussing the importance of corroborating an anonymous informant's tip in the employment context).

this form of GPS tracking should be limited to scenarios where it would be reasonable to believe that tracking the employee would in fact corroborate a report of employee wrongdoing. For example, if an employee is reported to have harassed a coworker at work, tracking the alleged wrongdoer outside of work would not be reasonable. If, however, an employee is reported to have harassed a coworker by stalking her after work hours at a local gym, GPS tracking might be a reasonable means of corroborating those allegations.[272] In combination, these requirements will ensure that employees suspected of committing relatively minor offenses are not subjected to this intrusive form of investigation, which will only be used by an employer when truly necessary.

Regarding the separate *O'Connor* requirement of being reasonable in scope, this Article proposes that once employed, GPS tracking of an employee should avoid uncovering purely private activity unconnected to work obligations or alleged workplace misconduct and should not extend any longer than truly necessary to corroborate the suspected wrongdoing. These principles are embedded in cases like *Quon* and *Cunningham*, which emphasize the obligation of employers to limit the scope of any employer-initiated investigation pursuant to the framework set forth in *O'Connor v. Ortega*,[273] and *Jones*, which reflects an acute concern for limiting the duration of such highly-invasive GPS tracking.

In sum, employers should consider surreptitious GPS tracking an ill-suited means of investigating most instances of employee wrongdoing. And even where the method may be appropriate, employers should utilize this highly intrusive investigative technique only as a last resort, and only insofar as is truly necessary to corroborate an allegation of serious misconduct.

Although the above proposals apply to employees' personal vehicles, this framework should generally remain the same when an employee is tracked in a company-owned vehicle via surreptitiously installed GPS. Although it is true that expectations of privacy in the employment context may shift depending on who owns the property subject to intrusion,[274]

---

272. *Cf.* CONN. GEN. STAT. § 31-48d(b)(2) (2018) (establishing an exception to a statutory requirement that an employer must provide written notice to any potentially affected employees prior to engaging in electronic monitoring on the employer's premises for situations "[w]hen (A) an employer has reasonable grounds to believe that employees are engaged in conduct which (i) violates the law, (ii) violates the legal rights of the employer or the employer's employees, or (iii) creates a hostile workplace environment, and (B) electronic monitoring may produce evidence of this misconduct, the employer may conduct monitoring without giving prior written notice").

273. *See* City of Ontario v. Quon, 560 U.S. 746, 761–63 (2010); Cunningham v. N.Y. Dep't of Labor, 997 N.E.2d 468, 472–73 (N.Y. 2013).

274. *See, e.g.*, United States v. Simons, 206 F.3d 392, 398 (4th Cir. 2000) (finding no legitimate expectation of privacy in employee's Internet use when employer's known policy allowed monitoring of "all file transfers, all websites visited, and all e-mail messages"); United

this factor will more likely alter the outcome when ownership is accompanied by notice and employee consent.[275] Notice and consent are not present, however, when a GPS device is secretly used to track an employee through the type of surreptitious installation that occurred in *Cunningham* and *Jones*.[276]

When notice and consent are present, courts have rejected privacy-based claims where an employer attaches a GPS tracking device to an employer-owned vehicle and uses that device to track the vehicle's movements, albeit often in cases not involving investigations of individual employee misconduct, as where an employer's entire fleet of vehicles are tracked via GPS.[277] Employer ownership has also played a role in cases involving investigations of employee wrongdoing. In one such case, *Elgin v. St. Louis Coca-Cola Bottling Co.*,[278] the court granted summary judgment to an employer on an intrusion claim that was brought against the employer after the employer surreptitiously attached a GPS device to its company-owned van, which was driven by the plaintiff, to investigate potential employee theft.[279] The *Elgin* court found no "substantial intrusion upon [the] plaintiff's seclusion" because the GPS tracker "revealed no more than highly public information as to the van's location."[280] In addition, the court declared that "defendant's use of the tracking device on its own vehicle does not rise to the level of being highly offensive to a reasonable person."[281]

States v. Hamilton, 778 F. Supp. 2d 651, 654 (E.D. Va. 2011) (finding that public school employee lacked a reasonable expectation of privacy in e-mails between him and his wife that were stored on his work computer because he was on notice that contents of his computer were subject to inspection, which he acknowledged).

275. *See, e.g.*, *Simons*, 206 F.3d at 398 (finding no legitimate expectation of privacy in employee's Internet use when employer's known policy allowed monitoring of "all file transfers, all websites visited, and all e-mail messages"); *Hamilton*, 778 F. Supp. 2d at 654 (finding that public school employee lacked a reasonable expectation of privacy in e-mails between him and his wife that were stored on his work computer because he was on notice that contents of his computer were subject to inspection, which he acknowledged).

276. *See* United States v. Jones, 565 U.S. 400, 403 (2012) (noting that law enforcement officers "installed a GPS tracking device on the undercarriage" of a vehicle to track a suspect's movements); *Cunningham*, 997 N.E.2d at 470 (stating that investigators covertly attached a GPS device to an employee's car).

