Journal of Consumer Attorneys Associations for Southern California
ADVOCATE
September 2017 Issue

**Kevin Pease**
ATTORNEY ADVISOR AT DEPARTMENT OF LABOR

**Nicholas Starkman**
WOHLNER KAPLON CUTLER HALFORD & ROSENFELD

# Deflategate and the California workplace

## A COMMONSENSE APPROACH TO WORKPLACE INVESTIGATIONS INVOLVING PERSONAL CELL PHONES

Recent legal commentary and analysis of workplace cell phone investigations is hyper-technical, attempting to hedge against liability in language far removed from the day-to-day experience on the job. This article presents a fresh, commonsense approach to understanding the rights and responsibilities of parties to a workplace investigation by providing a basic analytical framework and detailing a range of outcomes that can be anticipated and avoided. Taking a "macro" view of personal cell phones and workplace investigations, this article will assist employers and employees in making sound decisions from the start.

Five-time Super Bowl champion Tom Brady began the 2016 NFL season with much fanfare – but not for his on-field theatrics. Instead, Brady served a four-game suspension for his role in the deflated-football scandal tagged "Deflategate." The fracas began when the NFL suspected Brady's personal cell phone had information relevant to its investigation into whether the New England Patriots underinflated balls to Tom Brady's specifications, making them easier to grip and giving Brady an unfair advantage in a playoff game.

While the details of Deflategate have been discussed extensively in many forums, including the Second Circuit Court of Appeals, *Nat'l Football League Mgmt. Council v. Nat'l Football League Players Ass'n,* (2d Cir. 2016) 820 F.3d 527, few commentators have homed in on the fact that at its core, the Deflategate saga is not about high-flown vendettas between some of the most recognizable names in sports. Boiled down, Deflategate concerns a common workplace issue that is the subject of increasing judicial analysis, namely: what are the "ground rules" for a workplace investigation involving information or data contained on an employee's personal cell phone?

This article presents a fresh, commonsense approach to understanding this complex area of the law that affects workplaces up and down the state of California. Included in this analysis are several critical scenarios which may arise during an investigation involving a cell phone search and thereby establish an employee's right to relief from his or her employer. Because time and space are a concern, this piece focuses solely on the private, non-unionized California workplace.

### The Fourth Amendment is the starting point

Employees and employers alike will have at least a peripheral understanding of the 4th Amendment to the U.S. Constitution, rendering it a helpful baseline for any legal analysis of a workplace investigation. The 4th Amendment to the U.S. Constitution protects "the right of the people to be secure in their...effects, against unreasonable searches." U.S. Const., amend. IV. Although not controlling in the private, civil employment context, the 4th Amendment's "reasonableness" requirement, particularly as it informs an employee's expectation of privacy, forms the foundation upon which judges, mediators, and arbitrators often begin their approach to analyzing workplace investigations.

For example, in *United States v. Ziegler* (9th Cir. 2007) 474 F.3d 1184, 1189, the Court observed that "…in the private employer context, employees retain at least some expectation of privacy in their offices." The court went on to assess whether a company investigation involving an employee's use of his office computer to browse and store child pornography violated Ziegler's expectation of privacy. Ultimately, the Court concluded that a number of factors defeated any employee objection to the investigation based on reasonableness, including: the company's ownership of the employee's workplace computer, the policy and practice of regular monitoring of employee technology usage, and a company policy prohibiting private use of company technology.

Similar factors are determinative of the reasonableness of a workplace investigation involving an employee's personal cell phone. They include, as longtime labor and employment practitioner Philip Gordon points out, "the strength of the employer's suspicion that the smartphone contains evidence of unlawful conduct or policy violations; the time, place and manner of the search; and the nature and scope of the search." (Gordon, Phillip. *Five Lessons Learned From California v. Riley*, Littler Mendelson P.C. (2014), https://www.littler.com/five-lessons-employers-california-v-riley (last visited July 2, 2017).) Without the consideration of the reasonableness of a workplace investigation involving an employee's cell phone as gleaned from Fourth Amendment case law, the efficacy of that investigation could be jeopardized and a claim for relief may accrue to the employee.

### Cell phones as legally distinct from other items in modern life

After considering reasonableness factors at the beginning stages of a workplace investigation, the next step for all parties to the employment relationship is to internalize a key element of cell phones: they are legally different from other items of modern life. The ever-evolving photographic, recording, storage and cloud access capabilities of cell phones and other mobile technologies pose a distinct challenge to the legal

*See Pease & Starkman, Next Page*

Journal of Consumer Attorneys Associations for Southern California
ADVOCATE
September 2017 Issue

system's ability to keep pace. As one district court in California has observed: "The storage capacity of today's cell phone is immense…' [t[hat information is, by and large, of a highly personal nature: photographs, videos, written and audio messages (text, email, and voicemail), contacts, calendar appointments, web search and browsing history, purchases, and financial and medical records.'" (*United States v. Phillips* (E.D. Cal. 2014) 9 F. Supp. 3d 1130, 1141, citing *United States v. Cotterman* (9th Cir.2013)709 F.3d 952, 957 (en banc).) In attempting to cram cell phones into existing legal structures, counsel have trotted out a litany of analogies, including likening cell phones to: a pager or a computer memo book; a closed container, a diary, a computer, and a cigarette pack and a footlocker. (See, e.g., *People v. Diaz* (2011) 51 Cal.4th 84, 92.) Still, courts recognize there is nothing quite like a cell phone in terms of the range of potentially accessible data and privacy interests implicated and have been historically at somewhat of a loss to classify them.

