Nebraska Law Review

Volume 99 | Issue 4 Article 5

2021

Cell Phone Searches by Employers

Marc Chase McAllister
Coastal Carolina University, mcallistermarc22@gmail.com

Marc Chase McAllister*

Cell Phone Searches by Employers

TABLE OF CONTENTS

* Marc McAllister is an Assistant Professor of Business Law at Coastal Carolina University. The author's research focuses on employment law, including employment discrimination and employee privacy rights. His recent articles have appeared in the Boston College Law Review, Florida Law Review, Washington and Lee Law Review, and Alabama Law Review.

I. INTRODUCTION

This Article presents a framework for analyzing cell phone searches by employers. The framework proposed in this Article is structured around two primary variables: (1) whether the employee whose cell phone is searched works for a public or private employer, and (2) whether the cell phone is owned by the employer or employee.

The starting point for developing a framework for cell phone searches is the Fourth Amendment to the United States Constitution, which prohibits "unreasonable searches and seizures" by state actors, including public employers.[1] To be reasonable, a Fourth Amendment search or seizure must ordinarily be justified by a warrant or warrant exception.[2] One warrant exception of particular relevance here is the "workplace exception" established by the United States Supreme Court in *O'Connor v. Ortega*, which allows for certain employer-initiated searches on the basis of an employer's own determination of reasonable suspicion.[3] Other key Supreme Court precedents that impact employee cell phone searches include *City of Ontario v. Quon*, which applied the *O'Connor* exception to uphold an employer's review of text messages on an employer-owned device;[4] and *Riley v. California*, which established heightened privacy protections for personally-owned cell phones.[5]

1. U.S. CONST. amend. IV; *see also* O'Connor v. Ortega, 480 U.S. 709, 715 (1987) (establishing that employees of public employers enjoy Fourth Amendment protections in the workplace).
2. *See* U.S. CONST. amend. IV ("[N]o Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."); Katz v. United States, 389 U.S. 347, 357 (1967) ("[S]earches 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)); *accord* Riley v. California, 573 U.S. 373, 382 (2014).
3. *O'Connor*, 480 U.S. at 725–26; *see also infra* notes 59–61 and accompanying text (discussing the reasonable suspicion standard announced in *O'Connor*).
4. City of Ontario v. Quon, 560 U.S. 746, 750, 756–57 (2010); *see infra* notes 97–111 and accompanying text (discussing *Quon*).
5. *Riley*, 573 U.S. at 393–97; *see infra* notes 113–30 and accompanying text (discussing *Riley*).

Regarding device ownership, in *Quon* an employer's warrantless search of an employer-owned device was upheld as lawful, whereas in *Riley* a warrantless search of a personally-owned device was deemed unlawful.[6] As in *Quon* and *Riley*, this distinction in ownership may impact the lawfulness of a cell phone search by an employer.[7] As such, this Article develops a framework of analysis that depends, in part, on this ownership-based distinction.

For searches of personally-owned cell phones by public employers, this Article argues that such devices are generally beyond the reach of the *O'Connor* workplace exception; therefore, they should ordinarily not be searched by a public employer without a warrant due to their unique capacity to hold immense amounts of private information.[8] Despite this general rule, warrantless searches of personally-owned cell phones by public employers might be lawful if an employer has implemented a clear and narrowly-defined policy authorizing such searches. This proposed exception would apply, however, only if employees have voluntarily consented to the employer's policy and the policy is justified by a legitimate business need to manage or review particular employment-related data contained within the phone.

For employer-owned devices involving public employers, this Article recognizes that employees generally have limited expectations of privacy in such devices vis-à-vis their employers, particularly where an employer's policy permits their inspection, making such devices more freely searchable by employers. Nevertheless, in cases where an employee could reasonably expect privacy in an employer-issued cell phone, this Article argues, consistent with *O'Connor* and *Quon*, that such searches must be both reasonable at the inception and reasonable in scope.[9] Of particular relevance under the *O'Connor* framework, this Article emphasizes the need for employers to properly limit the scope of their search to avoid accessing private information untethered from the specific work-related purpose for the search.[10]

---

6. *Riley*, 573 U.S. at 378–81, 401; *Quon*, 560 U.S. at 750, 764.
7. *See infra* notes 92–95 and accompanying text.
8. As articulated by *Riley*, the contents of modern cell phones generate privacy concerns that exceed even those found in the home, the area that has enjoyed the most Fourth Amendment protection, thereby precluding their warrantless inspection in most instances. *Riley*, 573 U.S. at 396–97, 401 (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 "many sensitive records previously found in the home" as well as "a broad array of private information never found in a home in any form"); *id.* at 401 ("Our holding, of course, is not that the information on a cell phone is immune from search; it is instead that a warrant is generally required before such a search, even when a cell phone is seized incident to arrest.").
9. *See Quon*, 560 U.S. at 764; O'Connor v. Ortega, 480 U.S. 709, 725–26 (1987).
10. *See O'Connor*, 480 U.S. at 726 (explaining that two types of employer-initiated searches might fall within the scope of the *O'Connor* exception: (1) those made for

Turning to searches by private employers, this Article argues that the requirements for the tort of intrusion upon seclusion (tort of intrusion) provide the proper framework for analyzing searches of employee cell phones. The tort of intrusion is often used to challenge alleged privacy invasions by private employers[11] and typically requires a plaintiff to prove (1) the employer intentionally intruded upon the employee's solitude, seclusion, or private affairs, and (2) the employer's infringement would severely offend a reasonable person.[12]

Although facially distinct, the requirements for the tort of intrusion overlap with those of the Fourth Amendment, making this Article's proposed framework for private employers similar to that proposed for public employers. For example, whether as part of the first or second element of the tort, courts considering intrusion claims usually consider whether the plaintiff could reasonably expect privacy in the case at hand.[13] Accordingly, as under the Fourth Amendment, employees who believe their cell phones were unlawfully searched by

---

a noninvestigatory, work-related purpose, such as entering an office to retrieve a needed file; and (2) those made as part of an investigation of work-related misconduct).

11. *See* RESTATEMENT OF EMP'T LAW § 7.06 (AM. LAW INST. 2015) (stating that at least forty-one states and the District of Columbia have recognized the tort of intrusion upon seclusion, and noting that over thirty states have applied the tort in the employment context); *see also, e.g.*, Sunbelt Rentals, Inc. v. Victor, 43 F. Supp. 3d 1026, 1033–34 (N.D. Cal. 2014) (stating that California recognizes four categories of the tort of invasion of privacy, and discussing a tort of intrusion claim based on an employer's search of an employee's cell phone); Kaczmarek v. Cabela's Retail Ill., Inc., No. 1–14–3813, 2015 WL 6156352, at *1 (Ill. App. Ct. Oct. 16, 2015) (involving an employee's tort of intrusion claim challenging her employer's search of her personal cell phone); Koeppel v. Speirs, 808 N.W.2d 177, 181 (Iowa 2011) (involving a tort of intrusion claim challenging an employer's act of installing a hidden video camera in the employee restroom); K-Mart Corp. Store No. 7441 v. Trotti, 677 S.W.2d 632, 636 (Tex. App. 1984) (involving a tort of intrusion claim challenging an employer's search of an employee's locker).

12. *See* Ehling v. Monmouth-Ocean Hosp. Serv. Corp., 872 F. Supp. 2d 369, 373 (D.N.J. 2012) (applying New Jersey law); *K-Mart Corp. Store No. 7441*, 677 S.W.2d at 636 ("[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.").

13. 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 Koeppel*, 808 N.W.2d at 181; *see also Sunbelt Rentals, Inc.*, 43 F. Supp. 3d at 1033 (stating that under the first element of the tort of intrusion, "the defendant must intentionally intrude into a place, conversation, or matter as to which the plaintiff has a reasonable expectation of privacy"). 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* 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,

their employer cannot prevail on an intrusion claim if they have no reasonable expectation of privacy in the first place.[14] In addition, the inquiry regarding whether an employee can reasonably expect privacy in the contents of a device is identical for both types of employment situations, and in either context, it "must be addressed on a case-by-case basis" with a particular emphasis on the most common factors relevant to cell phone searches.[15] Beyond this threshold issue, Fourth Amendment claims and those based on the tort of intrusion each require an invasion of an employee's reasonable expectation of privacy *to such a degree as to be declared objectively unlawful*.[16] Accordingly, for intrusion claims involving cell phone searches by private employers, many of the same Fourth Amendment considerations would apply, including (1) whether the employee had a reasonable expectation of privacy in the device and its contents, and (2) whether the search or seizure is properly limited in scope so as to avoid accessing private information untethered to the intrusion's justifications.[17]

Part II of this Article summarizes the law governing searches and seizures of employee cell phones by both public and private employers. Part III more closely examines cell phone searches by public employers, including a summary of recent cases involving employer-issued and personally-owned cell phones. Following a similar structure, Part IV examines recent cases involving cell phone searches by private em-

---

stating that it need not address whether the alleged privacy intrusion was "highly offensive").

14. *O'Connor*, 480 U.S. at 715 (involving a public employer search); *Sunbelt Rentals, Inc.*, 43 F. Supp. 3d at 1034 (involving a private employer search); *see also* RESTATEMENT OF EMP'T LAW § 7.01 cmt. g ("[C]ourts have utilized Fourth Amendment principles in deciding whether employees generally have a reasonable expectation of privacy in their offices, regardless of whether they work for the government or for a private company.").

15. Stengart v. Loving Care Agency, Inc., 990 A.2d 650, 660 (N.J. 2010) (quoting *O'Connor*, 480 U.S. at 718); *see infra* section V.B. (setting forth the most common factors relevant to cell phone searches).

16. *See* Rush v. Portfolio Recovery Assocs. LLC, 977 F. Supp. 2d 414, 435 n.25 (D.N.J. 2013) (regarding a tort of intrusion claim, stating that "the Court is constrained to apply the objective standard to determine if there was a highly offensive breach of the individual's reasonable expectation of privacy"); *Stengart*, 990 A.2d at 660 ("As is true in Fourth Amendment cases, the reasonableness of a claim for intrusion on seclusion has both a subjective and objective component.").

17. *See* RESTATEMENT OF EMP'T LAW § 7.01 cmt. d (recognizing that although there are differences between the Fourth Amendment's standard of "reasonableness" and the intrusion tort's standard of "offensiveness," both tests "provide for a balancing of the nature and degree of privacy interests infringed as compared to the legitimate interests for the invasion"); *cf.* City of Ontario v. Quon, 560 U.S. 746, 764 (2010) ("For these same reasons—that the employer had a legitimate reason for the search, and that the search was not excessively intrusive in light of that justification—the Court also concludes that the search would be 'regarded as reasonable and normal in the private-employer context' . . . .").

ployers. Part V provides guidelines and proposals for cell phone searches by employers. Part VI concludes.

II. PRIVACY PROTECTIONS FOR EMPLOYER-INITIATED SEARCHES AND SEIZURES

American workers, whether employed by public or private employers, are entitled to a host of privacy protections in the workplace.[18] Because there is no single privacy law in America, employees may be protected from privacy invasions by various laws, including federal and state statutes, tort law, and constitutional requirements.[19] This Part deals specifically with the most common workplace privacy claims arising out of searches and seizures by employers. Because the law on this issue differs for public and private employers, this Part addresses each type of employer separately.

A. Employees of Public Employers

When employees of a public employer believe their privacy rights were violated, they will usually sue the employer under 42 U.S.C. § 1983, alleging a violation of the constitutional right to be free from "unreasonable searches and seizures" under the Fourth Amendment to the United States Constitution.[20]

---

18. *See O'Connor*, 480 U.S. at 715 (establishing that employees of public employers enjoy Fourth Amendment protections in the workplace).
19. Mauricio Paez & Mike La Marca, *The Internet of Things: Emerging Legal Issues for Businesses*, 43 N. KY. L. REV. 29, 40 (2016). Privacy-related statutes typically apply to specific industries or particular types of data. *See* Courtney Albini, Comment, *Borrowing from the Old [Common Law] to Litigate the New [Beacon Surveillance Claims]*, 2018 U. CHI. LEGAL F. 239, 239 (2018); *see also* Dirkes v. Borough of Runnemede, 936 F. Supp. 235, 238 (D.N.J. 1996) (listing various federal privacy statutes); RESTATEMENT OF EMP'T LAW § 7.01 (listing a variety of state and federal statutes that apply to particular types of privacy intrusions). Examples of federal privacy statutes include the Fair Credit Reporting Act of 1970, 15 U.S.C. §§ 1681–1681x (2020) ("recognizing," according to the court in *Dirkes*, 936 F. Supp. at 238, "an individual's right to privacy with regard to access and disclosure of credit records"); the Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232g (2020) ("recognizing," according to the court in *Dirkes*, 936 F. Supp. at 238, "the individual's right to privacy with regard to access and disclosure of student records"); and the Tax Reform Act of 1976, 26 U.S.C. § 6103 (2020) ("recognizing," according to the court in *Dirkes*, 936 F. Supp. at 238, "an individual's right to privacy with regard to disclosure of tax returns"). Along with federal statutes, state statutes might also restrain employers. For example, some state statutes make it unlawful for employers to utilize GPS tracking as a means of investigating their employees (usually with an exception based on employee consent). *See, e.g.*, 720 ILL. COMP. STAT. 5/21–2.5 (2014) (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).
20. U.S. CONST. amend. IV; *see, e.g.*, *O'Connor*, 480 U.S. at 714 (involving a Fourth Amendment claim based on an employer's search of a public employee's office);

Although the Fourth Amendment contains over fifty words and sets forth detailed requirements for obtaining a warrant, at its core, it prohibits "unreasonable searches and seizures."[21] Considering these four words, courts have broken Fourth Amendment analysis into three steps: (1) examining whether a Fourth Amendment "search" or "seizure" has occurred; (2) if so, determining whether that action was "unreasonable"; and (3) if so, deciding whether an appropriate remedy exists for the particular Fourth Amendment violation. These steps are outlined more fully below, with an emphasis on how the Fourth Amendment restrains public employers.

1. Step One: Determining Whether a "Search" or "Seizure" Has Occurred

In the first step of Fourth Amendment analysis, courts consider whether a Fourth Amendment "search" or "seizure" has occurred. This is the critical threshold issue in Fourth Amendment analysis because without a search or seizure, there is no Fourth Amendment action, without which there can be no Fourth Amendment violation.[22]

a. Fourth Amendment Seizures

Fourth Amendment claims may involve seizures of persons or 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."[23] A seizure would occur, for example, when police exercise control over a person's property by taking the property into police possession.[24] In the employment context, a seizure might occur when an employer downloads the contents of an employee's private cell phone onto the employer's work computer (to facilitate a subsequent search of those contents).[25]

---

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.").

21. U.S. CONST. amend IV; *see* Riley v. California, 573 U.S. 373, 381–82 (2014) ("As the text [of the Fourth Amendment] makes clear, 'the ultimate touchstone of the Fourth Amendment is "reasonableness."'" (quoting Brigham City v. Stuart, 547 U.S. 398, 403 (2006))); Pennsylvania v. Mimms, 434 U.S. 106, 108–09 (1977) ("The touchstone of our analysis under the Fourth Amendment is always 'the reasonableness in 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. *See* 19 MO. PRAC., CRIMINAL PRACTICE & PROCEDURE § 4:1 (3d ed., 2019) ("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.'").
23. United States v. Jacobsen, 466 U.S. 109, 113 (1984).
24. *See id.* at 120 n.18.
25. *See* Larios v. Lunardi, 445 F. Supp. 3d 778 (E.D. Cal. 2020).