277. *See, e.g.*, Tubbs v. Wynne Transp. Servs. Inc., No. H-06-0360, 2007 WL 1189640, at *2, *10 (S.D. Tex. Apr. 19, 2007) (finding no viable invasion of privacy claim where plaintiff's employer-owned commercial truck was outfitted with a GPS device that regularly transmitted the truck's location to the employer, which the employer used to determine whether its drivers were exceeding legal limitations on the number of hours they could drive).

278. No. 4:05CV970-DJS, 2005 WL 305063 (E.D. Mo. Nov. 14, 2005).

279. *Id.* at *1.

280. *Id.* at *4.

281. *Id.*

The result in *Elgin* is striking because the employer in that case tracked the van driven by the plaintiff in order to investigate cash shortages in machines the plaintiff serviced (a potentially criminal offense), and did not notify the plaintiff that it had done so until after he had been cleared of any wrongdoing,[282] such that notice and consent did not factor into the court's decision.[283] Nevertheless, because *Elgin* was decided several years before *Jones*, in an era in which most courts had drastically downplayed the privacy concerns inherent in surreptitious forms of GPS tracking,[284] the case does not compel alteration of the framework proposed above. In the end, employer ownership is just one of many factors to consider in any given investigation and does not in and of itself dictate Fourth Amendment outcomes.[285]

B. *GPS Tracking of a Segment of Employees for Legitimate Business Reasons*

Having established a framework for employers to follow when investigating employee wrongdoing, this Article next examines GPS tracking for noninvestigatory work-related purposes.[286]

In Fourth Amendment jurisprudence, individualized suspicion is generally required to make someone the target of a Fourth Amendment search or seizure, particularly when performed as part of a criminal investigation.[287] Given the historical development of the Fourth Amendment right——which was arguably created to prevent wide-ranging searches through the use of general warrants[288]——so-called

---

282. *See id.* at *1.

283. *See id.* at *4.

284. *See supra* note 141 and accompanying text.

285. Demonstrating that the ownership factor alone does not determine expectations of privacy, courts have sometimes ruled that an employee enjoys Fourth Amendment protection in an employer-owned device, and on the other hand have found no Fourth Amendment protection in a personally-owned device. *Compare, e.g.*, United States v. Barrows, 481 F.3d 1246, 1248–49 (10th Cir. 2007) (finding employee had no reasonable expectation of privacy in the contents of a personal computer he used at work), *with, e.g.*, United States v. Yudong Zhu, 23 F. Supp. 3d 234, 236, 238–39 (S.D.N.Y. 2014) (finding plaintiff could reasonably expect privacy in his work computer even though the computer was formally owned by his employer).

286. *See* O'Connor v. Ortega, 480 U.S. 709, 723 (1987) (adopting a framework for analyzing searches performed for "either a noninvestigatory work-related" purpose or to investigate "suspected work-related employee misfeasance").

287. *See, e.g.*, United States v. Kincade, 379 F.3d 813, 821–36 (9th Cir. 2004) (discussing the requirement of individualized suspicion in Fourth Amendment case law, including cases in which the requirement has been abandoned).

288. *See* Tracey Maclin, *Let Sleeping Dogs Lie: Why the Supreme Court Should Leave Fourth Amendment History Unabridged*, 82 B.U. L. REV. 895, 941 (2002) ("Although the [Fourth] Amendment's text bans only general warrants, the 'larger purpose for which the Framers adopted the text [was] to curb the exercise of discretionary authority by officers.'" (alteration in original)

"fishing expeditions for evidence" are generally considered unconstitutional, particularly those performed without individualized suspicion of wrongdoing.[289]

Given these fundamental Fourth Amendment principles, any employer program that subjects a large segment of employees to continual GPS surveillance should be used with caution. Yet, as with other "special needs" scenarios involving widespread searches, such as airport security screenings, an investigative method is not automatically unreasonable simply because it is applied to a large number of individuals in the absence of individualized suspicion.[290] Given that employer-initiated searches generally fall into this special needs category, GPS tracking of a segment of employees might be reasonable, particularly when performed for legitimate "work-related, noninvestigatory reasons" apart from any investigation into workplace misconduct, even where the data obtained is later used to discipline an individual employee.[291]

(quoting Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 MICH. L. REV. 547, 553, 555 (1999)). *But see* Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 771–72 (1994) (arguing that the Fourth Amendment contains no actual warrant requirement and that "at times, the Founders viewed judges and certain judicial proceedings with suspicion," adding that "[t]he Amendment's Warrant Clause does not require, presuppose, or even encourage warrants—it *limits* them" by imposing strict standards on their issuance). *Contra* Davies, at 591–619 (rejecting Amar's reasonableness view of the Fourth Amendment as "based in large measure on erroneous historical premises").

