"Bring Your Own Devices": A Cautionary Tale for Public Employees During Investigatory Searches

by JULIE CHOW*

Introduction

We live in a society where technological advancements have placed access to the world literally at our fingertips. We can simultaneously purchase a can of ketchup-flavored Pringles chips from Canada, read up on the sports game we missed, check our work email remotely, and chat with a relative across the country via webcam—all without ever having to get out of bed. All this is made possible through a vast array of handheld electronic personal devices, such as cellphones, tablets, and PDAs. For many Americans, these devices are crucial to organizing daily activities, maintaining social relationships, and staying informed of current world events and political news. Thus, it is no surprise that many Americans have begun to rely on such personal devices to meet the ever-pressing demands of both work and personal life. The line between "work time" and "personal time" becomes blurred, however, as more employees find themselves responding to emails, finalizing those last documents for tomorrow's important meeting, and accessing company databases after hours on their personal devices. For some, this may occur with their employer's authorization, while for others, this may occur in the absence of their employer's knowledge. This relatively new phenomenon whereby employees use their personal electronic devices for work purposes is referred to as "Bring Your Own Device," or "BYOD."[1] This growing

* J.D. Candidate 2014, University of California, Hastings College of the Law; B.S. 2004, University of California, Los Angeles. I would like to thank the editors of the *Hastings Constitutional Law Quarterly* for their guidance and patience throughout the editing process. I would also like to thank Professor Roberta Thyfault for her inspiration in writing this. Lastly, I thank my family and friends for their steadfast support and love—I could not have made it through this journey without each of you.

trend raises potentially problematic issues for both employers and employees—especially in the area of employee privacy for those who work in state and local government.

The Fourth Amendment to the United States Constitution established the requirement of probable cause to protect individuals from unreasonable searches and seizures by government agents.[2] With relatively little case law outlining the scope of public employees' privacy in the workplace, courts have been cautious in addressing the privacy expectations of public employees.[3] This has led courts to carefully balance employees' privacy rights under the Fourth Amendment with employers' interests in carrying on the work of the governmental agency to meet the public's needs.[4]

This area becomes particularly precarious when delimiting employees' privacy rights with respect to electronic devices used in the workplace, such as a computer's hard drive or an employer's email system. Though departmental policies may help provide guidelines to avoid potential privacy violations, uncertainty exists in the absence of such policies or when existing departmental policies inadequately address these issues. As such, courts will likely face this issue in the near future due to the continuing rapid pace of technological progress and the increased use of personal devices in the workplace.

In the absence of clearly defined departmental policies, employees' privacy interests are vulnerable to intrusion, particularly during the investigatory process when an employee is the subject of a workplace investigation. These workplace investigatory procedures, along with judicially enacted standards from case law, tend to favor the employer while failing to adequately protect the privacy interests of public employees. This scenario calls for the adoption of a more rigid standard to protect the privacy rights of public employees when

1. Tony Bradley, *The Pros and Cons of Bringing Your Own Device to Work*, PCWORLD (Dec. 20, 2011, 10:42 PM), http://www.pcworld.com/article/246760/pros_and_cons_of_byod_bring_your_own_device_.html.

2. U.S. CONST. amend. IV (providing that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause . . . .").

3. O'Connor v. Ortega, 480 U.S. 709, 719–20 (1987) ("In the case of searches conduced by a public employer, we must balance the invasion of the employee's legitimate expectations of privacy against the government's need for supervision, control, and the efficient operation of the workplace.").

4. *See id.*

it comes to the ability of an employer to access an employee's personal electronic device during workplace investigations.

This Note examines the constitutionality of applying existing public employee privacy protections and standards to electronic personal devices ("BYODs") owned by employees during the course of public employer-conducted workplace investigations. Part I examines the use of BYODs in the workplace and the current protections in place for public employer-owned electronic devices. Part II analyzes the realities of the investigatory and disciplinary process and discusses the vulnerabilities public employees face. Part III asserts that applying current standards to employee-owned electronic devices would be detrimental to the privacy rights of employees, given the existing vulnerabilities outlined in the prior sections, and recommends that the probable cause standard be applied for investigatory searches of BYODs.