Seizures of persons are less common in employment, but sometimes occur. As a general principle, a person is seized under the Fourth Amendment when there has been "a meaningful interference with his freedom of movement."[26] As noted, however, Fourth Amendment claims based on a seizure of an individual usually do not arise when the contents of an employee's cell phone are examined, which instead gives rise to Fourth Amendment search claims.[27]

b. Fourth Amendment Searches

Under Fourth Amendment law, the term "search" is a legal term of art distinct from its ordinary dictionary definition.[28] Indeed, many routine police activities that are specifically designed to uncover criminal evidence are not considered Fourth Amendment searches, such as a dog sniff for drugs at an airport.[29]

To determine whether a Fourth Amendment "search" has occurred, courts typically apply the "reasonable expectation of privacy" test derived from *Katz v. United States*.[30] Under the *Katz* test, a Fourth Amendment "search" occurs when the government violates a person's expectation of privacy that society recognizes as reasonable or legitimate.[31]

---

26. Skinner v. Ry. Labor Execs.' Ass'n, 489 U.S. 602, 616 (1989). In the criminal investigation context, seizures of persons include arrests or de facto arrests, which require probable cause. *See* New York v. Harris, 495 U.S. 14, 17–18 (1990) (involving an arrest); Dunaway v. New York, 442 U.S. 200, 206–16 (1979) (involving a de facto arrest). Seizures of persons also include less intrusive investigative detentions of limited scope and duration, known as "*Terry*-level" seizures, which require reasonable suspicion of wrongdoing, as opposed to probable cause. *See Terry*, 392 U.S. at 20–22, 27–28 (authorizing a brief, temporary seizure of a person suspected of committing a crime on the basis of reasonable suspicion). For a summary of the types of Fourth Amendment seizures, see generally United States v. Davis, 94 F.3d 1465, 1467–68 (10th Cir. 1996).

27. *See, e.g.*, *Skinner*, 489 U.S. at 618 (treating the collection and analysis of blood, urine, and breath samples from employees as Fourth Amendment searches, rather than seizures of the person, and noting that "any limitation on an employee's freedom of movement that is necessary to obtain the[se] . . . samples . . . must be considered in assessing the intrusiveness of the searches effected by the Government's testing program").

28. *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").

29. *See, e.g.*, United States v. Place, 462 U.S. 696 (1983).

30. 389 U.S. 347 (1967).

31. *See id.* at 361 (Harlan, J., concurring) ("[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 33 (discussing the *Katz* 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").

Whether an expectation of privacy is reasonable depends on context and may turn on a host of factors.[32] In the employment context, the most significant factors affecting whether an employee may reasonably expect privacy include (1) who owns the property subject to intrusion (recognizing that employees typically expect more privacy in personally-owned devices as opposed to devices owned by their employers);[33] (2) whether an employee has been notified of, and consented to, the employer's conduct;[34] and (3) whether the area or item searched was widely accessible, or instead accessible only to the individual claiming an expectation of privacy.[35] Additional factors commonly affecting expectations of privacy under Fourth Amendment

32. O'Connor v. Ortega, 480 U.S. 709, 715, 718 (1987) ("[T]he reasonableness of an expectation of privacy . . . 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 the 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 used at work).

33. *See, e.g.*, *Simons*, 206 F.3d at 398; United States v. Hamilton, 778 F. Supp. 2d 651, 654 (E.D. Va. 2011).

34. *See, e.g.*, *Simons*, 206 F.3d at 398 (recognizing that although "[g]overnment employees may have a legitimate expectation of privacy in their offices . . . . office practices, procedures, or regulations may reduce legitimate privacy expectations" (citations omitted)); *id.* (on the merits, finding that searching an employee's computer did not violate his Fourth Amendment rights because the employer's 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"); United States v. Yudong Zhu, 23 F. Supp. 3d 234, 238–40 (S.D.N.Y. 2014) (upholding a computer search over a Fourth Amendment challenge in part because employee gave written consent to inspection when he began his employment); *Hamilton*, 778 F. Supp. 2d at 654 (finding public school employee could not reasonably expect privacy in e-mails with his wife that were stored on his work computer because he was on notice and acknowledged that "contents of his computer were subject to inspection"); 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.").

35. *See O'Connor*, 480 U.S. at 718 ("[S]ome government offices may be so open to fellow employees or the public that no expectation of privacy is reasonable."). Regarding this particular factor, an employee could not reasonably expect privacy in most activities conducted in an open-air cubicle at work, such as a telephone conversation occurring within earshot of a fellow employee. *See id.* On the other hand, "[i]f [an] employer equips the employee's office with a safe or file cabinet or other receptacle in which to keep his private papers, he can assume that the contents of the safe are private." Muick v. Glenayre Elecs., 280 F.3d 741, 743 (7th Cir. 2002).

precedent include (4) the location of the search;[36] (5) the intrusiveness of an investigative technique;[37] and (6) the manner of investigation.[38]

Beyond these relatively common factors, any other relevant factor in the case at hand may impact whether an expectation of privacy is reasonable.[39] In addition, a person's status might fundamentally alter his or her expectations of privacy under the Fourth Amendment. Prisoners, K-12 students, and arrestees, for example, generally have reduced expectations of privacy as compared to ordinary adult citizens.[40] Along these lines, employees generally have lesser expectations of privacy vis-à-vis their employers than they ordinarily have in other contexts, simply as a result of the employment relationship.[41]

36. In the criminal investigation context, 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, United States v. Place, 462 U.S. 696 (1983) (involving a dog sniff of a passenger's luggage), or on a public road where the dog is employed to sniff around a car, Illinois v. Caballes, 543 U.S. 405 (2005). On the other hand, the Supreme Court has ruled that use 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 (2013).

37. Generally speaking, the closer one gets to a person's body, the more invasive the search or seizure becomes. A strip search, for example, requires a greater degree of suspicion than a search of a person's backpack or outer clothing. *See* Safford Unified Sch. Dist. #1 v. Redding, 557 U.S. 364, 373–77 (2009) (upholding warrantless search of a teenage girl's backpack and outer clothing, but striking down a search of her underwear and bra as a "quantum leap from outer clothes and backpacks").

38. This factor is often significant when sophisticated technology is used in an investigation. *See, e.g.*, 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."); Kyllo v. United States, 533 U.S. 27, 34–36 (2001) (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).

39. *See* State v. Granville, 423 S.W.3d 399, 407 (Tex. Crim. App. 2014) (listing factors courts use in deciding whether a person has a reasonable expectation of privacy in the place or object searched); State v. Tentoni, 871 N.W.2d 285, 288 (Wis. Ct. App. 2015) (listing similar factors).

40. Maryland v. King, 569 U.S. 435, 463 (2013) ("Once an individual has been arrested on probable cause for a dangerous offense that may require detention before trial, however, his or her expectations of privacy and freedom from police scrutiny are reduced."); Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 656–57 (1995) (recognizing that K-12 students have a reduced expectation of privacy); State v. Kisack, 17-0797 (La. 10/18/17); 236 So. 3d 1201, 1204 (recognizing that "prisoners have a reduced expectation of privacy" under Fourth Amendment law); *see also* Bernard James, T.L.O. *and Cell Phones: Student Privacy and Smart Devices After* Riley v. California, 101 IOWA L. REV. 343, 350 (2015) (discussing K-12 cases).

41. O'Connor v. Ortega, 480 U.S. 709, 723–25 (1987); RESTATEMENT OF EMP'T LAW § 7.01 cmt. b (AM. LAW INST. 2015) ("[E]mployees have different expectations of privacy than they may have outside of the workplace.").

As an alternative to the *Katz* test, courts sometimes apply the physical trespass test to determine whether a Fourth Amendment "search" has occurred.[42] Here, courts consider whether the government obtained information by physically intruding on a person, house, paper, or effect,[43] in which case a Fourth Amendment "search" has occurred (whether or not it would be reasonable to expect privacy in the case).[44] Such a trespass occurs when a government agent, without consent, encroaches an area or object protected by the Fourth Amendment, such as a vehicle or a home.[45] This alternative test, while important, has not been applied to employer-initiated investigations as often as the reasonable expectation of privacy test.[46]

2. Step Two: Determining Whether the Search or Seizure Is "Reasonable"

If a court determines that a Fourth Amendment search or seizure has occurred, the court then examines whether the search or seizure was "reasonable."[47] Exactly what makes a search or seizure reasonable varies by context. In the criminal investigation context, warrants and probable cause are often required for a search or seizure to be

42. Free Speech Coal., Inc. v. Att'y 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."); *see Jones*, 565 U.S. at 406–07, 409.

43. 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").

44. Florida v. Jardines, 569 U.S. 1, 5 (2013).

45. *Id.* at 11 ("That the officers learned what they learned only by physically intruding on Jardines' property to gather evidence is enough to establish that a search occurred."); *id.* at 7–10 (discussing the lack of consent on the part of Jardines); *Jones*, 565 U.S. at 410.

46. *See generally* Matthew Tokson, *The Normative Fourth Amendment*, 104 MINN. L. REV. 741, 741 (2019) (recognizing that searches are "[c]urrently . . . largely defined by the *Katz* test"). Under Fourth Amendment precedent, the physical trespass test had been mostly dormant after *Katz* and only recently returned to prominence as a result of the Supreme Court's decision in *Jones*. Thus, it should come as no surprise that in *O'Connor*, decided long before *Jones*, the Supreme Court treated the reasonable expectation of privacy test as controlling in the employment context. *See O'Connor*, 480 U.S. at 715 (stating that a government employee's Fourth Amendment rights are "implicated only if the [government employer] . . . infringed 'an expectation of privacy that society is prepared to consider reasonable'" (quoting United States v. Jacobsen, 466 U.S. 109, 113 (1984))).

47. *See, e.g.*, Katz v. United States, 389 U.S. 347, 353–54 (1967) (determining that after finding that a "search" had occurred, "[t]he question remaining for decision, then, is whether the search and seizure conducted in this case complied with constitutional standards"); *see also* Smith v. Maryland, 442 U.S. 735, 745–46 (1979) (declaring that "no warrant was required" after finding that no "search" occurred).

reasonable.[48] Neither warrants nor probable cause are required, however, when a search or seizure is conducted for a non-law enforcement or "special needs" purpose, as is the case with searches conducted by public school officials,[49] building inspectors,[50] and public employers.[51] Because such government actors are not usually engaged in criminal investigations, where warrants and probable cause take center stage, their actions must instead be "reasonable under all the circumstances," a standard that itself varies by context.[52]

In the employment context, the overall question of whether a search or seizure is "reasonable under all the circumstances" contains two separate inquiries: (1) whether the search was reasonable at its inception, and (2) whether the search was reasonable in scope.[53] According to the United States Supreme Court case that established this test, *O'Connor v. Ortega*,[54] a search by an employer will be reasonable at its inception when the employer has "reasonable grounds for suspecting" either (a) "that the search will turn up evidence that the employee is guilty of work-related misconduct" (like a suspected company theft); or (b) "that the search is necessary for a noninvestigatory, work-related purpose" (like entering an office to "retrieve a needed file").[55] Of particular relevance is the requirement that the search be "work-related" or based on some legitimate employer interest, which is

48. *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." (footnotes omitted) (quoting Wong Sun v. United States, 371 U.S. 471, 481–82 (1963)) (citing United States v. Jeffers, 342 U.S. 48, 51 (1951))). Although warrants require a showing of probable cause, U.S. CONST. amend. IV, many warrant exceptions also require probable cause. The automobile exception to the warrant requirement, for example, may allow police to search a vehicle without a warrant if they have probable cause to believe the vehicle contains evidence of a crime. *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 incident to the arrest. *See* United States v. Robinson, 414 U.S. 218, 235 (1973). The plain view exception to the warrant requirement likewise requires a showing of probable cause. *See* Arizona v. Hicks, 480 U.S. 321, 326 (1987) (stating "[w]e now hold that probable cause is required" to seize an item under the plain view exception). *But see* Terry v. Ohio, 392 U.S. 1 (1968) (explaining that a "stop and frisk" is not subject to the requirements of a warrant and probable cause).

49. *See* New Jersey v. T.L.O., 469 U.S. 325, 340–41 (1985).

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

51. *See O'Connor*, 480 U.S. at 719–22.

52. *See id.* at 725–26; *T.L.O.*, 469 U.S. at 341.

53. *See O'Connor*, 480 U.S. at 725–26 (citing *Terry*, 392 U.S. at 20).

54. *Id.*

55. *Id.* at 726.

built into these standards.[56] In addition, as used here, the term "reasonable grounds for suspecting" is synonymous with the Fourth Amendment's "reasonable suspicion" standard,[57] one that is less demanding than probable cause.[58]

According to *O'Connor*, 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]."[59] Under this standard, the very suspicion that justifies the search delineates its permissible scope.[60] For example, if an employer has sufficient reason to believe an employee has a red-colored file in her office that contains evidence of employee misconduct, such as stolen trade secrets, the employer would be justified in entering that office and searching through any file cabinet or container large

56. *See, e.g.*, City of Ontario v. Quon, 560 U.S. 746 (2010); *see also infra* notes 97–130 and accompanying text (discussing the facts of *Quon* and *Riley* while explaining the crux of the decisions).

57. *O'Connor*, 480 U.S. 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," similar phrasing has been used by the Supreme Court in Fourth Amendment cases as a substitute for the "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, the *O'Connor* language itself has been interpreted by courts as requiring a showing of "reasonable suspicion." *See In re* Cunningham v. N.Y. State Dep't of Labor, 997 N.E.2d 468, 472–73 (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)).

58. Comparing these two standards, the Supreme Court summarized "the required knowledge component of probable cause" as "rais[ing] a 'fair probability' or a 'substantial chance' of discovering evidence of criminal activity" and described "[t]he lesser standard" of reasonable suspicion as "a moderate chance of finding evidence of wrongdoing." Safford United Sch. Dist. No. 1 v. Redding, 557 U.S. 364, 371 (2009) (citations omitted) (quoting Illinois v. Gates, 462 U.S. 213, 238, 244 n.13 (1983)).

59. *O'Connor*, 480 U.S. at 726 (alterations in original) (quoting New Jersey v. T.L.O., 469 U.S. 325, 342 (1985)).

60. *See, e.g.*, *Quon*, 560 U.S. at 761 (finding an employer's review of text message transcripts reasonable because it was an efficient and expedient way to determine whether overages were the result of work-related messaging or personal use); *see also* Zimmerman v. Knight, 421 F. Supp. 3d 514, 522–23 (S.D. Ohio 2019) (discussing whether an employer's "download of 2,731 pages of text messages, photographs, web browser history, and call history from [p]laintiff's cell phone" was reasonable in scope by examining whether the downloaded material was relevant to the employee misconduct inquiry).

enough to hold that particular file.[61] Importantly, however, the right to search for the file extends only to those areas where it could reasonably be concealed.[62] Accordingly, in this example, it would not be reasonable to search inside a tiny pill bottle, nor would it be reasonable to search through a box of manila-colored files. Finally, once the red-colored file is found, the search should end so as to be no more intrusive than necessary.[63]

Beyond these basic reasonableness requirements, *O'Connor* emphasized that judicial oversight of public employer searches would not be particularly rigorous and that "public employers must be given wide latitude" to perform such intrusions.[64] The Court suggested, however, that the "workplace" exception to the warrant requirement would not apply beyond "the boundaries of the workplace context," which the Court delineated as "those areas and items that are related to work and are generally within the employer's control."[65] "At a hospital, for example, [the workplace includes] hallways, cafeteria, offices, desks, and file cabinets . . . [which] remain part of the workplace context even if the employee has placed personal items in them."[66] Still, the Court cautioned that "[n]ot everything that passes through

61. *Cf.* WAYNE R. LAFAVE, JEROLD H. ISRAEL & NANCY J. KING, PRINCIPLES OF CRIMINAL PROCEDURE: INVESTIGATION 217–18 (Thomson West 2004) (stating that "when the object the police indicated they are looking for could be concealed therein, they may even search unlocked containers found in that place," while discussing the scope of consent principles).