289. *See* Messerschmidt v. Millender, 565 U.S. 535, 560, 566 (2012) (Sotomayor, J., dissenting) (reviewing the purpose of the Fourth Amendment's warrant clause of protecting against general searches and complaining that officers, by their own admission, engaged in a "fishing expedition for evidence of unidentified criminal activity committed by unspecified persons," which "was the very evil the Fourth Amendment was intended to prevent"); *see also* Steagald v. United States, 451 U.S. 204, 220 (1981) ("The central objectionable feature of both [the general warrants that had occurred in England and of the writs of assistance used in the Colonies] was that they provided no judicial check on the determination of the executing officials that the evidence available justified an intrusion into any particular home.").

290. *See, e.g.*, Chandler v. Miller, 520 U.S. 305, 323 (1997) ("[W]here the risk to public safety is substantial and real, blanket suspicionless searches calibrated to the risk may rank as 'reasonable'—for example, searches now routine at airports and at entrances to courts and other official buildings."); *see also* United States v. Edwards, 498 F.2d 496, 500 (2d Cir. 1974) ("When the risk is the jeopardy to hundreds of human lives and millions of dollars of property inherent in the pirating or blowing up of a large airplane, the danger *alone* meets the test of reasonableness, so long as the search is conducted in good faith for the purpose of preventing hijacking or like damage and with reasonable scope and the passenger has been given advance notice of his liability to such a search so that he can avoid it by choosing not to travel by air." (quoting United States v. Bell, 464 F.2d 667, 675 (2d Cir. 1972) (Friendly, C.J., concurring))).

291. *See* O'Connor v. Ortega, 480 U.S. 709, 723 (1987) (stating that the reasonableness inquiry would not be particularly rigorous and that public employers should be afforded "wide latitude to enter employee offices for work-related, noninvestigatory reasons").

Another recent New York case, *Carniol v. The New York City Taxi and Limousine Commission*,[292] illustrates these principles.

In *Carniol*, petitioner Robert Carniol sued The New York City Taxi and Limousine Commission (TLC), arguing that the city's use of GPS technology to track its taxi drivers violated the New York Constitution, and that the fruits of that violation could not be used as evidence in disciplinary actions against individual taxi drivers.[293] According to Carniol's complaint, the TLC mandated in 2007 that all New York City medallion taxi cabs be equipped with a Taxi Technology System (TTS) that included a GPS system.[294] As originally developed, the intent of the TTS system was to collect information for the TLC's regulatory analysis. The goals were to gather data regarding pick-up and drop-off points, to assess trip time and distance, to eliminate the need for drivers to complete handwritten trip sheets, and to assist in locating a passenger's lost property.[295] Given its administrative purposes, the TLC never stated that it would use the information it gathered for investigatory purposes.[296] Yet, after receiving complaints that passengers were being overcharged by a certain driver, the TLC conducted a comprehensive review of the data generated by the TTS system for essentially all of its 42,000 cab drivers, including Carniol.[297] As a result, the TLC determined that more than 21,000 drivers, including Carniol, had overcharged passengers by charging the higher out of town rate for trips within New York City.[298]

Having determined that Carniol had overcharged passengers ninety-one times, the TLC commenced an administrative proceeding to revoke his TLC license.[299] Following a trial, an Administrative Law Judge issued a report and recommendation finding Carniol guilty of the charges against him and recommending revocation of his license.[300] The judge specifically found that Carniol had no reasonable expectation of privacy in the trip information gathered by the TLC, which had properly searched the records it lawfully possessed.[301] Shortly thereafter, Carniol's taxi driver's license was revoked.[302]

---

292. 975 N.Y.S.2d 842 (N.Y. Sup. Ct. 2013), *aff'd*, 126 A.D.3d 409 (N.Y. App. Div. 2015).
293. *Id.* at 844.
294. *Id*.
295. *Id.* at 844–45.
296. *Id.* at 845.
297. *Id.*
298. *Id.*
299. *Id.*
300. *Id.*
301. *Id.*
302. *Id.* at 846.

Carniol subsequently challenged the revocation, arguing that the TLC's use of GPS tracking violated his Fourth Amendment rights.[303] As an initial matter, the New York Supreme Court recognized that individuals "who choose to participate in a heavily regulated industry, such as the taxicab industry, have a diminished expectation of privacy, particularly in information related to the goals of the industry regulation,"[304] such that Carniol could not legitimately expect privacy in the trip data that had been gathered by GPS.[305]

The court went on to find that even if it assumed that Carniol could expect privacy, the TLC's GPS tracking program would have been "reasonable" in light of the competing interests at stake.[306] According to the court, Carniol's "privacy interest" in the GPS-generated trip data is "minimal," and the "intrusion is also minimal," given that "[i]t does not involve a physical intrusion into Carniol's body or home" and does not collect data regarding his whereabouts while off-duty.[307] When weighed against the "substantial" "government interest in improving taxi customer service and [the] ability to regulate it by using modern methods to promote passenger and driver safety," the court had no difficulty finding the TLC's actions reasonable.[308] Distinguishing *Jones*, which involved the surreptitious and trespassory attachment of a GPS device to a criminal suspect's vehicle, the court further noted that the GPS monitoring here was conducted with the knowledge and consent of the taxi driver and "was narrowly tailored to achieve a regulatory goal."[309] The court then re-emphasized that the GPS system did "not record information about the driver's personal life."[310] Accordingly, even if Carniol could legitimately expect privacy in the GPS data, the search would have been reasonable.[311]

For purposes of the instant analysis, five things are noteworthy regarding *Carniol*. First, because the GPS system at issue was installed with the knowledge and consent of the city's taxi drivers, the use of that system was not governed by *Jones*, leaving only the question of whether a "search" occurred pursuant to the *Katz* reasonable expectation of

303. *Id.* (noting that Carniol also brought a similar state law claim).