The chorus of attorneys and judges clambering for guidance concerning phones apparently reached the ears of the United States Supreme Court justices, who determined unanimously in *Riley v. California* that, absent a warrant, police are generally prohibited from searching a cell phone following an arrest. (*Riley v. California* (2014) 134 S.Ct. 2473, 2494-96.) Reinforcing the notion that cell phones are a category unto themselves, Chief Justice Roberts noted: "Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans 'the privacies of life.'" (*Ibid.*) To bring *Riley* from the criminal into the employment context, employers and employees alike should be vigilant in recognizing that personal cell phone searches require special care and consideration beyond that which is accorded to searches of an employee's office, backpack, purse, wallet, or other objects.

## Pitfalls in workplace investigations: causes of action

The issue of whether private employers are entitled to seize and search their employee's private cell phones turns on context. Improper searches and seizures potentially give rise to several different causes of action. Generally, these claims hinge not on ownership of the phone, but on a balancing test applied to the facts at hand, i.e., whether the Employer's interest in the information on the phone justifiably outweighs the privacy interest the employee has in their own data, texts, photos and videos, etc. Invasion of privacy, wrongful discharge, and intrusion into private matters are several of the major causes of action an employee may allege against an employer based on improper conduct around the cell phone search.

## Invasion of privacy

The lead case on invasion of privacy under the California constitution and the privacy violation based on the common law tort of intrusion into private matters is *Hernandez v. Hillsides, Inc.* (2009) 47 Cal.4th 272. In that case, the employer, a private, non-profit residential facility for neglected and abused children, installed a camera in the office of two employees without their knowledge and consent in order to "catch" a third party who was utilizing employer computers after hours to access pornography. The camera never actually recorded during business hours. Nonetheless, when the employees learned of the camera, they sued, alleging a California constitutional claim of invasion of privacy and intrusion into private matters. The California Supreme Court noted that these sources of privacy protection are "not unrelated" and analyzed each cause of action and its elements.

In a successful claim based on invasion of the California constitutional right of privacy, a plaintiff must first demonstrate that he or she has a legally cognizable privacy interest. Such interests boil down to carrying out personal tasks without being surveilled as dictated by the norms and mores of the time. For example, one of the plaintiffs in *Hernandez* pointed out that she would change into athletic clothes before working out at the end of the day.

Second, a plaintiff's privacy interest must be reasonable (note the Fourth Amendment's influence here). Whether an interest is reasonable is evaluated on a case-by-case basis in the context of the situation. While that is of little help to the reader here, the Court in *Hernandez* did note that a reasonable privacy interest involves the opportunity to be notified in advance and provide consent.

Finally, the intrusion must be serious – the Court describes it as an "egregious breach of social norms." One can imagine a scenario where an employer confiscates a private cell phone and publishes photos, videos, texts, and data from the phone on social media or otherwise without the employee's consent as potentially reaching this threshold. Conversely, a defendant may prevail in a state constitutional privacy case by proving that the invasion of privacy is justified because it substantively furthers one or more countervailing interests based on a general balancing test. This can be accomplished by demonstrating that less intrusive means were not immediately available.

A word of caution on *Hernandez*: while this case is helpful for understanding rights and responsibilities under California law, federal courts have distinguished *Hernandez* in matters involving the Fourth Amendment and the secret recording of employees, particularly where the recording is done in areas where employees perform non-work tasks. (See, e.g., *Richards v. County of Los Angeles* (C.D. Cal. 2011) 775 F.Supp.2d 1176, 1186.)