62. *See* 1 JOSHUA DRESSLER & ALAN C. MICHAELS, UNDERSTANDING CRIMINAL PROCEDURE 256–57 (5th ed. 2010) (discussing scope of search principles under the Fourth Amendment and recognizing that "it would be improper for the [searching party] to open a container too small to hide the object of the search").

63. *See* RESTATEMENT OF EMP'T LAW § 7.06 cmt. f (AM. LAW INST. 2015) (recognizing under the tort of intrusion that the scope of an intrusion is relevant to determining whether it is wrongful, and that "[i]f the scope extends beyond the purpose of the intrusion in furthering the employer's legitimate business interest, the intrusion is unjustified"). Scope of search problems are common in the Fourth Amendment. *See, e.g.*, Mincey v. Arizona, 437 U.S. 385, 388–95 (1978) (upholding, in the criminal investigation context, an immediate warrantless search of a home for potential homicide victims by officers inside the home when a shooting occurred, but striking down a subsequent warrantless search of the entire premises by different officers occurring long after the emergency had ended); Warden v. Hayden, 387 U.S. 294, 298–99 (1967) (upholding police officers' warrantless entry of a home in hot pursuit of a fleeing armed robber and permitting a search of the home "for persons and weapons" in light of this particular exigency); *In re* Cunningham v. N.Y. State Dep't of Labor, 997 N.E.2d 468, 470–74 (N.Y. 2013) (finding an employer's 30-day surreptitious GPS tracking of its employee's private vehicle unlawful because unreasonable in scope).

64. *See O'Connor*, 480 U.S. at 723–25. This is because, according to the Court, the employer's interest in efficient operation of the workplace is "substantial," whereas employees have limited expectations of privacy at work that "are far less than those found at home or in some other contexts." *Id.* at 724–25.

65. *Id.* at 715.

66. *Id.* at 715–16.

the confines of the business address can be considered part of the workplace context."[67] The Court noted, for example, that its "standard for a workplace search does not necessarily apply to a piece of closed personal luggage . . . that happens to be within the employer's business address," such as when an employee "bring[s] closed luggage to the office prior to leaving on a trip"[68] (presumably because such an item would not be one that is "related to work and . . . generally within the employer's control").[69]

In sum, *O'Connor* provides five important lessons for searches by government employers. First, government employees may reasonably expect privacy in the workplace, depending on the workplace's unique circumstances.[70] Second, Fourth Amendment claims of public employees will usually depend on whether the employer's actions were reasonable both at the inception and in scope.[71] Third, for a search to be reasonable at its inception, the employer must have "reasonable suspicion"[72] that either the search will turn up evidence of work-related misconduct, such as a suspected company theft, or that "the search is necessary for a noninvestigatory[,] work-related purpose[,] such as to retrieve a needed file" from an employee's office.[73] Fourth, to be reasonable in scope, the employer's search must not be "excessively intrusive" in light of the underlying business justification for the search.[74] Finally, not every employer intrusion will fall within the scope of the warrant requirement's workplace exception, as some items will not be within "the boundaries of the workplace context" if they are not sufficiently "related to work and . . . generally within the employer's control."[75]

3. Step Three: Determining the Appropriate Remedy for a Fourth Amendment Violation

If the court finds that an unreasonable Fourth Amendment search or seizure has occurred, the court will then determine the appropriate remedy for the constitutional violation. In the criminal prosecution context, the usual remedy is exclusion of evidence obtained as a result of the Fourth Amendment violation.[76] Exclusion of evidence might

67. *Id.* at 716.
68. *Id.*
69. *Id.* at 715.
70. *See id.* at 715–16.
71. *Id.* at 725–26.
72. *See supra* note 57.
73. *O'Connor*, 480 U.S. at 726.
74. *Id.*
75. *Id.* at 715–16.
76. *See* Mapp v. Ohio, 367 U.S. 643, 655 (1961).

also be appropriate in certain employee disciplinary proceedings.[77] But more commonly, in a 42 U.S.C. § 1983 civil suit based on an alleged Fourth Amendment violation by an employer, the usual remedy is money damages for the employee whose Fourth Amendment rights were violated.[78]

B. Employees of Private Employers

Given the lack of state action, private employers are typically not subject to Fourth Amendment constraints.[79] For alleged privacy invasions, private employers may instead face liability through tort law, including the torts of intrusion upon seclusion (intrusion),[80] public disclosure of truthful but private facts about an individual,[81] placing a person in a "false light" by unreasonable and highly objectionable publicity,[82] and appropriating the name or likeness of another for one's own commercial use or benefit.[83] These distinct forms of invasion each

77. *See, e.g.*, *In re* Cunningham v. N.Y. State Dep't of Labor, 89 A.D.3d 1347, 1350 (N.Y. App. Div. 2011) (applying the exclusionary rule in an employee disciplinary proceeding), *rev'd on other grounds*, 997 N.E.2d 468 (N.Y. 2013).

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

79. *See* Skinner v. Ry. Labor Execs.' Ass'n, 489 U.S. 602, 613–14 (1989) ("The [Fourth] 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."); *see also* United States v. Jacobsen, 466 U.S. 109, 114–15 (1984) (distinguishing between the actions of private individuals, which are not subject to the Fourth Amendment, and those of government agents, which must generally comply with Fourth Amendment requirements). In limited instances, however, the actions of a private employer could trigger constitutional constraints, particularly where the private party acts as an instrument or agent of the government. *See Skinner*, 489 U.S. at 614.

80. Koeppel v. Speirs, 808 N.W.2d 177, 180–81 (Iowa 2011).

81. *Id.* This tort involves publication of information that would be highly offensive to a reasonable person and not of legitimate public interest. 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 (Cal. Ct. App. 1982).

82. *See, e.g.*, Taha v. Bucks Cty., 9 F. Supp. 3d 490, 493 (E.D. Pa. 2014) ("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.'" (alteration in original) (quoting Santillo v. Reedel, 634 A.2d 264, 266 (Pa. Super. Ct. 1993))); *id.* at 493–94 (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).

83. 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 (AM. LAW INST. 1979).

involve an interference with a person's general "right to be left alone."[84]

The tort of intrusion is commonly used to sue private employers for privacy invasions arising out of workplace searches and seizures.[85] To prevail on an intrusion claim, a plaintiff must typically prove "that (1) her solitude, seclusion, or private affairs were intentionally infringed upon, and that (2) the infringement would highly offend a reasonable person."[86] Whether as part of the first or second element, courts considering intrusion claims usually also consider whether the plaintiff could reasonably expect privacy in the case at hand.[87] Beyond this threshold requirement, the tort of intrusion requires proof that the invasion of the plaintiff's privacy is "a substantial one, of a kind that would be highly offensive to the ordinary reasonable man."[88]

III. CELL PHONE SEARCHES BY PUBLIC EMPLOYERS

Having outlined the most common privacy claims arising out of searches and seizures by public and private employers, this Part examines cases involving searches of employee cell phones by public employers, including those involving employer-issued devices and personal cell phones, as well as seizures of evidence contained within those devices.

A. Employer-Issued Cell Phones

In the employment context, one of the most significant factors affecting whether an employee may reasonably expect privacy in a particular case is whether the employer or the employee owns the property subject to intrusion.[89] In today's economy, employers sometimes provide employees with employer-owned devices, like computers or cell phones, to be used for work-related purposes. Employers may or may not permit employees to use these devices for personal reasons as

84. *Koeppel*, 808 N.W.2d at 181 (citing RESTATEMENT (SECOND) OF TORTS § 652A cmt. b); *see also* RESTATEMENT OF EMP'T LAW § 7.01 cmt. a (AM. LAW INST. 2015) ("The great majority of jurisdictions have made these four privacy torts part of their common law.").

85. *See supra* note 11.

86. Ehling v. Monmouth-Ocean Hosp. Serv. Corp., 872 F. Supp. 2d 369, 373 (D.N.J. 2012) (applying New Jersey law); K-Mart Corp. Store No. 7441 v. Trotti, 677 S.W.2d 632, 636 (Tex. App. 1984) (applying Texas law).

87. *See supra* note 13.

88. RESTATEMENT OF EMP'T LAW § 7.06 cmt. b (quoting RESTATEMENT (SECOND) OF TORTS § 652B cmt. d); *see also* Stengart v. Loving Care Agency, Inc., 990 A.2d 650, 660 (N.J. 2010) (recognizing that "[a] high threshold must be cleared to assert a cause of action based on th[e] tort" of intrusion).

89. *See supra* subsection II.A.1.b.

well.[90] In other cases, an employer may permit an employee to use a personally-owned device for work-related tasks.[91]

Device ownership is important under the Fourth Amendment because, generally speaking, employees enjoy greater expectations of privacy in their personally-owned devices as compared to employer-owned devices.[92] Nevertheless, the commingling of personal and work-related information that can occur in either type of device may complicate an employee's privacy rights in a device.[93] In addition, although ownership is significant, it is merely one factor courts may consider in determining whether an asserted expectation of privacy is

90. *See* City of Ontario v. Quon, 560 U.S. 746, 759 (2010) ("[M]any employers expect or at least tolerate personal use of such [employer-provided] equipment by employees because it often increases worker efficiency."); *see also, e.g.*, United States v. Finley, 477 F.3d 250, 259 (5th Cir. 2007) (noting that plaintiff's employer had permitted him to use his employer-issued phone for his own personal purposes), *abrogated by* United States v. Govan, 641 F. App'x 434 (5th Cir. 2016).

91. When a device is provided by the employer, the device is commonly referred to as "company-owned, personally enabled," or COPE. When an employer allows an employee to use a personally-owned device for work-related tasks, such policies are commonly referred to as "bring your own device," or BYOD. *See* SHIRA A. SCHEINDLIN, ELECTRONIC DISCOVERY AND DIGITAL EVIDENCE IN A NUTSHELL 51, 138 (2d ed. 2016); Paul G. Lannon & Phillip M. Schreiber, *BYOD Policies: What Employers Need to Know*, HR MAG. (Feb. 1, 2016), https://www.shrm.org/hr-today/news/hr-magazine/pages/0216-byod-policies.aspx [https://perma.unl.edu/4LEK-X6SY].

92. *Compare* Port Auth. Police Benevolent Ass'n v. Port Auth. of N.Y. & N.J., No. 15-CV-3526 (KMW) (RLE), 2017 WL 4403310, at *3 (S.D.N.Y. Sept. 29, 2017) (striking down searches of personal cell phones), *with* Sunbelt Rentals, Inc. v. Victor, 43 F. Supp. 3d 1026, 1034–35 (N.D. Cal. 2014) (finding that a former employee of a private rental company could not legitimately expect privacy in an iPhone belonging to his former employer).

93. *See, e.g.*, *Finley*, 477 F.3d at 259 (finding employee had a reasonable expectation of privacy in the call records and text messages sent on his cell phone, even though the phone was issued to him by his uncle's business, because employer permitted the employee to use the business phone for personal texts and phone calls); Larios v. Lunardi, 442 F. Supp. 3d 1299, 1309 (E.D. Cal. 2020) ("Much like [the officer in *Quon*], [Larios] comingled his work life and personal life on a single device."); Sollenberger v. Sollenberger, 173 F. Supp. 3d 608, 624 (S.D. Ohio 2016) (noting that the cell phone at issue in that case had "been used as a personal cell phone in the past" and "was also used for work purposes and claimed as a work expenditure for tax purposes"); Cunningham v. Terrebonne Par. Consol. Gov't, No. 09-8046, 2011 WL 651997, at *2, *5 (E.D. La. Feb. 11, 2011) (analyzing an employer's search of an employee's cell phone that is a "personal cell phone," but for which the plaintiff received a monthly stipend from his employer to pay toward his cell phone bill for the "business use" of his phone).

reasonable.[94] Thus, determining ownership of a device will not, in and of itself, resolve the case.[95]

Given the lack of a bright-line rule regarding device ownership, when an employee challenges a public employer's search of an employer-issued device, courts sometimes refuse to decide whether a reasonable expectation of privacy exists and instead resolve the case under the reasonableness prong of *O'Connor*. A recent Supreme Court case, *City of Ontario v. Quon*, demonstrates this approach.[96]

Quon involved a city employer's review of text messages sent and received on police officer Jeff Quon's employer-issued pager.[97] The City issued pagers to SWAT Team members, including Quon, to help the SWAT Team respond to emergency situations.[98] At that time, the City informed its officers that it had a right to monitor text messages sent and received using the pagers and would treat those text messages "as public information . . . eligible for auditing."[99]

After 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 were incurring overage fees for work-related or personal messages.[100] To that end, Quon's supervisors obtained two months of pager transcripts from provider Arch Wireless.[101] After redacting all messages

94. *See* United States v. Barrows, 481 F.3d 1246, 1248 (10th Cir. 2007) (in analyzing an employee computer search, recognizing that "private ownership is an important factor telling in favor of Fourth Amendment protection," but that "[i]t is not . . . dispositive" because "[i]f it were, the Fourth Amendment would track neither tort law nor social expectations of privacy, for neither affords individuals an absolute veto over third-party access to an item by virtue of ownership alone" (citations omitted)); United States v. Erwin, 875 F.2d 268, 270–71 (10th Cir. 1989) ("Although ownership of the item seized is not determinative, it is an important consideration in determining the existence and extent of a defendant's Fourth Amendment interests."); State v. Granville, 423 S.W.3d 399, 408–09 (Tex. Crim. App. 2014) ("Ownership or legal possession of the property searched is not the 'be-all-end-all' in deciding whether a person has a legitimate expectation of privacy in it.").

95. *Compare* United States v. Yudong Zhu, 23 F. Supp. 3d 234, 238 (S.D.N.Y. 2014) (finding an employee had a reasonable expectation of privacy in a computer only he used, even though the computer was owned by his employer), *with Barrows*, 481 F.3d at 1248–49 (finding an employee had no reasonable expectation of privacy in his personal laptop computer that he brought to work). *See also* K-Mart Corp. Store No. 7441 v. Trotti, 677 S.W.2d 632, 638 (Tex. App. 1984) (finding a reasonable expectation of privacy in an employer-provided locker).

96. 560 U.S. 746 (2010).

97. *Id.* at 752–53. As the Court noted, the City of Ontario is a political subdivision of the State of California. *Id.* at 750.

98. *Id.* at 751.

99. *See id.* at 751–52.

100. *Id.* at 752.

101. *Id.*

Quon sent while off duty, officials learned that most of Quon's text messages sent during work hours were not work-related.[102] As a result, Quon was disciplined for pursuing personal matters while on duty.[103] Quon then sued the City, alleging that it violated his Fourth Amendment rights by reviewing his text messages.[104]

Applying the *O'Connor* framework, the Supreme Court assumed, without deciding, that Quon reasonably expected privacy in the contents of his text messages[105] and went on to address the overall reasonableness of the search.[106] Finding the search reasonable in all respects, 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.'"[107] Namely, to ensure the City was paying for work-related, rather than personal communications, and to determine whether the character limit on the City's pager contract should be increased.[108] As for the search's scope, reviewing the transcripts was reasonable because it was an efficient way to determine the nature of Quon's messages.[109] In addition, the Court emphasized the limited scope of 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.[110] For these reasons, the Court upheld the City's review of Quon's messages.[111]

B. Personal Cell Phones

Quon involved an employer's review of text messages on a device owned by the employer. In more recent years, courts have been confronted with the more difficult issue of employer searches of personally-owned devices, including cell phones.