304. *Id.* at 848 (quoting Buliga v. N.Y.C. Taxi Limousine Comm'n, No. 07 Civ. 6507 (DLC), 2007 WL 4547738, at *2 (S.D.N.Y. Dec. 21, 2007)).

305. *Id.*

306. *Id.* at 848–49 (quoting *Buliga*, 2007 WL 4547738, at *3).

307. *Id.* at 849.

308. *Id.*

309. *Id.*

310. *Id.*

311. *Id.*

privacy test.[312] Second, taxi drivers subject to GPS monitoring could not reasonably expect privacy under *Katz*, at least in part because of their consent.[313] Third, that same consent contributed to the court's ultimate determination that the employer's wholesale GPS monitoring of its taxi drivers was reasonable.[314] Fourth, the legitimate government interests at issue—to regulate and improve the taxi industry and to enhance the safety and convenience of the driver and the passengers—tilted the scale of reasonableness in the employer's direction.[315] Finally, the fact that no data was collected regarding Carniol's personal life, including his off duty whereabouts, made the GPS surveillance relatively unintrusive, and hence more likely to be deemed reasonable.[316]

Carniol's combination of employee consent to the GPS monitoring program, the existence of legitimate business purposes necessitating the use of GPS, and the employer's decision not to collect GPS data while employees are off duty, are in essence the key guidelines for employers to follow in using across-the-board GPS tracking programs. When adopted, these ingredients will ensure both that the monitoring remains reasonable at its inception (that is, based upon employee consent and performed for a legitimate business reason) and reasonable in scope (that is, not excessively intrusive given that it does not encompass off-duty activity).[317] Moreover, *Carniol* reveals that when an employer tracks an entire segment of employees in a reasonable manner through GPS, the employer may then utilize the GPS data it acquires to discipline individual employees for misconduct that data reveals.[318] Quite simply,

312. *See id.*; *see also* United States v. Jones, 565 U.S. 400, 411 (2012) ("Situations involving merely the transmission of electronic signals without trespass would *remain* subject to *Katz* analysis.").

313. *Carniol*, 975 N.Y.S.2d at 848 (emphasizing that the taxicab industry is heavily regulated, which reduces expectations of privacy, and that "the TTS system was installed with the knowledge of the taxicab owners and all taxicab drivers are required to follow TLC regulations which mandate the use of the TTS system").

314. *See id.* at 848–49.

315. *See id.* at 849.

316. *See id.*

317. *See* O'Connor v. Ortega, 480 U.S. 709, 725–26 (1987).

318. *See Carniol*, 975 N.Y.S.2d at 845–46, 851; *see also* Tubbs v. Wynne Transp. Servs. Inc., No. H-06-0360, 2007 WL 1189640, at *10 (S.D. Tex. Apr. 19, 2007) (finding no viable invasion of privacy claim where plaintiff's employer-owned commercial truck was outfitted with a GPS device that regularly transmitted the truck's location to the employer, which the employer used to determine whether its drivers were exceeding legal limitations on the number of hours they could drive); Gerardi v. City of Bridgeport, 985 A.2d 328, 330 (Conn. 2010) (involving a case, dismissed on unrelated grounds, brought by city fire inspectors who were disciplined for improper job performance, "which was detected through the [employers'] use of global positioning system devices (GPS devices) without the [employees'] knowledge").

because the GPS tracking itself is not unlawful, the employer's subsequent use of its own GPS data is not unlawful either.[319]

The same variables present in *Carniol*—consent, legitimate business reasons, and narrow scope—are, in the author's view, the necessary ingredients of a lawful system of employer-initiated cell phone tracking, a topic addressed in the next section.

IV. TRACKING EMPLOYEES THROUGH THEIR CELL PHONES

This section examines the most common types of cell phone tracking that exist today. It then considers how employers may use cell phones to lawfully track the locations of their employees.

A. *Cell Phone Tracking Methods*

The Supreme Court's ruling in *Jones* generally requires law enforcement to obtain a warrant before attaching a GPS device to a suspect's vehicle as part of a criminal investigation.[320] As a result, law enforcement officials have turned to more sophisticated methods of location tracking, including tracking through cell phones.[321] Given that law enforcement can typically monitor a cell phone's location without having to commit a trespass upon it, this method of investigation is generally subject to fewer constitutional constraints as compared to the more traditional form of GPS tracking that occurred in *Jones* and *Cunningham*.[322]

Cell phone tracking by law enforcement comes in two primary forms. One common form occurs through the acquisition of cell site location data.[323] Under this method, which does not involve a trespass,[324] police

319. *See Carniol*, 975 N.Y.S.2d at 851 (denying Carniol's motion in its entirety).