## Intrusion into private matters

The *Hernandez* case also addressed the elements of a common law action for intrusion into private matters. The employee must prove two elements: (1) intentional intrusion into a private place, conversation or matter, including private affairs or concerns (2) in a manner highly offensive to a reasonable person. Whether this cause of action translates to intrusion into a device (as opposed to intrusion into an office or other potentially private area in *Hernandez*) is still a matter of debate. Yet, case law addressing electronic intrusion into an employee's privacy indicates some protection to employees. While it may be from New

*See Pease & Starkman, Next Page*

Journal of Consumer Attorneys Associations for Southern California
ADVOCATE
September 2017 Issue

York, *In re Petition of John W. Danforth Grp., Inc.*, No. 13-MC-33S, 2013 WL 3324017 (W.D.N.Y. July 1, 2013) provides some guidance. In that case, the court found that a generalized concern that an employee might destroy evidence relevant to a lawsuit was not a compelling enough reason to require the phone to be turned over before the litigation even commenced. Still, the breadth of this protection is unclear. At the very least, unknowingly accessing a claimant's cell phone through secret electronic means would be an unlawful intrusion into privacy. Physically taking a cellular phone without permission to search it for information would raise the question of liability and support a finding for employee. Since context is key, concerns for safety may balance the scales in favor of an employer.

### Wrongful discharge in violation of public policy

If an employee refuses to comply with a request to turn over data from a private cell phone and the employer terminates the employee, may the employer be liable for wrongful discharge? Privacy is an "inalienable right" enumerated in the California constitution. Article 1, Section 1 states: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and *privacy*." Cal. Const., art. I, § 1. (emphasis added). Case law is silent on this matter, but we do have some clues. Employees discharged for refusing to waive their constitutional right of privacy may assert a claim for wrongful discharge in violation of public policy against the employer. (*Green v. Ralee Eng'g Co.* (1998) 19 Cal.4th 66, 79.) Further, firing an employee for asserting a *reasonable* claim in *good faith* may be actionable even if the employee fails to prove the employer actually violated the law. (*Barbosa v. Impco Techs., Inc.* (2009) 179 Cal.App.4th 1116, 1123.) Ultimately, this is a matter of first impression yet to be considered by the Courts.

### State law

California Penal Code section 632, the Stored Communications Act, the Federal Wiretapping Act and the federal Stored Communications Act are examples of statutes that reduce the importance of context. Under California law, "(e)very person who, intentionally and without the consent of *all* parties to a confidential communication, by means of any electronic amplifying or recording device, eavesdrops upon or records the confidential communication" shall be subject to fine or imprisonment. (Cal. Penal Code § 632.) Persons injured by a violation of Penal Code section 632 may bring a civil action for treble damages or a statutory penalty of $5,000 for each violation, plus injunctive relief. (Cal. Penal Code § 637.2.) Should an employer rely on an electronic amplifying or recording device to eavesdrop or record an employee's confidential communications on their cell phone without consent, they may be opening themselves to criminal and/or civil liability.

### Federal law

Various federal laws may limit an employer's ability to search and seize an employee's private cell phone. For example, the Federal Wiretapping Act, 18 U.S.C.A. §§ 2510 *et seq*., which prohibits capturing certain communications without the consent of the communicating party, impacts an employer's consideration of how to obtain critical information from a personal phone. In theory, this protection would prevent a private employer in California from monitoring an employee's private cell phone. In addition, federal law protects employees' right to communicate with each other while at work on unionization and other matters of common concern, such as wages, hours and working conditions. (29 U.S.C.A. § 157; see also *Beth Israel Hosp. v. NLRB* (1978) 98 S.Ct. 2463, 2469; *Purple Commc'ns, Inc.*, 361 NLRB No. 126 (Dec. 11, 2014).) These protections might also prevent an employer from searching and seizing an employee's cell phone on the grounds that it contains communication about concerted activities for the purpose of collective bargaining or other mutual aid or protection.

### Conclusion

In sum, Tom Brady and the highly visible Deflategate investigation raise important issues for California workplaces, namely: what are the rights and responsibilities of an employer who seeks information or data from the private cell phone of an employee? While cell phone technology is evolving at breakneck speed and the law struggles to keep pace, the foundational elements of workplace investigations involving personal cell phones remain the same.

First, the Fourth Amendment, while not controlling, acts as a yardstick to measure the reasonableness of a private cell phone search. The warrant-type factors are especially helpful in this regard. Further, cell phones require a different privacy analysis than other items in modern life given the range and accessibility of private information**.** Finally, cell phone searches can give rise to multiple torts, state constitutional and statutory claims and common law claims, which turn on the context of the search. Ultimately, whether either the California Legislature or Congress choose to legislate the issue will determine whether there will be increased clarity.

*Kevin Pease has been an Attorney Adviser in the Office of Administrative Law Judges in the Department of Labor since 2015. He graduated in the top 5% from UC Davis School of Law in 2013. Immediately after law school he worked as a Civil Rights Fellow at the California Department of Fair Employment and Housing. His specialties include worker's compensation and employment law.*

*Nicholas Starkman is a labor and employment attorney with four years of experience counseling individuals, employers, and labor organizations. He graduated in 2013 from UC Davis School of Law where he received the Clinical Legal Education Association's Outstanding Student Award for his work in the federal court and U.S. immigration systems on behalf of immigrants. He currently represents jointly managed labor and employer Taft Hartley Trust Funds in ERISA litigation in federal court.*