Anytime the contents of a personal cell phone are searched without a warrant, courts will closely scrutinize the search.[112] This is because,

102. *Id.* at 752–53.
103. *Id.* at 753. The Court said that "Quon was allegedly disciplined." *Id.*
104. *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.
105. *Id.* at 759–60.
106. *Id.* at 760–61.
107. *Id.* at 761 (alteration in original) (quoting O'Connor v. Ortega, 480 U.S. 709, 726 (1987)).
108. *Id.*
109. *Id.*
110. *Id.* at 761–62.
111. *Id.* at 763–65.
112. *See, e.g.*, Port Auth. Police Benevolent Ass'n v. Port Auth. of N.Y. & N.J., No. 15-CV-3526 (KMW) (RLE), 2017 WL 4403310, at *4 (S.D.N.Y. Sept. 29, 2017) (analyzing *Riley*'s effect upon an employer cell phone search).

as established by the United States Supreme Court in *Riley v. California*, cell phone users generally expect privacy in the immense amount of personal data and private information stored on such devices.[113]

In *Riley*, the Court considered whether police may search digital information on a cell phone seized from an arrestee without a warrant.[114] As *Riley* noted, warrants are generally required to search for evidence of criminal wrongdoing.[115] Under the "search incident to arrest" warrant exception, however, an individual who has been placed under custodial arrest may be subject to an immediate, warrantless search for weapons or destructible evidence potentially within the arrestee's reach.[116] Even though cell phones found on arrestees could easily contain destructible evidence, such as an incriminating photograph, the *Riley* Court refused to extend this exception to cell phone searches due to the substantial privacy interests inherent in a cell phone's digital contents.[117]

Most importantly for the instant analysis, *Riley* made sweeping pronouncements regarding the modern cell phone's unique privacy concerns. *Riley* recognized that "[c]ell phones . . . place vast quantities of personal information literally in the hands of individuals."[118] The Court declared, for example, that modern cell phones are "minicomputers" capable of being used as telephones, "cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers."[119] Cell phones also have "immense storage capacity," typically allowing the user to store "millions of pages of text, thousands of pictures, or hundreds of videos."[120] Also, the Court noted that a cell phone contains various types of information, such as prescriptions and bank statements, that may reveal a great deal of information about an individual's private life.[121] According to the Court, "[t]he sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and de-

113. *See* Riley v. California, 573 U.S. 373, 393–97 (2014); *see also* United States v. Bercoon, No. 1:15-CR-022-LMM-JFK, 2016 WL 9404865, at *17 (N.D. Ga. Nov. 1, 2016) (discussing *Riley* and citing cases finding that "[a]n owner of a cell phone generally has a reasonable expectation of privacy in the electronic data stored on the phone" (alteration in original) (quoting United States v. Qunitana, 594 F. Supp. 2d 1291, 1299 (M.D. Fla. 2009))).

114. *Riley*, 573 U.S. at 378.

115. *Id.* at 382.

116. *See id.*; Chimel v. California, 395 U.S. 752, 762–63 (1969).

117. *See Riley*, 573 U.S. at 385–98 (discussing the privacy concerns inherent in modern cell phones as compared to the privacy concerns at issue in more traditional searches of purely physical evidence).

118. *Id.* at 386.

119. *Id.* at 393.

120. *See id.* at 393–95.

121. *Id.* at 394.

scriptions," whereas "the same cannot be said of a photograph or two of loved ones tucked into a wallet."[122]

The *Riley* Court found it significant that cell phones often contain a rich history of information, including a person's Internet search and browsing history over a lengthy period of time.[123] Likewise, cell phone data could show the phone's precise location at various moments in time, enabling police to reconstruct someone's movements based on the location of the phone.[124] Apps might also reveal a great deal of information about a person's private affairs, such as political and religious affiliations, addictions, and finances.[125] Finally, the Court noted that the prevalence of remote data storage magnifies the privacy interests at stake, as searching a cell phone may enable police to access additional files stored in the Cloud.[126]

Given the breadth of private information contained in most modern cell phones, *Riley* concluded that cell phone searches are far more invasive of privacy than searches of a person and his or her effects.[127] In addition, *Riley* suggested that the privacy protections owed modern cell phones are even greater than what we enjoy in our homes,[128] the area that has traditionally received the most Fourth Amendment protection,[129] thereby implying that personal cell phones are generally owed the greatest constitutional protection.[130]

---

122. *Id.*
123. *See id.* at 394–96.
124. *See id.* at 396.
125. *Id.*
126. *Id.* at 397.
127. *Id.* at 386.
128. *Riley* declared that "a cell phone search would typically expose to the government far more than the most exhaustive search of a house." *Id.* at 396 (emphasis omitted). This is because, according to *Riley*, "[a] phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form." *Id.* at 396–97.
129. The United States Supreme Court has repeatedly emphasized the heightened Fourth Amendment protections in the home. *See, e.g.*, Kyllo v. United States, 533 U.S. 27, 31 (2001); Payton v. New York, 445 U.S. 573, 585 (1980).
130. *See Riley*, 573 U.S. at 401–02 (stating that, absent "exigent circumstances" or similar "case-specific exceptions," law enforcement officers are not permitted to search an individual's cell phone without a warrant). Legal scholars and commentators have argued that *Riley* should be extended beyond the search incident to arrest context. *See, e.g.*, Eunice Park, *The Elephant in the Room: What Is a "Nonroutine" Border Search, Anyway? Digital Device Searches Post-*Riley, 44 HASTINGS CONST. L.Q. 277 (2017) (proposing a bright-line rule requiring reasonable suspicion for border searches of laptops and other digital devices); Alexandra Crandall, Note, *A Call for Probationer Data Privacy: Can States Require Cell Phone Search Waivers?*, 49 ARIZ. ST. L.J. 1487, 1488 (2017) (arguing that it is unconstitutional to require all probationers to submit their cell phones to probationary searches); Thomas Mann Miller, Comment*, Digital Border Searches After* Riley v. California, 90 WASH. L. REV. 1943, 1987–96 (2015) (arguing that, after

1. Search of Personal Cell Phone by Public Employer Struck Down as Illegal

As a result of *Riley*, public employer searches of personal cell phones have sometimes been deemed unlawful. A recent case from New York, *Port Authority Police Benevolent Ass'n v. Port Authority of New York & New Jersey*,[131] provides an interesting example.

In *Port Authority*, plaintiffs sued the Port Authority of New York and New Jersey (Port Authority) for allegedly violating their Fourth Amendment rights by searching numerous employee cell phones.[132] The events leading to that search began when the 113th class of the Port Authority Police Department (PAPD) graduated from police academy training.[133] On that day, graduates became Probationary Police Officers (PPOs) of the PAPD, making their employment easily terminable.[134] The following day, many of these PPOs attended a post-graduation party and after-party at the Texas Arizona Bar & Grill.[135]

The Texas Arizona after-party was rowdy. At that party, PPOs reportedly engaged in a range of misconduct, including damaging property, stealing beer, inappropriately touching other patrons, and fighting with a bouncer.[136] "The bouncer at the Texas Arizona stated it was the 'worst night' he had 'ever worked.'"[137]

The next morning, Lieutenant Timothy McGovern, the officer in charge of the unit responsible for police misconduct investigations (the

---

Riley, courts should require at least reasonable suspicion for all digital border searches); Sean O'Grady, Note, *All Watched Over by Machines of Loving Grace: Border Searches of Electronic Devices in the Digital Age*, 87 FORDHAM L. REV. 2255 (2019) (arguing that courts should extend *Riley* to border searches of travelers' electronic devices). *See generally* Note, *The Border Search Muddle*, 132 HARV. L. REV. 2278, 2299 (2019) (discussing *Riley*'s impact on warrantless border searches); *cf.* Tristan M. Ellis, *Reading* Riley *Broadly: A Call for a Clear Rule Excluding All Warrantless Searches of Mobile Digital Devices Incident to Arrest*, 80 BROOK. L. REV. 463, 468 (2015) (arguing that courts should extend *Riley* to exclude personal electronic devices altogether from the search-incident-to-arrest warrant exception).

131. No. 15-CV-3526 (KMW) (RLE), 2017 WL 4403310, at *3 (S.D.N.Y. Sept. 29, 2017).

132. Plaintiffs also sued certain individuals involved in the cell phone searches at issue, including Lieutenant Steven Adelhelm, Karen Connelly, Superintendent Michael Fedorko, Lieutenant Timothy McGovern, Michael Nestor, and Steven Pasichow. The district court, however, dismissed the claims against these individual defendants after finding they were entitled to qualified immunity. *Id.* at *1.

133. *Id.*

134. *Id.* at *2 (stating that because the PPOs were probationary employees, "all of them could have . . . been fired for any non-arbitrary and non-discriminatory reason").

135. *Id.* at *1.

136. *Id.*

137. *Id.*

PIU unit),[138] opened a PIU investigation into those events.[139] Thereafter, McGovern led a team of investigators in interviews of all PPOs who were present at the Texas Arizona after-party.[140] Before these interviews began, McGovern warned "the PPOs that 'they were required to cooperate in an investigation'" and "could face termination" if they did not.[141]

On the first day of the interviews, McGovern learned that PPOs who attended the Texas Arizona after-party had used a cell phone application called GroupMe to communicate about the after-party.[142] "GroupMe allows a group of individuals to participate in a private chat room that the entire group can view."[143] McGovern then directed his investigators to ask PPOs whether they participated in the GroupMe chats and, when applicable, instructed investigators to request to view those messages.[144]

Investigators ultimately reviewed the contents of thirty-six personally-owned PPO cell phones.[145] At the start of each interview, PPOs were informed they had to "cooperate in this investigation"[146] and were not informed they had the right to refuse the cell phone search.[147] As a result, many of the PPOs understood that they had no choice but to consent to the cell phone search and believed they would be fired if they did not consent.[148]

After the investigation, a group of PPOs sued the Port Authority and various individuals involved in the search, alleging their phones had been unreasonably searched and seized under the Fourth Amendment.[149] In rejecting the defendants' summary judgment motion on the claim, District Court Judge Kimba Wood began by proclaiming: "In *Riley v. California*, the Supreme Court held that a warrant is generally required before law enforcement officers may search a cell phone."[150] If a "case-specific" exception to the warrant requirement

138. *Id.*
139. *Id.* at *2.
140. *Id.*
141. *Id.*
142. *Id.*
143. *Id.*
144. *Id.*
145. *Id.* The Port Authority did not own any of the phones, did not pay for them, and did not pay for the cellular service. *Id.* at *3.
146. *Id.* Interview transcripts reveal that during thirty-three of those interviews, PPOs were given the opportunity to speak with their union representative before acceding to the search. It is unclear whether three of the PPOs were given the opportunity to speak with a representative. *Id.*
147. *Id.*
148. *See id.* (summarizing testimony of various PPOs on this point).
149. *Id.*
150. *Id.* at *4. In support, Judge Wood seemingly referenced the following passage in *Riley*: "Our holding, of course, is not that the information on a cell phone is immune from search; it is instead that a warrant is generally required before such a

did not apply, "a reasonable jury could find that these Defendants . . . violat[ed] the PPOs' Fourth Amendment rights."[151]

Defendants first sought to justify their warrantless cell phone searches under the "work-related" investigation exception of *O'Connor v. Ortega*,[152] which, as noted, permits certain warrantless searches by employers that are reasonable at the outset and reasonable in scope.[153] According to *O'Connor*, however, this warrant exception applies solely to searches conducted in the "workplace context," meaning searches of "those areas and items that are related to work and are generally within the employer's control."[154] In the words of the *O'Connor* Court:

> An employee may bring closed luggage to the office prior to leaving on a trip, or a handbag or briefcase each workday. While whatever expectation of privacy the employee has in the existence and the outward appearance of the luggage is affected by its presence in the workplace, the employee's expectation of privacy in the contents of the luggage is not affected in the same way. The appropriate standard for a workplace search does not necessarily apply to a piece of closed personal luggage, a handbag, or a briefcase that happens to be within the employer's business address.[155]

Based on this passage, Judge Wood found the search of the PPOs' cell phones unreasonable. According to Judge Wood:

> The fact that Defendants were engaging in a purportedly "work-related" investigation did not permit them to conduct warrantless searches of items outside of the "workplace context." It is undisputed that the cell phones at issue here were purely personal. They were not the property of or paid for by the Port Authority. Like the closed "handbag or briefcase" described in *O'Connor*, PPOs had a strong expectation of privacy in these personal devices. Indeed, as the Supreme Court noted in *Riley*, the privacy interest in a person's cell phone is similar to, if not greater than, the privacy interest in one's home. For this reason, just as courts have held that searches of . . . an employee's home generally qualify as outside of the "workplace context," so too do searches of a personal cell phone. The *O'Connor* exception therefore does not apply here.[156]

Simply put, like the closed "handbag or briefcase" described in *O'Connor*, the PPOs did not relinquish their legitimate expectation of privacy in the contents of their personally-owned cell phones.[157] More-

---

search, even when a cell phone is seized incident to arrest." Riley v. California, 573 U.S. 373, 401 (2014).

151. *Port Auth. Police Benevolent Ass'n*, 2017 WL 4403310, at *4; *see also Riley*, 573 U.S. at 401–02 (stating that absent "exigent circumstances" or similar "case-specific exceptions," law enforcement officers are not permitted to search an individual's cell phone without a warrant).

152. *Port Auth. Police Benevolent Ass'n*, 2017 WL 4403310, at *4.

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

154. *Port Auth. Police Benevolent Ass'n*, 2017 WL 4403310, at *4 (quoting *O'Connor*, 480 U.S. at 715).

155. *O'Connor*, 480 U.S. at 716 (emphasis omitted).

156. *Port Auth. Police Benevolent Ass'n*, 2017 WL 4403310, at *5 (citations omitted).

157. *See id.*

over, because the personal cell phones searched in this case were constitutionally on par with the employees' homes, and were not "related to work [nor] . . . generally within the employer's control," the *O'Connor* workplace exception did not permit their warrantless inspection.[158]

Having found that *O'Connor*'s workplace exception did not authorize the cell phone searches at issue, Judge Wood then rejected the defendants' second defense based on the PPOs' purported consent. Judge Wood noted that, to be valid, "[c]onsent must be a 'product of . . . free and unconstrained choice,' rather than a 'mere acquiescence in a show of authority.'"[159] In addition, consent must "not be coerced, by explicit or implicit means, by implied threat or covert force."[160] And in the employment context, "[c]oercion may be found where one is given a choice between one's employment and one's constitutional rights."[161] Applying these principles, Judge Wood concluded that a reasonable jury could find that the PPOs' acquiescence was coerced.[162]

Indeed, evidence showed that the PPOs were told more than once that if they did not cooperate with the investigation, they could be fired, causing them to believe they would be punished if they did not consent.[163] In addition, investigators never corrected that understanding.[164] Thus, a reasonable jury could find that the PPOs did not voluntarily consent to these searches.[165] As such, Judge Wood concluded, "a warrant was required before initiating the searches."[166]

2. Search of Personal Cell Phone by Public Employer Upheld as Lawful

The lawfulness of a search of an employee's personal cell phone might change under *O'Connor* when the cell phone, or at least the particular contents that were searched, is sufficiently "related to work and . . . generally within the employer's control."[167] In 2020, the United States District Court for the Eastern District of California upheld such a search in *Larios v. Lunardi*, granting summary judgment in favor of the employer on this basis.[168]

158. *Id.* at *4–5 (quoting *O'Connor*, 480 U.S. at 715).
159. *Id.* at *5 (quoting Anobile v. Pelligrino, 303 F.3d 107, 124 (2d Cir. 2001)).
160. *Id.*
161. *Id.*
162. *Id.*
163. *Id.* at *6.
164. *Id.*
165. *Id.*
166. *Id.*
167. *Id.* at *4 (quoting O'Connor v. Ortega, 480 U.S. 709, 715 (1987)).
168. *See* Larios v. Lunardi, 445 F. Supp. 3d 778 (E.D. Cal. 2020) (analyzing the Fourth Amendment seizure issue in the case); Larios v. Lunardi, 442 F. Supp. 3d 1299 (E.D. Cal. 2020) (analyzing the Fourth Amendment search issue in the case).