320. *See* United States v. Jones, 565 U.S. 400, 404 (2012).

321. *See* Jonathan Bard, *Unpacking the Dirtbox: Confronting Cell Phone Location Tracking with the Fourth Amendment*, 57 B.C. L. REV. 731, 744 (2016) ("GPS devices remain a popular option for location tracking, but this attachment-based technology presents practical and legal obstacles. [As such,] [l]aw enforcement is increasingly turning to cell phone tracking as an appealing alternative to attachment-based tracking devices." (footnote omitted)).

322. *See* Christian Bennardo, *The Fourth Amendment, CSLI Tracking, and the Mosaic Theory*, 85 FORDHAM L. REV. 2385, 2396–401 (2017) (examining judicial trends in cell site location tracking cases).

323. *See* United States v. Davis, 785 F.3d 498, 502–03 (11th Cir. 2015) (describing this type of data).

324. *See id.* at 514 (distinguishing *Jones* on this point) ("The government's obtaining MetroPCS records, showing historical cell tower locations, did not involve a physical intrusion on private property or a search at all. The records belonged to a private company . . . [and] were obtained through a court order authorized by a federal statute, not by means of governmental trespass."); *see also* United States v. Wheeler, 169 F. Supp. 3d 896, 911 (E.D. Wis. 2016) ("The court concludes that the government's collection of cell tower location data from the cell phone provider does not constitute a 'search' under the Fourth Amendment [because] [t]he collection of

are able to obtain cell phone location data by identifying which cell tower communicated with the phone when the phone was used to make a call, send a text or e-mail, or engage in other data transmission functions.[325] When accumulated over a period of time, such cell site location data—which can be incredibly comprehensive given the number of times a typical cell phone is used each day—allows a person reviewing the data to infer both the phone's and the user's location at numerous times throughout the day.[326] Cell phone companies maintain records of this information,[327] making it possible for law enforcement to request either "historical" or "real-time" cell-site information.[328]

With historical cell-site information, law enforcement may request all such data accumulated over a period of time in the past, whereas with real-time data, law enforcement may seek to obtain this information on a real-time basis into the future.[329] In one recent robbery investigation, for example, the Government obtained 129 days of historical cell-site location information from one suspect's wireless providers. The Government then used this information as evidence of the suspect's seemingly incriminating location with respect to four robberies.[330]

Prior to June 2018, government officials generally did not need a warrant to acquire historical cell-site location data[331] as most courts had ruled that no Fourth Amendment "search" occurs in that instance, either under the trespass test or under the reasonable expectation of privacy

---

the data does not involve a trespass upon an individual's person or property, nor into a physical area in which the person has established a reasonable expectation of privacy.").

325. *See* Carpenter v. United States, 138 S. Ct. 2206, 2212 (2018).

326. *See id.* at 2217–19; *see also In re* Application of the U.S. for an Order Authorizing the Release of Historical Cell-Site Info., 809 F. Supp. 2d 113, 115 (E.D.N.Y. 2011) ("If a user's cell phone has communicated with a particular cell-site, this strongly suggests that the user has physically been within the particular cell-site's geographical range.").

327. *See Carpenter*, 138 S. Ct. at 2212; *In re* Application of the U.S. for Historical Cell Site Data, 724 F.3d 600, 611–12 (5th Cir. 2013) ("[C]ell site information is clearly a business record [because] [t]he cell service provider collects and stores historical cell site data for its own business purposes, perhaps to monitor or optimize service on its network or to accurately bill its customers for the segments of its network that they use."); *In re Application of the U.S. for an Order Authorizing the Release of Historical Cell-Site Info.*, 809 F. Supp. 2d at 115 ("By technical and practical necessity, cell-phone service providers keep historical records of which cell-sites each of their users' cell phones have communicated. The implication of these facts is that cellular service providers have records of the geographic location of almost every American at almost every time of day and night.").

328. *See* United States v. Jones, 908 F. Supp. 2d 203, 207 (D.D.C. 2012).

329. *See id.*

330. *See Carpenter*, 138 S. Ct. at 2212–13.