The plaintiff in that case, Timothy Larios, worked as a California Highway Patrol (CHP) officer and served on the Shasta Interagency Narcotics Task Force (SINTF).[169] In this role, Larios communicated with confidential informants, who provided information concerning suspected criminal activity. Most significantly, SINTF policy prohibited agents from having relationships with informants that were not "completely ethical and professional in nature."[170]

Larios began communicating with confidential informant, Tawnya Mellow, during SINTF's investigation of a suspected marijuana dealer named Nathan Santana. Mellow provided information that allowed Larios to obtain a search warrant for Santana's residence, which led to the discovery of illegal contraband and felony charges against Santana.[171]

SINTF had issued its agents cell phones to use for "SINTF business," including speaking with informants. Larios, however, used his personal cell phone to communicate with Mellow. Although SINTF policy allowed agents to use their personal phones for SINTF business, agents who produced CHP work product on their personal devices were required to transfer that work to an electronic data storage device. CHP policy declared, "[w]ork stored on any type of electronic device is the property of the state and must be relinquished on demand."[172] Larios received and reviewed this policy when he was a SINTF agent.[173]

After Santana's arrest, Larios continued to speak with Mellow but failed to abide by SINTF's policy for agent-informant communication.[174] By January 2014, Larios and Mellow were romantically involved.[175] Several months later, a domestic incident occurred at Mellow's home involving Santana, who had discovered a greeting card on Mellow's car from Larios that revealed his romantic feelings for Mellow.[176] After Santana left, the police were called, and Mellow told

169. *Larios*, 442 F. Supp. 3d at 1302.
170. *Id.*
171. *Id.*
172. *Id.* at 1303 (alteration in original).
173. *Id.*
174. *Id.*
175. *Id.*
176. *Id.* The statements made in the card included:

- "Since our first date (12/6/13), I have not been the same . . . And our walk across the bridge and kiss on the cheek shortly after your innocent text 'Marry me' has me wanting to ask you the same thing.";
- "Please know I want to spend forever with you as us !!! [sic]";
- "I want to make you happier than you've ever been before, just like you were in Tahoe. . . .": and
- "I love you for who you are Tawnya Rachelle and want nothing more than to unite as one!!"

Id.

the responding officers that Santana had threatened to kill her over the incident.[177]

After this incident, CHP's Internal Affairs Section began investigating Larios's relationship with Mellow. Investigators Scott Lunardi and Mel Hutsell reviewed Larios's SINTF phone and the card he sent Mellow and came to suspect that Larios and Mellow were in a prohibited romantic relationship. Investigators also suspected, given the absence of texts with Mellow on Larios's SINTF phone, that Larios had been using his personal cell phone to contact her.[178]

Larios was ordered to produce his personal cell phone so investigators could search the device for work product. Investigators first attempted to extract Larios's texts with Mellow but were unable to do so. Investigators then tried to video record the string of messages in Larios's and Mellow's text thread but found this approach too time intensive. As a result, investigators created a backup of Larios's entire phone on a computer and later extracted Larios's messages with Mellow from that backup.[179]

Larios later sued the CHP Commissioner and officers involved in the search, including Lunardi and Hutsell. Larios brought two separate Fourth Amendment claims, alleging that the defendants (1) conducted an unlawful *seizure* when they downloaded the contents of his personal cell phone onto a CHP computer; and (2) engaged in an unlawful *search* when they inspected the contents of his cell phone.[180]

On the search issue, Larios argued that *Riley v. California* creates a blanket rule against warrantless cell phone searches.[181] The court disagreed, finding instead that "*Riley* is not sufficiently similar to the case at hand to inform this [c]ourt's analysis."[182] In the court's view, *Riley* involved a criminal investigation that resulted in the search of personal information on a personal device. In this case, however, the defendants acted in their capacity as supervisors and conducted an employee misconduct investigation, rather than a criminal investigation.[183] And most importantly, as part of that inspection, the defendants reviewed text messages that CHP considered "work product" under its governing policy. Accordingly, the court determined that the workplace exception of *Quon* and *O'Connor* applied, rather than *Riley*.[184]

177. *Id.*
178. *Id.* at 1304.
179. *Id.*
180. *Id.* at 1302.
181. *Id.* at 1308.
182. *Id.*
183. *Id.*
184. *Id.* at 1309–10.

Applying *O'Connor*'s two-part reasonableness test, the court first found that the defendants' "inspection of CHP work product" within Larios's phone was justified at its inception in light of the evidence that Larios had "inexplicably left a romantic greeting card at the residence of a confidential informant and the target of a criminal investigation," which in turn prompted a domestic violence incident and resulted in the dismissal of Santana's charges.[185] In searching Larios's text messages, CHP simply "sought to understand the scope of [Larios]'s communication with Mellow and mitigate harm that might flow from his potential misconduct," making the search reasonable at the outset.[186]

Turning to the scope of search, the court emphasized that the defendants appropriately restricted their search to Larios's texts with Mellow, and even further "to a subset of [those] messages . . . from September 1, 2013 (the month Mellow initially contacted SINTF with information about Santana) to November 5, 2014 (the day before CHP directed [Larios] to produce his phone)."[187] In this respect, the case again resembled *Quon*'s "tailored review of an employee's text messages."[188] In sum, the court concluded that the "limited search of [Larios]'s texts with Mellow was reasonably related to the objectives of the investigation and not excessively intrusive given the grave abuse of power suspected."[189]

In the end, the critical difference between the *Port Authority* and *Larios* cases is the courts' opposing decisions regarding whether the *O'Connor* workplace exception applied. As noted in *Larios*, the search of the personal cell phone in that case was done pursuant to a valid workplace misconduct investigation as authorized under *O'Connor*.[190] Moreover, under the employer's policy, CHP work product produced on personal devices is "the property of the state and must be relinquished on demand,"[191] making these particular cell phone contents "related to work and . . . generally within the employer's control" under *O'Connor*.[192] Finally, in regards to the employer's search of the cell phone's contents, the investigating officers limited their review to Larios's texts with Mellow during the relevant time frame, making the

185. *Id.* at 1310.
186. *Id.*
187. *Id.*
188. *Id.*
189. *Id.* Although the court later found the defendants' *seizure* of the phone's entire contents separately unreasonable, *see* Larios v. Lunardi, 445 F. Supp. 3d 778, 785 (E.D. Cal. 2020), the case is nevertheless significant in demonstrating how a properly limited *search* of a personal cell phone may fall within the parameters of the *O'Connor* exception.
190. *Larios*, 445 F. Supp. 3d at 783.
191. *Larios*, 442 F. Supp. 3d at 1303.
192. O'Connor v. Ortega, 480 U.S. 709, 715 (1987).

search both reasonable at its inception (on the basis of reasonable suspicion to believe those texts would contain evidence of work-related misconduct) and reasonable in scope (by adopting "measures [that were] . . . not excessively intrusive in light of . . . the nature of the [misconduct]").[193] Accordingly, *Larios* demonstrates that employer-initiated searches of personal cell phones might be justified if the search falls within the confines of the *O'Connor* workplace exception.

IV. CELL PHONE SEARCHES BY PRIVATE EMPLOYERS

Cell phone searches by private employers are seemingly rare.[194] When they do occur, however, they may give rise to a claim of intrusion upon seclusion.[195]

A. Employer-Issued Cell Phones

As noted, expectations of privacy are often greatly reduced in employer-owned devices, particularly when combined with an employer policy permitting its inspection.[196] In certain circumstances, however, expectations of privacy in employer-issued devices can be reasonable, especially in the case of exclusive use or possession by the employee.[197] Nevertheless, the lack of an employee's ownership or present possessory interest in a device can help defeat the employee's intrusion claim. A recent California case, *Sunbelt Rentals, Inc. v.*

193. *Id.* at 726 (second alteration in original) (quoting New Jersey v. T.L.O., 469 U.S. 325, 342 (1985)); *see Larios*, 445 F. Supp. 3d at 783–84 (recognizing that such "[a] customized data withdrawal would have fallen squarely within the workplace inspection exception"); *see also O'Connor*, 480 U.S. at 726 (establishing these reasonableness requirements).

194. This statement is based on the author's research and review of relevant legal authorities. *Cf.* Port Auth. Police Benevolent Ass'n v. Port Auth. of N.Y. & N.J., No. 15-CV-3526 (KMW) (RLE), 2017 WL 4403310, at *5 (S.D.N.Y. Sept. 29, 2017) (noting that, "[i]n support of their motion, Defendants have cited no decisions applying *O'Connor* to personally-owned cell phones or to similar objects," but that upon conducting its "own research," the court found "decisions where *O'Connor* was held to justify searches of certain personal objects and places, including closed backpacks and even an individual's home as part of 'sick check'").

195. *See, e.g.*, Kaczmarek v. Cabela's Retail Ill., Inc., No. 1-14-3813, 2015 WL 6156352, at *1 (Ill. App. Ct. Oct. 16, 2015).

196. *See supra* section III.A (discussing City of Ontario v. Quon, 560 U.S. 746 (2010)).

197. *See generally Quon*, 560 U.S. at 759–60. *See also* United States v. Finley, 477 F.3d 250, 259 (5th Cir. 2007) (finding that defendant-employee had a reasonable expectation of privacy in the call records and text messages sent on a cell phone issued to him by his uncle's business); State v. Granville, 423 S.W.3d 399, 407 (Tex. Crim. App. 2014) (listing factors courts consider in determining whether a person has a reasonable expectation of privacy in a place or object, including "whether the defendant had a proprietary or possessory interest in the place or object searched" and "whether the defendant had a right to exclude others from the place or object").

Victor,[198] demonstrates how a company's former employee may lose any expectation of privacy he might have had in an employer-issued cell phone once he no longer has possession of the phone.

Sunbelt Rentals involved a lawsuit filed by an equipment rental company, Sunbelt Rentals, Inc., against one of its former employees, Santiago Victor, alleging that he misappropriated the company's trade secrets after his termination.[199] Victor began working for Sunbelt in 2000 and was promoted to an outside sales representative position in 2007.[200] According to Sunbelt's complaint, Sunbelt had invested substantial time and money in developing confidential information relating to its customers, including their renting and purchasing needs, habits, and histories.[201] To protect the confidentiality of its customer information, Sunbelt required its outside sales representatives to sign employment agreements containing post-employment non-disclosure and non-solicitation provisions.[202] Victor signed such an agreement when he was promoted.[203]

While employed with Sunbelt, "Victor was assigned a Sunbelt-owned iPhone ('Sunbelt iPhone') . . . for both work and personal purposes. Thereafter, Victor 'created and paid for a personal "Apple account" that was linked to [his Sunbelt iPhone].'"[204] In 2013, Victor left Sunbelt to work for one of Sunbelt's competitors, Ahern Rentals (Ahern).[205] At that time, Victor returned his Sunbelt iPhone to Sunbelt.[206] In addition, Victor's new employer, Ahern, provided him a new iPhone (Ahern iPhone). Victor then "registered or linked his Ahern iPhone to the same personal Apple account he had previously used while at Sunbelt. This process 'synced' Victor's Ahern iPhone with his personal Apple account."[207] Because Victor had failed to unlink the Sunbelt iPhone from his Apple account, his electronic data, including the text messages sent to and from his Ahern iPhone, were also transmitted to the Sunbelt iPhone.[208]

198. 43 F. Supp. 3d 1026 (N.D. Cal. 2014).
199. *Id.* at 1028.
200. Complaint for Injunctive Relief and Damages at 5–6, *Sunbelt Rentals, Inc*., 43 F. Supp. 3d 1026 (No. C13-4240).
201. *Id.* at 4.
202. *Id.* at 5.
203. *Id.* at 6–8.
204. *Sunbelt Rentals, Inc.*, 43 F. Supp. 3d at 1028 (citations omitted).
205. *Id.*
206. *Id.*
207. *Id.* at 1028–29 (citations omitted).
208. *Id.* at 1029. Several weeks later, when Victor linked a new iPad to his personal Apple account, Victor discovered the telephone number associated with the Sunbelt iPhone was still linked to his personal Apple account. *Id.* He "then deleted the Sunbelt number from his account 'to ensure that his new Ahern issued Apple products were not in any way linked to Sunbelt.'" *Id.*

According to Sunbelt's complaint, once Victor began working for Ahern, Victor immediately began contacting and soliciting Sunbelt's customers and employees, and successfully solicited business for Ahern from many of those customers, causing Sunbelt financial harm.[209] Apparently, Sunbelt learned of Victor's misconduct through his old Sunbelt iPhone, prompting Victor to file counterclaims against Sunbelt for allegedly accessing and reviewing his "post-employment private electronic data and electronic communications (including but not limited to text messages sent and received from Victor's Ahern . . . issued iPhone) without authority, permission, or consent."[210]

Sunbelt moved to dismiss Victor's counterclaims.[211] Construing one of Victor's claims as a claim for intrusion upon seclusion, the court noted that, under California law, the tort of intrusion first requires proof that "the defendant . . . intentionally intrude[d] into a place, conversation, or matter as to which the plaintiff has a reasonable expectation of privacy."[212]

On this element, the court explained that "Victor had no right to exclude others from accessing the Sunbelt iPhone—which he did not own or possess and no longer had any right to access."[213] Moreover, Victor failed to maintain the privacy of his text messages when he failed to unlink his Sunbelt iPhone from his Apple account.[214] Thus, Victor's intrusion claim failed because he could not "legitimately claim an expectation of privacy in . . . the Sunbelt iPhone."[215]

Sunbelt Rentals is an unusual case in that it involved cell phone content (text messages) sent from one phone, which itself was not searched by the employer, that was inadvertently transmitted to a different phone, which was searched by a former employer. Despite these unusual circumstances, there are two fundamental problems with Victor's intrusion claim. First, Victor failed to maintain the privacy of his text messages vis-à-vis his former employer—including those texts sent using his new employer's iPhone—because he failed to unlink his Sunbelt iPhone from his Apple account.[216] In this respect, the case is arguably analogous to the numerous decisions finding no reasonable

209. Complaint for Injunctive Relief and Damages, *supra* note 200, at 9–10.
210. *Sunbelt Rentals, Inc.*, 43 F. Supp. 3d at 1029 (emphasis omitted).
211. *Id.*
212. *Id.* at 1033 (quoting Hernandez v. Hillsides, Inc., 211 P.3d 1063 (Cal. 2009)). As in other jurisdictions, under California law, "the intrusion must occur in a manner highly offensive to a reasonable person." *Id.* (quoting *Hernandez*, 211 P.3d at 1072).
213. *Id.* at 1035.
214. *Id.*
215. *Id.* Turning to the second element of the tort, regarding whether the alleged intrusion was "highly offensive," the court found that it would not be offensive for Sunbelt to "have reviewed text messages sent to a cell phone which it owned and controlled." *See id.* at 1035–36.
216. *Id.* at 1035.

expectation of privacy in text messages an individual sends to another person when those texts are retrieved from that other person's device (as opposed to the device from which the messages were sent).[217] Second, Victor could not establish a reasonable expectation of privacy in the contents of the Sunbelt iPhone, which now inadvertently contained data sent from his new iPhone, because Victor was not the owner or subscriber of the cell phone *and* he no longer had any possessory interest in the device when the text messages at issue were transmitted to that device.[218] Stated differently, although an employee can sometimes legitimately expect privacy in the contents of an employer-issued cell phone, that would usually only occur when the employee is the exclusive user of the phone, which was no longer true when the search occurred in *Sunbelt Rentals*.[219]

B. Personal Cell Phones

As with public employers, private employers have at times searched the contents of a personally-owned cell phone. In one recent case, *Kaczmarek v. Cabela's Retail Illinois, Inc.*, plaintiff Michelle Kaczmarek sued her former employer, Cabela's, for the tort of intrusion upon seclusion based on her employer's review of her personal cell phone to investigate a rumored sexual relationship she had with a manager, Tim Slaby.[220]

---

217. *See* State v. Tentoni, 871 N.W.2d 285, 288–89 (Wis. Ct. App. 2015) (finding that criminal defendant did not have reasonable expectation of privacy in text messages sent by him and discovered through warrantless search of recipient's phone); *cf.* State v. Marcum, 319 P.3d 681, 686–87 (Okla. Crim. App. 2014) (finding that a criminal defendant had no reasonable expectation of privacy in the text messages she sent to her co-defendant that were obtained not from either defendant's cell phone, but rather, from the business records of the co-defendants' cell phone company, which kept a record of the texts in the regular course of business).