331. *See In re Application of U.S. for Historical Cell Site Data*, 724 F.3d at 615 (concluding that the government can seek judicial orders under the Stored Communications Act to obtain historical cell-site information on the basis of reasonable suspicion rather than probable cause).

test.[332] In finding no legitimate expectation of privacy in such data, most courts had invoked the Fourth Amendment's assumption of risk rationale, a principle that there can be no reasonable expectation of privacy in information knowingly disclosed to a third party, such as a cell phone provider.[333]

Overturning many of these decisions, in June 2018, the United States Supreme Court refused to apply the assumption of risk doctrine to historical cell-site location data in *Carpenter v. United States*.[334] It held that "an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through [cell-site location information],"[335] such that a Fourth Amendment search occurred when the FBI obtained detailed location information from a criminal suspect's wireless carriers.[336] The *Carpenter* Court specifically rejected the Government's attempt to extend the third-party assumption of risk doctrine to this type of cell phone data, explaining that "a detailed chronicle of a person's physical presence compiled every day, every moment, over several years," which can be obtained through the acquisition of historical cell site location data, "implicates privacy concerns far beyond" those at issue in the Supreme Court's previous

332. *See, e.g.*, United States v. Graham, 824 F.3d 421, 428 (4th Cir. 2016) (finding no Fourth Amendment search when police obtained historical cell-site location information (CSLI) from robbery suspects' cell phone provider where the historical CSLI indicated which cell tower—usually the one closest to the cell phone—transmitted a signal when the suspects used their cell phones to make and receive calls and texts), *abrogated by* United States v. Chavez, 894 F.3d 593 (4th Cir. 2018); *see also id.* at 428 (recognizing that the court's holding on the CSLI issue "accords with that of every other federal appellate court that has considered the Fourth Amendment question before us," and further noting that "the vast majority of federal district court judges" have determined that no "search" occurs when police obtain historical cell site location data); *In re Application of U.S. for Historical Cell Site Data*, 724 F.3d at 615 (reaching a similar result as *Graham*). *See generally* Bennardo, *supra* note 322 (examining judicial trends in cell-site location tracking cases and noting that four of the five federal circuit courts that have addressed whether cell phone customers have a reasonable expectation of privacy in CSLI have answered in the negative).

333. *See, e.g.*, United States v. Carpenter, 819 F.3d 880, 887–89 (6th Cir. 2016) ("[F]or the same reasons that Smith had no expectation of privacy in the numerical information at issue [in *Smith v. Maryland*, 442 U.S. 735 (1979)], the defendants have no such expectation in the [CSLI] locational information here"), *rev'd*, 138 U.S. 2206 (2018); *see also* United States v. Davis, 785 F.3d 498, 511–13 (11th Cir. 2015) ("[Defendant] has no objective[ly] reasonable expectation of privacy in MetroPCS's business records showing the cell tower locations that wirelessly connected [defendant's] calls."). *See generally* Smith v. Maryland, 442 U.S. 735, 742–44 (1979) (establishing, under the third-party assumption of risk doctrine, that an individual can claim "no legitimate expectation of privacy" in information that he has voluntarily turned over to a third party).

334. 138 S. Ct. at 2217.

335. *Id.*

336. *Id.*

third-party assumption of risk cases.[337] The *Carpenter* Court further emphasized that, unlike the Court's prior third-party cases, a cell phone user does "not truly share[]" the "trail of location data" routinely generated by his or her cell phone, and thus does not voluntarily assume the risk that such data will be compiled and transmitted to the government.[338]

Beyond cell-site location data, an alternative method of cell phone tracking is to utilize the phone's internal GPS.[339] Under this method, for example, cell phone providers may monitor a phone's location through its internal GPS and transmit that information to law enforcement anytime a user activates the GPS on her phone.[340] Law enforcement may also utilize this method without the cell phone provider's assistance.[341]

Finally, smartphone apps offer location tracking or sharing services, including, for example, Google Maps and Snapchat, and there are various websites that claim to allow users to find a phone's location.[342] As such, there are numerous ways in which an employee's location might be tracked via cell phone.

B. *Using Cell Phone Apps to Track Employees*

Of the various methods of cell phone tracking described in the previous section, employers are most likely to track an employee's cell

---

337. *See id.* at 2220.

338. *See id.*

339. Jeremy H. Rothstein, *Track Me Maybe: The Fourth Amendment and the Use of Cell Phone Tracking to Facilitate Arrest*, 81 FORDHAM L. REV. 489, 493–94 (2012). According to Rothstein, all cell phones sold since 2003 are GPS-enabled, making most phones today at least potentially trackable. *Id.* at 493. However, a user can disable her phone's GPS. *Id.* Moreover, whether a phone transmits GPS data may depend on the network and on the phone's applications. *Id.*

340. *See* United States v. Jones, 565 U.S. 400, 428–29 (2012) (Alito, J., concurring) (describing this method); *see also* United States v. Jones, No. 2:12CR30-MEF, 2012 WL 2568200, at *1 (M.D. Ala. June 15, 2012), *report and recommendation adopted*, No. 2:12-CR-030-MEF, 2012 WL 2568082 (M.D. Ala. July 3, 2012) (describing an investigation where police obtained a warrant to receive "pings" with the location of a suspect's cell phone for a thirty-day period, after which cell phone provider Sprint sent e-mails, directly to the officer's phone, containing longitudinal and latitudinal coordinates and a link to a map indicating the phone's location).

341. *See In re* Application of U.S. for Historical Cell Site Data, 724 F.3d 600, 615 (5th Cir. 2013) (refusing to "address situations where the Government surreptitiously installs spyware on a target's phone or otherwise hijacks the phone's GPS, with or without the service provider's help").