218. *See Marcum*, 319 P.3d at 683, 686–87 (discussing cases from numerous jurisdictions finding a reasonable expectation of privacy in a phone's contents where the person was the exclusive user of the phone but not the phone's owner or account holder); *Tentoni*, 871 N.W.2d at 289 n.5 (stating that although "courts have recognized an expectation of privacy in text messages on a cell phone," such an expectation "belongs to the owner or user of the phone"); *see also* State v. Granville, 423 S.W.3d 399, 407 (Tex. Crim. App. 2014) (listing factors courts commonly use in deciding whether a person has a reasonable expectation of privacy in the place or object searched, including "whether the defendant had a proprietary or possessory interest in the place or object searched" and "whether the defendant had a right to exclude others from the place or object"); *Tentoni*, 871 N.W.2d at 287–88 (listing similar factors).

219. *See Sunbelt Rentals, Inc.*, 43 F. Supp. 3d at 1035.

220. Kaczmarek v. Cabela's Retail Ill., Inc., No. 1-14-3813, 2015 WL 6156352, at *1–2 (Ill. App. Ct. Oct. 16, 2015).

Kaczmarek was employed as a cashier at a Cabela's store in Illinois from April 2011 until September 2012.[221] During that time, Kaczmarek befriended Slaby, a senior retail operations manager.[222] In her deposition, Kaczmarek stated that there was nothing inappropriate about her relationship with Slaby, who was considerably older than her. She explained that she got to know Slaby during breaks at work, and they would exchange texts regarding topics such as movies, music, and internet links. According to Kaczmarek, Slaby once invited her to "'go drinking with him' via text, but this never happened."[223] Thereafter, Kaczmarek "told her co-worker, Krystle Magsino, about her texts with Mr. Slaby and showed her some of those texts."[224]

On July 14, 2012, Kaczmarek's supervisor, Tammi Killis, confronted her about rumors that she and Slaby were involved in a sexual relationship.[225] Kaczmarek denied the rumors and further denied that she had Slaby's phone number or had exchanged texts with him.[226] The next day, however, Kaczmarek admitted to Killis that she had texted with Slaby.[227] Kaczmarek then showed Killis some of her recent texts with Slaby "to prove that there was nothing going on" between them.[228]

On July 16, 2012,[229] Kaczmarek was called to a meeting with Killis and Frank Mazzocco, the defendant's human resource manager, to discuss the rumors. During that meeting, Mazzocco allegedly "told [Kaczmarek] that she needed to give him her cell phone or she would be fired."[230] Describing Kaczmarek's deposition testimony, the court states that Kaczmarek "admitted that she provided her cell phone for Mr. Mazzocco to review, albeit only after he indicated that he needed to determine [the] nature of her relationship with Mr. Slaby and that she might be fired if she refused."[231]

According to Kaczmarek's complaint,[232] after she reluctantly provided her cell phone to Mazzocco, he "proceeded to access its various

221. *Id.*
222. *Id.*
223. *Id.*
224. *Id.* at *2.
225. *Id.*
226. *Id.*
227. *Id.*
228. *Id.*
229. The court initially stated that the meeting with Killis and Mazzocco occurred on July 15, 2012, *id.* at *1, but later stated that it occurred on July 16, 2012, *id.* at *3. The important point, however, is that the meeting occurred after Kaczmarek had initially showed Killis some of her recent texts with Slaby. *See id.* at *2–3.
230. *Id.* at *1 (internal quotation marks omitted).
231. *Id.* at *3.
232. The "Background" section of the court's opinion appears to summarize the allegations of the plaintiff's complaint, but at times it is not clear in that regard. *Id.* at *1–3.

features and applications including her text messages and possibly her photos."[233] Kaczmarek alleged that Mazzocco "took notes (presumably of the texts) and photos with his own cell phone (presumably of the texts or photos) and/or transferred data to his cell phone."[234] Later in her deposition, Kaczmarek stated that Mazzocco reviewed her phone for between five and ten minutes; she observed Mazzocco taking pictures of her phone but could not tell exactly what content he had reviewed.[235] During the meeting, Kaczmarek was allegedly "scared, crying and fearful for her employment."[236]

After the cell phone search, Kaczmarek was allegedly shunned by her coworkers[237] and formally disciplined for initially lying to Killis about her communications with Slaby.[238] According to Kaczmarek, these circumstances caused her emotional distress and anxiety, prompting her to resign.[239]

After the trial court granted Cabela's motion for summary judgment on Kaczmarek's intrusion claim, she appealed that decision to the Appellate Court of Illinois.[240] Applying the Illinois tort of intrusion, as derived from the *Restatement (Second) of Torts*,[241] the court declared: "One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person."[242] Under Illinois law, a plaintiff must prove the following elements of the tort of intrusion: "(1) the defendant committed an unauthorized intrusion or prying into the plaintiff's seclusion; (2) the intrusion would be highly offensive or objectionable to a reasonable person; (3) the matter intruded on was private; and (4) the intrusion caused the plaintiff anguish and suffering."[243]

---

233. *Id.* at *1 (alteration in original).
234. *Id.*
235. *Id.* at *3.
236. *Id.* at *1.
237. *Id.* at *2.
238. *Id.* at *3.
239. *Id.* at *2–3.
240. *Id.* at *3. The trial court found that: "(1) [Kaczmarek] had no factual basis to conclude that Mr. Mazzocco reviewed anything other than the texts between [her] and Mr. Slaby; and (2) '[p]laintiff cannot demonstrate that the intrusion is not only offensive, but highly offensive to a reasonable person.'" *Id.* (third alteration in original).
241. *See id.* at *4 n.2.
242. *Id.* at *4 (quoting Busse v. Motorola, Inc., 813 N.E.2d 1013, 1017 (Ill. App. Ct. 2004)); *see also* Lawlor v. N. Am. Corp. of Ill., 983 N.E.2d 414, 425 (Ill. 2012) (discussing Illinois appellate court cases that have recognized the tort of intrusion upon seclusion and opting to "join the vast majority of other jurisdictions that recognize the tort of intrusion upon seclusion").
243. *Kaczmarek*, 2015 WL 6156352, at *4 (quoting *Busse*, 813 N.E.2d at 1017).

According to the appellate court, "[t]he third element of the tort [of intrusion] appears to be the predicate for the other three."[244] Under this element, "[p]rivate facts must be alleged," without which "the other three elements of the tort need not be reached."[245] Under Illinois precedent, "it is not sufficient if the behavior complained of only intrudes into *personal*, rather than *private*, matters."[246] In this context, private matters are those "which are facially embarrassing and highly offensive if disclosed,"[247] such as those relating to "'family problems, romantic interests, sex lives, health problems, future work plans and criticism of [an employer].'"[248]

Turning to the merits, the court first found no genuine dispute regarding the scope of the information reviewed by Mazzocco.[249] The court reasoned that:

> Mazzocco's affidavit, filed in support of defendant's motion for summary judgment, [averred] that he only "reviewed and counted up the number of recent text messages between Tim Slaby and Michelle Kaczmarek that were on [plaintiff's] cell phone" and that he "did not review any personal text messages or any other items in Ms. Kaczmarek's cell phone."[250]

And for her part, Kaczmarek admitted that "she had no way of knowing exactly what Mr. Mazzocco reviewed on her phone."[251] Based on Kaczmarek's response, the court concluded that Mazzocco's affidavit was "not contradicted by counteraffidavit," making the statements in Mazzocco's affidavit admitted for purposes of summary judgment analysis.[252] Accordingly, the court assumed "as true" Mazzocco's description of his search.[253]

Having narrowed the scope of Mazzocco's search to only the recent text messages between Kaczmarek and Slaby, the court then rejected the argument that those texts were private under Illinois law.[254] The court provided several reasons to support this finding. First, the court "fail[ed] to see how [Kaczmarek's] recent text messages to Mr. Slaby [could] be viewed as a private matter at the time they were reviewed by Mr. Mazzocco, when [Kaczmarek] had already shared them with at

244. *Id.* at *5 (first alteration in original) (quoting *Busse*, 813 N.E.2d at 1017).
245. *Id.* at *5; *Busse*, 813 N.E.2d at 1017.
246. *Kaczmarek*, 2015 WL 6156352, at *5 (quoting Vega v. Chi. Park Dist., 958 F. Supp. 2d 943, 959 (N.D. Ill. 2013)).
247. *Id.* (quoting Cooney v. Chi. Pub. Schs., 943 N.E.2d 23, 32 (Ill. App. Ct. 2010)).
248. *Id.* (alteration in original) (quoting *Vega*, 958 F. Supp. 2d at 959).
249. *Id.*
250. *Id.* (second alteration in original).
251. *Id.*
252. *Id.* (citing Vill. of Arlington Heights v. Anderson, 963 N.E.2d 949, 954 (Ill. App. Ct. 2011)).
253. *Id.* Under these circumstances, the court noted that it would require speculation or conjecture to assume Mazzocco reviewed any additional information on Kaczmarek's cell phone, which is insufficient to withstand summary judgment. *Id.*
254. *Id.* at *6.

least two other people" (Masingo and Killis).[255] Employing a reasonable expectation of privacy analysis, the court thus declared, "[p]ersons cannot reasonably maintain an expectation of privacy in that which they display openly."[256] Second, the court reasoned that Kaczmarek herself maintained there was nothing inappropriate about her relationship with Slaby, adding that she showed Killis the texts "to prove that there was nothing going on."[257] For an intrusion claim, however, private matters are those "which are facially embarrassing and highly offensive if disclosed."[258] "By [Kaczmarek's] own admission," the court reasoned, "her texts with Mr. Slaby were just the opposite."[259] Finally, the court reasoned that "[t]here is nothing facially embarrassing or highly offensive" about the few texts that were actually included in the record.[260] With this crucial element lacking, the court affirmed summary judgment for the defendant.[261]

Although the point of this Article is not to criticize the opinion in *Kaczmarek*, a case with some unusual aspects,[262] a few points about the case are warranted. As noted, to prevail on a tort of intrusion claim under Illinois law, a plaintiff must typically prove "(1) the defendant committed an unauthorized intrusion or prying into the plaintiff's seclusion; (2) the intrusion would be highly offensive or objectionable to a reasonable person; (3) the matter intruded on was private; and (4) the intrusion caused the plaintiff anguish and suffering."[263]

---

255. *Id.*
256. *Id.* (alteration in original) (quoting Acosta v. Scott Labor LLC, 377 F. Supp. 2d 647, 650 (N.D. Ill. 2005)).
257. *Id.* (internal quotation marks omitted).
258. *Id.* (quoting Cooney v. Chi. Pub. Schs., 943 N.E.2d 23, 32 (Ill. App. Ct. 2010)).
259. *Id.*
260. *Id.*
261. *Id.*
262. This case is unusual in many respects. First, the court notes that immediately after the investigation regarding Kaczmarek and Slaby was complete, Slaby was fired. *Id.* at *3. Yet, it is unclear why he was fired (because the court does not specify), other than perhaps a conclusion by Mazzocco that Kaczmarek and Slaby were indeed involved in an inappropriate relationship. Moreover, in response to Cabela's motion for summary judgment, Kaczmarek voluntarily dismissed, with prejudice, two defamation counts in her complaint that alleged she had been defamed by the untrue statements made by Killis and others. *Id.* at *2. These circumstances may reinforce the notion that there was, in fact, evidence indicating that Kaczmarek and Slaby were indeed involved in an inappropriate relationship. And if that is true, then it becomes more likely that the cell phone contents reviewed by Mazzocco were indeed *private* under Illinois law—at least, there might have been a genuine issue of material fact on that point. *See* Busse v. Motorola, Inc., 813 N.E.2d 1013, 1017–18 (Ill. App. Ct. 2004) (noting that "[p]rivate facts were at issue and clearly alleged in" another Illinois case where investigators gathered and reported personal information about employees, including their "romantic interests" and "sex lives").
263. *Busse*, 813 N.E.2d at 1017.

Regarding the first element, there is no doubt that Mazzocco "committed an unauthorized intrusion or prying into the plaintiff's seclusion" when he forced Kaczmarek to reveal the contents of her personal cell phone after threatening to fire her if she refused.[264] In this respect, where coerced consent seems apparent, the similarities to *Port Authority* are striking.[265] Regarding the fourth element, there also seems to be no real dispute that Kaczmarek suffered "anguish and suffering" as a result.[266] Accordingly, the issues that remain are whether the contents of Kaczmarek's cell phone were private, and, if so, whether Mazzocco's review of those contents was highly offensive, an issue not reached by the court.[267]

The court's conclusion that the contents of Kaczmarek's cell phone were not private, including that she could not reasonably expect privacy in those particular contents,[268] is questionable. First, the true issue in this case is not, as the court put it, whether Kaczmarek's recent text messages with Slaby "can be viewed as a private matter *at the time* they were reviewed by Mr. Mazzocco,"[269] implying that a full history of text messages between two individuals became entirely unprotected after a few of those messages were shown to another individual. Rather, the question is whether Kaczmarek could reasonably expect privacy vis-à-vis a seemingly unrestrained search of her phone by her employer's human resource manager during a formal investigation into a matter he apparently viewed as very serious.

As noted by the court, when Kaczmarek elected to show Killis a few of her recent text messages with Slaby the day before Mazzocco's search, she did so voluntarily "to prove that there was nothing going on in hopes that [Killis] saw it was just friendly conversations."[270] In effect, the court ruled that Kaczmarek's initial, limited consent some-

264. *Kaczmarek*, 2015 WL 6156352, at *3 (describing plaintiff's seemingly undisputed deposition testimony in this regard).

265. *See supra* notes 151–166 and accompanying text.

266. *See Kaczmarek*, 2015 WL 6156352, at *1. In her complaint, Kaczmarek states that she was allegedly "very upset at these accusations [about her alleged relationship with Slaby] and specifically and vehemently denied any sexual relationship." *Id.* Further, the court notes that during her meeting with Mazzocco, Kaczmarek "was allegedly 'scared, crying and fearful for her employment.'" *Id.* at *2. Thereafter, Kaczmarek was allegedly shunned by her coworkers, and Kaczmarek contended that these circumstances caused her emotional distress and anxiety, evidenced by the fact that she then sought professional help resulting in a leave of absence from her employment. *Id.* In the author's view, this is enough to at least establish a genuine issue of material fact regarding the tort's second element.

267. *Id.* at *6.

268. *Id.* (applying the principle that "[p]ersons cannot reasonably maintain an expectation of privacy in that which they display openly" (alteration in original) (quoting Acosta v. Scott Labor LLC, 377 F. Supp. 2d 647, 650 (N.D. Ill. 2005))).

269. *Id.* (emphasis added).