342. *See* United States v. Wheeler, 169 F. Supp 3d 896, 908 (E.D. Wis. 2016) (recognizing website and cell phone apps as location tracking methods); *see also* Brian X. Chen, *When You Should (and Shouldn't) Share Your Location Using a Smartphone*, N.Y. TIMES (July 12, 2017), https://www.nytimes.com/2017/07/12/technology/personaltech/using-location-sharing-apps.html [https://perma.cc/K92G-CKTD].

phone location through smartphone apps, including apps designed for human resources purposes and employers' individual apps. Many of the largest employers in the United States,[343] for example, have apps that can be downloaded from the Google Play Store that request access to a user's location information upon download.[344] Presumably, when a user consents to such data capture, the employer is capable of tracking the location of that user's phone.[345]

One popular timekeeping app, Humanity's "Time Clock," is designed to capture not only the times an employee is reportedly working, but also the location of an employee's cell phone every time she logs in and out of the app.[346] Every time a Time Clock user opens the app on her smartphone, before she can "Clock In," she is provided the following message: "Please enable GPS on your device, if it's not already turned ON, because it is required for clocking In and Out."[347] After the user clicks "Clock In," the app reminds the user that "'https://www.humanity.com' Would Like to Use Your Current Location."[348] When the user clicks "Ok," the app displays a map of the

343. *See* Alexander E.M. Hess, *The 10 Largest Employers in America*, USA TODAY (Aug. 22, 2013), https://www.usatoday.com/story/money/business/2013/08/22/ten-largest-employers/2680249/ [https://perma.cc/F9F5-9DGR] (reporting the 10 largest American employers, beginning with the largest, as Walmart, Yum! Brands, Inc., McDonald's Corp., International Business Machines (IBM), United Parcel Service, Inc. (UPS), Target Corp., Kroger Co., Home Depot Inc., Hewlett-Packard Co., and General Electric Co.); *see also* Jennifer Calfas, *The 6 Biggest Employers in the U.S. Right Now*, TIME (Apr. 27, 2017), http://time.com/money/4754123/biggest-us-companies/ [https://perma.cc/5EPU-2ZUE] (reporting the five largest employers in the United States, beginning with the largest, as Walmart, Kroger, Home Depot, IBM, and McDonald's).

344. On March 12, 2018, the author installed the apps of five of the largest U.S. employers on his Android smartphone: Walmart, Kroger, Home Depot, Target, and McDonald's. All five of those apps requested to track the location of the author's phone almost immediately upon install.

345. *See* BRUCE SCHNEIER, DATA AND GOLIATH: THE HIDDEN BATTLES TO COLLECT YOUR DATA AND CONTROL YOUR WORLD 3 (2015) (reporting that smartphone apps are often designed to permit transaction-based data collection and location tracking). *See generally* FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY (2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf [https://perma.cc/5V5W-QHVM] (reporting information and findings of the FTC in a study of nine data brokers regarding their practices related to the collection and use of consumer data).

346. *See Online Time Clock Software*, HUMANITY (2018) https://www.humanity.com/timeclock [https://perma.cc/6GB3-CCA5].

347. The author's wife, who works remotely, is required by her employer to use the Humanity "Time Clock" app every time she logs in to work. In March 2018, the author used the Time Clock app on his wife's iPhone to complete the login process, which is accurately described herein.

348. *See supra* note 347.

phone's nearby area and asks the user to confirm that the map accurately depicts her current location.[349]

Because there is no trespassory invasion of an employee's cell phone under these circumstances, gathering an employee's physical location through an app like Time Clock will trigger Fourth Amendment protection only if an employee can demonstrate a legitimate expectation of privacy in her use of the app,[350] an analysis that is fact-specific and based on the totality of circumstances in a given case.[351] In the employment context, expectations of privacy often depend on whether an employee has been notified of and consented to the monitoring at issue.[352] Where an employee has consented to a particular form of monitoring, it is nearly impossible for her to expect privacy in that action.[353] Moreover, even assuming a reasonable expectation of privacy exists, employee consent will impact the reasonableness of the employer's actions under the second step of Fourth Amendment analysis, and may alternatively impact whether the employer's action would be deemed "offensive" under the tort of intrusion upon seclusion.[354]

These consent-based principles likely apply to timekeeping apps that track a user's location, given that every time an employee logs in or out of apps like Time Clock, she willingly agrees to permit the tracking of her phone's location. Such consent will, in turn, eliminate any privacy-based claim the employee might assert. Coupled with the employee's consent, the third-party assumption of risk doctrine would likely prevent

---

349. *See supra* note 347.

350. *See* United States v. Jones, 565 U.S. 400, 411 (2012) ("Situations involving merely the transmission of electronic signals without trespass would remain subject to *Katz* analysis." (emphasis omitted)).

351. As one court put it, "when a defendant takes possession of a piece of property on which a GPS device has already been installed, the continued monitoring of [the] device" would not be a "search" of that particular defendant under the trespassory test, but may constitute a "search" of the defendant under the *Katz* reasonable-expectation-of-privacy test, depending, of course, on the specific facts of the case. United States v. Barraza-Maldonado, 879 F. Supp. 2d 1022, 1027–28 (D. Minn. 2012), *aff'd*, 732 F.3d 865 (8th Cir. 2013); *cf. Jones*, 565 U.S. at 430 (Alito, J., concurring) ("The best that we can do in this case is to apply existing Fourth Amendment doctrine and to ask whether the use of GPS tracking *in a particular case* involved a degree of intrusion that a reasonable person would not have anticipated." (emphasis added)).

352. *See supra* note 32 and accompanying text.

353. *See supra* note 32 and accompanying text.

354. *City of Ontario v. Quon*, 560 U.S. 746 (2010), illustrates the significance of consent in the employment context as it pertains to the Fourth Amendment's ultimate reasonableness inquiry. There, in finding the search of Quon's text messages reasonable, the Court reasoned, in part, that Quon had been informed his text messages were subject to auditing and thus had "received no assurances of privacy" in his pager messages. *Id.* at 761–62. This limited expectation of privacy "lessened the risk that the [city's] review would intrude on highly private details of Quon's life," making it relatively unintrusive. *Id.* at 762–63.

an employee from claiming a reasonable expectation of privacy in such data when it has been willingly conveyed in this particular manner, as it would be difficult for an employee to argue that such information had not been voluntarily conveyed to her employer through the timekeeping app, which has an obvious purpose of collecting employment-related data.[355] Given this combination of consent and assumption of risk, tracking an employee's location through a timekeeping app is generally not unlawful.[356]

Finally, because wholesale employee tracking for timekeeping purposes replaces traditional methods of clocking in and clocking out that have been used for decades, it constitutes a form of tracking for non-investigatory, work-related purposes, for which employers are provided great latitude. In discussing such non-investigatory searches, the Court in *O'Connor* declared that public employers should be afforded "wide latitude" to conduct such searches for "work-related, noninvestigatory reasons" in order "[t]o ensure the efficient and proper operation of the agency."[357] Accordingly, when employee tracking is performed for a "work-related" purpose, particularly when it is done to improve the efficiency of operations—as is the case with most time-keeping apps—the "wide latitude" that must be afforded employers would seemingly justify an across-the-board monitoring of employees' locations.

Although tracking an employee's location through a timekeeping app is generally not unlawful, the analysis may change somewhat with respect to location tracking via an employer's individual app. This is because, unlike apps designed specifically for timekeeping purposes, such broad-based employer apps generally do not distinguish between on-duty and off-duty activity, making them more invasive of privacy.[358]

This leaves only the scenario of tracking an individual employee via cell phone in the context of a workplace misconduct investigation. On

355. *See* Smith v. Maryland, 442 U.S. 735, 743–44 (1979) ("This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."). For timekeeping apps in particular, the obvious connection between the app's employment-related function and the data generated by the app, including the phone's location information, should distinguish the case from *Carpenter v. United States*, which involved a far more comprehensive and "exhaustive chronicle of location information casually collected by wireless carriers" for a much more general business purpose. *See* 138 S. Ct. 2206, 2219–20 (2018). When an employer utilizes other apps to track an employee's location in this manner, such as an employer's general app that anyone, including employees and customers, can access, the assumption of risk argument carries less force.

356. *Cf. Carpenter*, 138 S. Ct. at 2222 ("We hold only that a warrant is required in the rare case where the suspect has a legitimate privacy interest in records held by a third party.").

357. O'Connor v. Ortega, 480 U.S. 709, 723 (1987).

358. *Cf. supra* notes 292–319 and accompanying text (emphasizing that GPS tracking by an employer becomes more defensible when the employer avoids collecting data while its employees are off-duty).

this issue, it is difficult to imagine an employer using any method of cell phone tracking only with respect to a particular employee. Accordingly, where cell phone location data is used in the context of an employee misconduct investigation, it would likely be in the manner used in *Carniol*—that is, where the employer simply reviews a batch of data it had previously collected on a widescale basis, with employee consent, for legitimate business reasons.[359] And, as in *Carniol*, because such data would have been lawfully acquired, possessed, and owned by the employer, nothing would prevent the employer from reviewing its data to determine whether a particular employee engaged in misconduct, in which case disciplinary proceedings may commence despite any Fourth Amendment challenge.[360]

CONCLUSION

This Article has examined the tracking of employees through both GPS and smartphones, conduct that may cause disgruntled employees to sue for an invasion of privacy. Employers will have a much stronger defense against such claims when they use either tracking method to monitor an entire segment of employees for legitimate business reasons, rather than as part of an investigation into individual employee malfeasance. In addition, notifying employees in advance of any surveillance program, such as through a written GPS tracking policy, and limiting the scope of any surveillance to avoid collecting data regarding employees' off duty conduct, will help avoid liability for such claims.

359. *See supra* notes 292–319 and accompanying text.

360. *See supra* notes 318–19 and accompanying text.