270. *Id.* at *2.

how also extended to a more extensive search of potentially all of her cell phone's contents at a later date by a different person. This reasoning is like finding that a criminal suspect's consent to one police officer's search of his bedroom on Monday also authorizes a search of his entire house by a different officer on Tuesday, a finding that would violate Fourth Amendment consent principles.[271] Under Fourth Amendment precedents, after all, there is a difference between a search based on valid consent that is limited in scope, and a subsequent search based on coerced consent that is not so limited.[272]

Second, the identity of the individual conducting each search matters, as expectations of privacy may vary as between different searching parties. The Supreme Court has noted, for example, that an employee may have different expectations of privacy regarding a search by an employer versus a search by other government officials.[273] Accordingly, it is possible that Kaczmarek could have relinquished any expectation of privacy she had vis-à-vis her direct supervisor, while failing to do so vis-à-vis a human resources investigator in the context of a more formal investigation of employee misconduct.[274]

Third, the court's conclusion regarding the scope of Mazzocco's review is problematic. As the court notes, Kaczmarek had no way of knowing exactly what contents of her phone Mazzocco reviewed. Kaczmarek's lack of knowledge on this issue, however, should not preclude her from withstanding summary judgment. In this respect, the case is similar to other intrusion claims in which, given the secretive nature of the apparent intrusion, the plaintiff is unable to prove the exact dimensions of the intrusion but can still survive summary judgment based on its *inherently invasive* nature. In *Koeppel v. Speirs*,[275] for example, where an employer installed a hidden video camera in the bathroom used by his female employees, the Iowa Supreme Court ruled that an actual intrusion on the employees' privacy could be in-

271. *See* DRESSLER & MICHAELS, *supra* note 62, at 256 ("If *A* consents to a ten-minute search, the police may not invoke consent to justify the search after the consent expires."); LAFAVE ET AL., *supra* note 61, at 218 ("As a general rule, it would seem that a consent to search may be said to have been given on the understanding that the search will be conducted forthwith and that only a single search will be made.").

272. *See* Florida v. Jimeno, 500 U.S. 248, 251 (1991) ("The scope of a search is generally defined by its expressed object.").

273. Mancusi v. DeForte, 392 U.S. 364, 369 (1968).

274. *See* 2 L. CAMILLE HÉBERT, EMPLOYEE PRIVACY LAW § 8A:51 (2020) (discussing *Kaczmarek* and finding "[t]he court's analysis . . . subject to challenge"; reasoning "that one voluntarily shares private information with some individuals should not compel one to share that information with an employer conducting an investigation upon pain of termination; an employee should have the choice to selectively share private information with some and not others").

275. 808 N.W.2d 177 (Iowa 2011).

ferred from the mere discovery of a functional camera in the bathroom, despite no evidence that the defendant actually used the camera to spy on the plaintiffs.[276] So too could a reasonable jury infer that Mazzocco's extensive review of Kaczmarek's phone intruded upon her private matters. This is especially true in light of Kaczmarek's testimony that Mazzocco reviewed her phone for up to ten minutes and that she observed Mazzocco taking pictures of her phone. As another commentator has noted: "The mere fact of being compelled to share private and personal information with an employer upon pain of termination should be viewed as highly offensive without some compelling justification for that compulsion."[277] This is particularly true for private communications made on a personal cell phone.[278] As established by the Supreme Court in *Riley*, the "privacy-related concerns" in cell phones are so substantial that searching those devices without a warrant is generally unlawful under the Fourth Amendment—even for persons whose expectations of privacy are generally reduced—despite the searching party's assurances regarding the limited nature of the invasion.[279]

V. PROPOSALS

Having examined the law governing private and public employers, particularly as it pertains to cell phone searches, this Part provides guidelines and proposals for cell phone searches by employers.

A. Overall Framework of Analysis

In light of the search and seizure principles outlined in this Article, when a court reviews an employer's search or seizure of the contents of an employee's cell phone, the court should engage in the simple, three-step analysis outlined below.

In the first step, the court should determine whether the searching party acted in its capacity as an employer.[280] If so, the court should identify whether the employer is a public or private employer, as this distinction will alter the applicable legal framework and potentially

276. Koeppel v. Speirs, 779 N.W.2d 494 (Iowa Ct. App. 2010), *aff'd*, 808 N.W.2d 177 (Iowa 2011); *see also Koeppel*, 808 N.W.2d at 182–83 (discussing similar cases that focus on the "potential for viewing" created by the defendant's actions).

277. L. CAMILLE HÉBERT, *supra* note 274.

278. *See id.*

279. *See* Riley v. California, 573 U.S. 373, 386 (2014) (holding that police must generally secure a warrant before searching data within a cell phone found on an arrestee); *id.* at 393 (rejecting the government's argument that searching the contents of a cell phone found on an arrestee is analogous to searching personal items carried by an arrestee, such as billfolds or address books).

280. If an employer is acting as an agent of law enforcement as part of a criminal investigation, different Fourth Amendment principles would apply. *See* Larios v. Lunardi, 442 F. Supp. 3d 1299 (E.D. Cal. 2020).

impact the lawfulness of the employer's action in close cases (given the differing inquiries of *reasonableness* and *extreme offensiveness*).[281]

In the second step, the court should apply the factors discussed in section V.B of this Part to determine whether the employee can reasonably expect privacy in the particular cell phone contents at issue. If the court determines that the employee cannot reasonably expect privacy in those contents, the employer's review should be deemed lawful, ending the court's inquiry.

Finally, if the court determines that the employee can reasonably expect privacy in the cell phone contents at issue, the court should determine whether the employer's search or seizure of those contents is either (a) unreasonable for a public employer's actions, or (b) highly offensive for a private employer's actions. Of particular relevance under this final step for either type of employer is whether the employer limits the scope of its review to avoid accessing private information untethered to the intrusion's justifications.

The remainder of this Part provides additional details and proposals for steps two and three above.

B. Reasonable Expectations of Privacy

Under either the Fourth Amendment or the tort of intrusion, if an employee cannot reasonably expect privacy in the contents of the cell phone, the employee cannot prove an unlawful invasion of privacy.[282] Accordingly, the critical threshold issue for any employer-initiated cell phone search is whether the employee can legitimately expect privacy in the cell phone's contents.

Although this is a totality of circumstances inquiry that examines any relevant factor in the case at hand, the most critical factors that may impact an employee's expectation of privacy in a cell phone include (a) whether the device at issue is owned by the employer or employee; (b) whether the employee is the exclusive user or possessor of the device; (c) whether an employer policy permits a search of the device or a seizure of its contents; (d) whether the employee voluntarily consented either to the employer's policy or to the particular search at issue; and (e) whether the employer reviews the contents of a communication stored within the device, or instead limits its search to determining whether a communication occurred. Each of these factors are discussed below. In addition, because device ownership may dramatically alter expectations of privacy, this section addresses employer-owned and personally-owned cell phones separately and presents specific proposals for each type of device.

281. *See supra* note 88 and accompanying text.
282. *See supra* note 14 and accompanying text.

1. Employer-Issued Cell Phones

As discussed, device ownership is important under the Fourth Amendment because, generally speaking, employees enjoy greater expectations of privacy in personally-owned devices as compared to employer-owned devices.[283] Nevertheless, device ownership is merely one factor courts may consider in determining whether an asserted expectation of privacy is reasonable, and the commingling of personal and work-related information that can occur in either type of device can muddy the waters in this area.[284] Thus, ownership alone does not determine whether an employee can reasonably expect privacy in a cell phone's contents.

Even for employer-owned devices, where expectations of privacy are generally reduced, courts have recognized that when an employee is the *exclusive user* of a device, it might be reasonable for the employee to expect privacy in that device.[285] In *United States v. Finley*, for example, the United States Court of Appeals for the Fifth Circuit struck down a police officer's warrantless search of an arrestee's cell phone discovered in his pocket upon arrest.[286] The phone belonged to Southwest Plumbing and had been issued to the arrestee, Jacob Finley, for work, but Finley was permitted to use the phone for personal purposes as well.[287] Although the court recognized that "Finley's interest was possessory only,"[288] the court declared that Finley's lack of an ownership interest in the phone was not dispositive.[289] The court concluded that even though "Finley's employer could have read the text messages once he returned the phone," as in a case like *Sunbelt Rentals*, this "does not imply that a person in Finley's position should not have reasonably expected to be free from intrusion from both the government and the general public" at a time when the phone remained in the employee's possession.[290] In these circumstances, where "Finley had a right to exclude others from using the phone," the court concluded that Finley had a reasonable expectation of privacy in the call records and text messages on the cell phone, and therefore, had standing to challenge the search of that device by law enforcement.[291]

283. *See supra* notes 90–95 and accompanying text.
284. *See supra* notes 90–95 and accompanying text.
285. *See supra* note 218; United States v. Ibarra, 948 F.2d 903, 906 (5th Cir. 1991) (listing similar factors as those in *Granville* and *Tentoni*).
286. United States v. Finley, 477 F.3d 250, 254 (5th Cir. 2007).
287. *Id.*
288. *Id.* at 259 n.5.
289. *Id.* at 259.
290. *Id.*
291. *Id.* The court went on to find, however, that this search was reasonable under the search incident to arrest exception to the warrant requirement, *id.* at 259–60, a ruling that is now called into doubt by *Riley*.

In *Finley*, the employee's cell phone was searched by a police officer, rather than Finley's employer. The identity of the searching party is important because an employee's expectations of privacy may differ as between different state actors.[292] For searches by employers, expectations of privacy might be altered by the existence of an employer policy giving the employer the right to inspect an employer-owned device for certain business-related reasons or more broadly stating that the employee cannot reasonably expect privacy in the device's contents.[293] Accordingly, if an employer's policy, to which an employee has voluntarily consented, clearly states that an employer-issued cell phone may be searched by the employer or that the employee cannot reasonably expect privacy in the cell phone's contents, that policy might override any expectation of privacy the employee otherwise enjoys in regards to his or her employer.[294]

Finally, when a person's communications are at issue, such as an employee's text messages, Fourth Amendment law often distinguishes between the content of communications and the addressing information associated with those communications.[295] And although this distinction arose in the criminal investigation context, courts have applied this distinction to employer-initiated searches.[296] This distinc-

292. *See, e.g.*, United States v. Yudong Zhu, 23 F. Supp. 3d 234, 239 (S.D.N.Y. 2014) (finding an employee had a reasonable expectation of privacy in his employer-owned laptop vis-à-vis a search by law enforcement, rather than a search by the employer itself).

293. *See, e.g.*, *id.* at 236–37 (discussing two policies of employer NYU: one which applied to faculty acknowledging "that [NYU] may inspect the computers it owns, as well as personal PCs used for work, to ensure that its data and software are used according to its policies and procedures"; and another applying to staff and stating that "[c]omputers, e-mail systems, and electronic communications and equipment are the sole property of NYU . . . and staff should not have any expectation of privacy" (second alteration in original)); *see also id.* at 239–40 (finding Yudong Zhu, a faculty member, was not bound by the broader policy pertaining to staff).

294. *See id.* at 239–40; *see also* City of Ontario v. Quon, 560 U.S. 746, 760 (2010) ("[E]mployer policies concerning communications will of course shape the reasonable expectations of their employees, especially to the extent that such policies are clearly communicated.").

295. *See* Smith v. Maryland, 442 U.S. 735, 741–43 (1979) (discussing the distinction between the content of communications and the addressing information associated with those communications).

296. Under both the Fourth Amendment and the tort of intrusion, courts have recognized that it is generally more invasive to access the contents of text messages, as opposed to accessing a list of numbers and names with which a person has communicated. *See, e.g.*, McGreal v. AT&T Corp., 892 F. Supp. 2d 996, 1015 (N.D. Ill. 2012) (tort of intrusion); Cunningham v. Terrebonne Par. Consol. Gov't, No. 09-8046, 2011 WL 651997, at *2, *5 (E.D. La. Feb. 11, 2011) (rejecting summary judgment for employee on his Fourth Amendment claim due to genuine issues of fact as to whether the employee had a reasonable expectation of privacy in his cell phone records containing only numbers dialed and received, but not names or substance); *cf.* Sunbelt Rentals, Inc. v. Victor, 43 F. Supp. 3d 1026, 1035 (N.D.

tion helps explain why the human resources manager who searched the employee's phone in *Kaczmarek* was careful to state that he merely "counted up the number of [relevant] text messages" on the plaintiff's cell phone and "did not review any personal text messages or any other items in [the] cell phone."[297] In essence, the more content an employer reviews—particularly content unrelated to the legitimate objectives of the search—the more likely a court will conclude that the employer has infringed the employee's reasonable expectation of privacy.

From an employer's perspective, then, when a public or private employer wishes to search an employer-issued cell phone or seize its contents, the employer should carefully consider the factors identified above, along with any other relevant factors in the case, to determine whether the employee can reasonably expect privacy in the contents the employer wishes to review. Key factors that might reduce expectations of privacy, even for devices used exclusively by one employee, include clearly written and communicated policies authorizing searches and seizures of those devices, and employer actions that are narrow in scope and generally avoid the content of employee communications. In the end, there can be no one-size-fits-all determination regarding whether an employee can reasonably expect privacy in an employer-owned cell phone, as the variables identified above can lead to different outcomes in different cases.

2. Personal Cell Phones

Turning to searches of personal cell phones, in light of *Riley*, there can be no doubt that employees can generally expect privacy in the contents of their personal cell phones.[298] Although *Riley* involved a cell phone found on an arrestee,[299] a distinct context, *Riley* elevated personal cell phones to a unique Fourth Amendment position.[300] *Riley* indicated, for example, that personal cell phones may deserve even greater constitutional protection than what is owed to the home.[301]

Cal. 2014) ("This and other courts have concluded that there is no 'legally protected privacy interest and reasonable expectation of privacy' in electronic messages, 'in general.' Rather, a privacy interest can exist, if at all, only with respect to the *content* of those communications." (citations omitted)); *In re* Yahoo Mail Litig., 7 F. Supp. 3d 1016, 1040–41 (N.D. Cal. 2014) (discussing the importance of identifying particular content in intercepted e-mail).

297. Kaczmarek v. Cabela's Retail Ill., Inc., No. 1-14-3813, 2015 WL 6156352, at *3 (Ill. App. Ct. Oct. 16, 2015).

298. Riley v. California, 573 U.S. 373, 393–97 (2014) (discussing the privacy interests at stake in cell phone searches).

299. *See id.* at 386 (holding that police must generally secure a warrant before searching the contents of personal cell phones).

300. *See supra* notes 114–30 and accompanying text (discussing *Riley*).

301. On that note, *Riley* stated that, "[a] phone not only contains in digital form many sensitive records previously found in the home," such as bank statements, "it also

Riley also noted that the storage capacity of modern smart phones is massive and, by analogy to physical searches, is like housing a vast warehouse of information.[302]

Given the unique privacy concerns of the modern cell phone, this Article proposes a rebuttable presumption that employees of both public and private employers can reasonably expect privacy in the contents of a personal cell phone. Under this Article's proposal, this presumption could be defeated if an employer has implemented a clear and narrowly-defined policy permitting the employer to search or seize specified contents of a personally-owned device used for work-related purposes, as in a case like *Larios*.[303] As in *Larios*, however, this proposed exception would apply only if employees have voluntarily consented to the employer's policy, and only if the policy is justified by a legitimate business need to manage or review particular employment-related data contained within the phone.[304]

C. Overall Lawfulness of Cell Phone Searches and Seizures

In cases where an employee can reasonably expect privacy in the particular contents of his or her cell phone, the question becomes whether an employer's search or seizure of those contents is either unreasonable or highly offensive, depending on the type of employer. This section examines this ultimate inquiry for both public and private employers.

1. Public Employer Searches and Seizures

a. Employer-Issued Cell Phones

As discussed in the previous section, employees often have limited expectations of privacy in employer-owned cell phones, particularly where an employer's policy permits their inspection, making them more freely searchable by employers. Nevertheless, there will be times when a public employee can reasonably expect privacy in an employer-issued cell phone. In those cases, this Article argues, consistent with

---

contains a broad array of private information never found in a home in any form," such as an Internet search and browsing history or a collection of apps that reveal a person's hobbies and interests. *Riley*, 573 U.S. at 396–97.

302. *See id.* at 397.

303. *See supra* subsection III.B.2.

304. *See supra* subsection III.B.2. To be clear, both the *Larios* court and the Supreme Court in *Quon* assumed *arguendo* that a search occurred but ruled that the search was reasonable under the Fourth Amendment. *See* Larios v. Lunardi, 442 F. Supp. 3d 1299, 1310 (E.D. Cal. 2020); City of Ontario v. Quon, 560 U.S. 746, 760 (2010). Under Fourth Amendment precedents, however, notice and consent by an employee can impact both an employee's expectations of privacy as well as the ultimate reasonableness of a search. *See* Marc Chase McAllister, *GPS and Cell Phone Tracking of Employees*, 70 FLA. L. REV. 1265, 1305–10 (2018) (discussing the role of notice and consent in an employer-initiated GPS tracking case).

O'Connor and *Quon*, that such searches must be both reasonable at the inception and reasonable in scope.[305]

Of particular relevance under the *O'Connor* framework, this Article emphasizes the need for employers to properly limit the scope of their search to avoid accessing private information untethered from the specific work-related purpose for the search.[306] In *Quon*, for example, the Court emphasized the limited scope of the employer's review. 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 were more likely to be personal in nature.[307] Likewise, in *Larios*, although the case involved a personally-owned cell phone, the court distinguished between downloading the phone's entire contents, which was deemed an unreasonable seizure, and the relatively limited search of only the particular text messages that were relevant to the employee's act of misconduct, which was deemed reasonable.[308] In sum, when a public employer searches an employer-issued device to investigate employee misconduct (as in *Larios*) or for a noninvestigatory, work-related purpose (as in *Quon*), the employer should review no more content than necessary to accomplish the employer's objective. As a general rule, the less content that is reviewed, the more likely the search will be considered reasonable.

b. Personal Cell Phones

As previously discussed, there can be no doubt that employees can reasonably expect privacy in the contents of their personal cell phones, particularly in light of *Riley*.[309] Accordingly, the question becomes what makes a search of those devices lawful.

For searches by public employers, this Article argues that personally-owned cell phones are generally beyond the reach of the *O'Connor* workplace exception and should not be searched due to their unique capacity to hold immense amounts of private information. As articulated by *Riley*, modern cell phones generate privacy concerns that exceed even those found in the home, the area that has enjoyed the most

305. *See* O'Connor v. Ortega, 480 U.S. 709, 725–26 (1987).
306. *See id.* at 726 (explaining that two types of employer-initiated searches might fall within the scope of the *O'Connor* exception: (1) those made for a noninvestigatory, work-related purpose, such as entering an office to retrieve a needed file; and (2) those made as part of an investigation of work-related misconduct).
307. *Quon*, 560 U.S. at 761–62.
308. *See supra* notes 187–89 and accompanying text. Regarding the search, the court emphasized that the defendants restricted their search of Larios's phone to reviewing only his texts with confidential informant Mellow, and even further to a subset of those messages from the time period during which Larios and Mellow might have communicated through the device. *Larios*, 442 F. Supp. 3d at 1310.
309. *See supra* notes 114–30 and accompanying text (discussing *Riley*).

Fourth Amendment protection.[310] And just as courts have held that searches of an employee's home fall outside the "workplace context," so too should searches of personal cell phones.[311]

To be sure, *Riley* involved a warrantless search of a personally-owned cell phone conducted on the heels of an arrest, which is distinct from the employment setting. Nevertheless, the potential privacy concerns do not change simply because the phone is used by an employee, rather than an arrestee.[312] In addition, arrestees and employees are on similar Fourth Amendment ground, as both groups have reduced expectations of privacy as a class.[313] Yet, despite acknowledging that arrestees have "diminished privacy interests," *Riley* found that the "privacy-related concerns" in cell phones' digital data are so substantial that searching such data requires a warrant.[314] Employees personally-owned cell phones are entitled to at least the same protection. Quite simply, if "privacy-related concerns are weighty enough"[315] to require a warrant to search personal cell phones of arrestees, who on the whole have reduced Fourth Amendment protection, then those same privacy-related concerns are likewise weighty enough for employees, who also have reduced Fourth Amendment protection.[316]

Beyond *Riley*, for the *O'Connor* workplace exception to apply, the device at issue, or at least the particular contents of the device at is-

310. *See* Riley v. California, 573 U.S. 373, 396–97 (2014) (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 "many sensitive records previously found in the home" as well as "a broad array of private information never found in a home in any form"); *id.* at 401 ("Our holding, of course, is not that the information on a cell phone is immune from search; it is instead that a warrant is generally required before such a search, even when a cell phone is seized incident to arrest."); *see also* Port Auth. Police Benevolent Ass'n v. Port Auth. of N.Y. & N.J., No. 15-CV-3526 (KMW) (RLE), 2017 WL 4403310, at *5 (S.D.N.Y. Sept. 29, 2017) (refusing to apply the workplace exception outlined in *O'Connor* and noting that "the privacy interest in a person's cell phone is similar to, if not greater than, the privacy interest in one's home").

311. *Port Auth. Police Benevolent Ass'n*, 2017 WL 4403310, at *5.

312. First, the underlying digital data is generally the same. In addition, across the run of cases, the volume of private information on an employee's cell phone is likely similar enough to that found on the typical arrestee's phone to warrant the same Fourth Amendment protection. For these reasons, searches of employee cell phones demand the same Fourth Amendment protection.

313. *See supra* notes 40–41 and accompanying text.

314. *See Riley*, 573 U.S. at 392–93.

315. *Id.* at 392.

316. *See also* Maryland v. King, 569 U.S. 435, 463 (2013) (recognizing that in some searches, such as invasive surgery or a search of an arrestee's home, for which "the Court must 'balance the privacy-related and law enforcement-related concerns to determine if the intrusion was reasonable,' the privacy-related concerns are weighty enough that the search may require a warrant, notwithstanding the diminished expectations of privacy of the arrestee" (quoting Illinois v. McArthur, 531 U.S. 326, 331 (2001))).

sue, must be "related to work . . . and generally within the employer's control."[317] For most employees who bring their personal cell phone to work, that device would not typically meet this standard (similar to the closed "handbag, or a briefcase that happens to be within the employer's business address" described in *O'Connor*).[318] Simply put, in most cases, a personal cell phone brought to work is not an "item[ ] . . . related to work and . . . within the employer's control."[319] Accordingly, as *Port Authority* determined, the *O'Connor* workplace exception should not apply, leaving employee consent as the primary justification for such a search.[320]

On the issue of consent, as in *Larios*, searches of personally-owned cell phones by public employers might be permissible if an employer has implemented a clear and narrowly-defined policy authorizing such searches.[321] This proposed exception would apply, however, only if employees have voluntarily consented to the employer's policy. Moreover, as an aspect of reasonableness, this proposed exception would apply only if the employer's policy is justified by a legitimate business need to manage or review particular employment-related data contained within the phone, a requirement that is necessary to protect the generally private contents of most personal cell phones. In combination, these requirements would help ensure that the device at issue is sufficiently "related to work and . . . within the employer's control" to be subject to a warrantless search under *O'Connor*.[322]

2. Private Employer Searches and Seizures

Under the Fourth Amendment, what is reasonable depends on the context within which a search takes place.[323] Moreover, when the Supreme Court applies "traditional standards of reasonableness," including in the employment context, the Court typically weighs "'the promotion of legitimate governmental interests' against 'the degree to which [the search] intrudes upon an individual's privacy.'"[324]

317. O'Connor v. Ortega, 480 U.S. 709, 715 (1987).

318. *Id.* at 716.

319. *Id.* at 715.

320. Port Auth. Police Benevolent Ass'n v. Port Auth. of N.Y. & N.J., No. 15-CV-3526 (KMW) (RLE), 2017 WL 4403310, at *5 (S.D.N.Y. Sept. 29, 2017).

321. *See supra* subsection III.B.2 (discussing *Larios*).

322. *O'Connor*, 480 U.S. at 715.

323. *Id.* at 719 ("[T]o hold that the Fourth Amendment applies to searches conducted by [public employers] is only to begin the inquiry into the standards governing such searches . . . . [W]hat is reasonable depends on the context within which a search takes place." (alterations in original) (quoting New Jersey v. T.L.O., 469 U.S. 325, 337 (1985))).

324. Maryland v. King, 569 U.S. 435, 448 (2013) (alteration in original) (quoting Wyoming v. Houghton, 526 U.S. 295, 300 (1999)).

Under the tort of intrusion, a similar balancing of interests has been used when determining the overall offensiveness of an employer's search or seizure—one that balances the employer's legitimate business interests in intruding against the nature, manner, and scope of the intrusion.[325] On the employer's side, the typical private employer's interest in searching cell phones is usually no different than that for public employers, which the *O'Connor* Court described as "the efficient and proper operation of the workplace."[326] For example, in *Larios*, a Fourth Amendment case, the employer's interest in searching the personal cell phone of its employee was to determine "the scope of [Larios]'s communication with [confidential informant] Mellow and mitigate harm [to the employer] that might flow from his potential misconduct."[327] Similarly, in *Kaczmarek*, a tort of intrusion case, the employer searched the personal cell phone of one of its young, female employees to determine whether she was involved in an inappropriate relationship with an older manager, presumably to mitigate any disruption to the work environment.[328] In both cases, the employer's overriding interest was the same: to ensure the workplace was operating properly and efficiently.

On the employee's side, the nature, manner, and scope of intrusion can all impact the overall offensiveness of an employer's privacy invasion.[329] As used here, "nature" refers to the employee's privacy interest on which the employer intruded, such as an intrusion upon the employee's person, as opposed to her bag or briefcase.[330] "Manner" refers to the means the employer used in effecting the intrusion, which takes into account the possibility of employing less intrusive means.[331] "Scope" refers to the extensiveness or breadth of the intrusion when considered in light of the employer's underlying purpose for the action.[332] As discussed in this Article, these variables—nature,[333]

325. *See* RESTATEMENT OF EMP'T LAW § 7.06 (AM. LAW INST. 2015); *see also id.* cmt. a (noting that "[a]n intrusion upon an employee's protected privacy interest is actionable only when that intrusion is highly offensive to a reasonable person under the circumstances," and stating that "[t]he purpose of the highly offensive inquiry is to balance the degree of the intrusion against its private and social justifications").

326. *O'Connor*, 480 U.S. at 723.

327. Larios v. Lunardi, 442 F. Supp. 3d 1299, 1310 (E.D. Cal. 2020).

328. Kaczmarek v. Cabela's Retail Ill., Inc., No. 1-14-3813, 2015 WL 6156352, at *1–2 (Ill. App. Ct. Oct. 16, 2015).

329. RESTATEMENT OF EMP'T LAW § 7.06.

330. *See id*. § 7.02 (discussing various employee privacy interests).

331. This variable would consider, for example, an employer's use of a powerful telephoto lens to take pictures of an employee as she moves about inside her home, as opposed to simply observing those same activities in public. *See id.* § 7.06 cmt. e, illus. 8.

332. *See id.* § 7.06 cmt. f (recognizing, under the tort of intrusion, that the scope of an intrusion is relevant to determining whether it is wrongful, and that "[i]f the

manner,[334] and scope[335]—are also relevant under the Fourth Amendment in determining the overall reasonableness of a public employer's actions. Accordingly, the proposed framework of analysis is similar for both public and private employers.

Under this framework, when a private employer searches or seizes the contents of an employee's cell phone, it is critical to identify the precise reason for the employer's intrusion and weigh that against the nature, manner, and scope of the intrusion itself to determine its overall offensiveness.[336] When a private employer has a strong business justification for searching an employee's cell phone (as in a case like *Sunbelt Rentals* involving a former employee's likely violation of his non-disclosure and non-solicitation agreement) this makes the search less offensive.[337] If, however, the employer's justification for the search is relatively weak, the search becomes more offensive, especially if the cell phone is personally owned.

On the other side of the scale, the nature, manner, and scope of intrusion must be considered. Regarding the nature of intrusion, searches of personally-owned cell phones are potentially far more invasive of privacy than searches of employer-owned devices, given that personally-owned cell phones would typically contain more purely pri-

---

scope extends beyond the purpose of the intrusion in furthering the employer's legitimate business interest, the intrusion is unjustified").

333. As for the nature of the intrusion, this Article summarizes Fourth Amendment cases involving searches by public employers of both employer-issued and personally-owned devices under circumstances giving rise to differing expectations of privacy. *Compare* Port Auth. Police Benevolent Ass'n v. Port Auth. of N.Y. & N.J., No. 15-CV-3526 (KMW) (RLE), 2017 WL 4403310, at *4–5 (S.D.N.Y. Sept. 29, 2017) (involving an employer's search of personal cell phones that were not sufficiently related to work to fall within the scope of the workplace exception), *with* Larios v. Lunardi, 442 F. Supp. 3d 1299, 1319 (E.D. Cal. 2020) (involving an employer's search of a personal cell phone that contained the employer's work product). *See also* RESTATEMENT OF EMP'T LAW § 7.06 cmt. e (stating that "[t]he nature of the intrusion is related to the employee's reasonable privacy expectations in not revealing the information," which "in turn depends on how personal the information is, . . . and what degree of privacy the employer generally gives employee activities in the physical or electronic work location in question").

334. In *Larios*, for example, the court distinguished between downloading a phone's entire contents and a potentially more targeted acquisition of a string of text messages. *See* Larios v. Lunardi, 445 F. Supp. 3d 778, 784 (E.D. Cal. 2020) (finding unreasonable the employer's seizure of all data stored on Larios's cell phone to retrieve a single thread of texts, which the court described as "like watering a plant with a firehose," where "[t]he means far exceeds the need"); *see also id.* (stating that "[a] customized data withdrawal" of only the work-related text messages in Larios's cell phone "would have fallen squarely within the workplace inspection exception").

335. *See supra* notes 109–11 and accompanying text (discussing the limited scope of the search in *Quon*).

336. *See supra* note 17.

337. *See supra* section IV.A (discussing *Sunbelt Rentals, Inc.*).

vate content. Regarding manner of search, and as *Larios* demonstrates, when an employer is faced with alternative methods for uncovering certain cell phone data, the employer should select the least intrusive means available to reduce the overall offensiveness of the employer's actions.[338] Regarding scope of search, the more content the employer reviews—particularly content unrelated to the objectives of the search—the more likely the intrusion will be deemed highly offensive.

With this balancing of interests in mind, this Article argues that nearly any search of a personally-owned cell phone would be highly offensive under the tort of intrusion, with the exception of only the most narrowly-drawn searches authorized by some form of employee consent. Accordingly, this Article proposes that searches of personally-owned cell phones should be deemed permissible under the tort of intrusion only when employees have voluntarily consented to an employer's clear and narrowly-defined policy authorizing such searches, and only if the employer's policy is justified by a legitimate business need to manage or review particular employment-related data within the phone.

Finally, when a private employer wishes to search an employer-issued cell phone, where the nature of the intrusion is inherently less invasive, the employer should ensure it has a strong business-related justification for the search. As for the search itself, the employer should carefully limit the scope of its search to avoid accessing private information unrelated to the intrusion's justifications and should select the least intrusive means available for conducting the search. In essence, the employer's search should be tied to a legitimate business objective and should uncover the least amount of cell phone data necessary to accomplish that objective.

VI. CONCLUSION

As cases like *Riley* and *Port Authority* make clear, cell phones occupy a unique position in American privacy laws. As this Article has shown, when an employer wishes to search or seize the contents of an employee's cell phone, the employer should consider whether the employee can reasonably expect privacy in those contents and should carefully evaluate the overall reasonableness or offensiveness of its intrusion. In the end, a case-specific analysis must be conducted when determining whether an employer may lawfully search or seize the contents of an employee's cell phone. However, the principles identified in this Article will serve as helpful guides for employers and reviewing courts in specific cases.

338. *See supra* note 189.