I. The History of Personal Devices in the Workplace and the Scope of Public Employee Privacy Rights During Workplace Searches

A. The Use of BYODs in the Workplace

Rapid technological advancements have influenced how business is conducted in the workplace. Where it was once the norm for employees to use employer-provided electronic devices, more employees are now using their own personal devices to carry out their work duties.[5] This behavior—which employees may engage in at the encouragement, authorization, or incognizance of their employers—is referred to as "Bring Your Own Device," or "BYOD."[6] Within the BYOD trend, employers permit and even encourage employees to bring their own mobile and electronic devices to work to access company data and applications.[7] Such devices include mobile phones, smartphones, laptops, tablets, and other similar electronic communication devices.[8]

5. *See* Tony Bradley, *When Alien Hardware Invades: 4 Keys to BYOD Success*, PCWORLD (Feb. 28, 2013, 3:30 AM), http://www.pcworld.com/article/2029540/when-alien-hardware-invades-4-keys-to-byod-success.html.

6. *See id.*

7. *Id.*; *see also* Bradley, *supra* note 1.

8. Charles McLellan, *Consumerization, BYOD and MDM: What You Need to Know*, ZDNET (Feb. 1, 2013, 6:00 PM), http://www.zdnet.com/consumerization-byod-and-mdm-what-you-need-to-know-7000010205/.

The increase in employees utilizing their own devices for work purposes occurs for various reasons. Some companies do so to stay competitive with larger companies.[9] Some have adopted BYOD policies to reduce the costs of having to constantly purchase, maintain, and upgrade equipment.[10] For smaller companies and for those with limited resources, this is especially attractive in helping to minimize overhead costs.[11] Though larger businesses may be able to provide the latest electronic communication gadgets to their employers, this is not always feasible for smaller companies.[12] Permitting employees to use personal devices that are more familiar and comfortable to the employees themselves also encourages productivity and improves operational efficiencies.[13] This policy may further boost morale by allowing for more flexible work hours.[14] The implementation of BYOD use in workplaces may also facilitate teamwork and collaboration, help to foster creativity, and speed innovation.[15] BYOD use also allows employees to reduce the number of devices they have to carry since they can utilize the same device for work and personal use.[16]

The concept of utilizing one's personal device for work-related purposes has particularly flourished in the fields of information technology ("IT"), finance, and media, where prompt communication is vital.[17] In a survey conducted of over 600 business and IT

9. *See* Bradley, *supra* note 1.

10. *Id.*

11. *Id.*

12. *See* Don Schoen, *Find IT Tools That Fit How You Do Business*, BLOOMBERG BUSINESSWEEK (Dec. 1, 2010), http://www.businessweek.com/smallbiz/tips/archives/2010/12/find_it_tools_that_fit_how_you_do_business.html.

13. *Id. See also* Press Release, Dell, Dell Unveils Global BYOD Survey Results: Embrace BYOD or Be Left Behind (Jan. 22, 2013), *available at* http://www.dell.com/Learn/us/en/uscorp1/secure/2013-01-22-dell-software-byod-survey?c=us&l=en&s=corp.

14. VANSON BOURNE, BYOD: PUTTING USERS FIRST PRODUCES BIGGEST GAINS, FEWER SETBACKS, *available at* http://software.dell.com/documents/byod-putting-users-first-produces-biggest-gains-fewest-setbacks-datasheet-19142.pdf.

15. *Id. See also* Press Release, Avanade Inc., Global Survey: Companies Enable Employee Use of Consumer Technologies; Report Positive Impact on Sales, Profits and Employee Satisfaction (Jan. 29, 2013), http://www.avanade.com/Documents/Press%20Releases/work-redesigned-press-release.pdf.

16. Pamela S., *BYOD Spells Danger: The Bring Your Own Device Debacle*, IPOST BLOG (Feb. 4, 2013), http://www.ipost.com/blog/cloud_computing/byod-spells-danger-the-bring-your-own-device-debacle/.

17. *See* McLellan, *supra* note 8.

executives, 60% reported employees using personal devices.[18] In another survey conducted of over 1,400 IT executives around the world, 70% said they believed BYODs could boast employee productivity and customer response time, and 59% said they felt their company would be at a competitive disadvantage if they did not implement BYOD use.[19]

BYOD practices have also extended to public employers and government agencies. For example, in 2012, the Equal Employment Opportunity Commission ("EEOC") implemented a BYOD program.[20] The Federal Aviation Administration ("FAA") followed suit.[21] These programs were implemented due to budgetary issues and were viewed as a way to cut costs.[22] A survey also showed that many public employees have already begun to use their personal devices for work-related purposes, without considering whether their employers had ever authorized such use.[23] While the EEOC and the FAA were prepared, that is not always the case for governmental organizations.[24] The use of personal devices for work-related purposes raises privacy implications under the Fourth Amendment by highlighting the issue of whether employers may search these devices for work purposes, and if so, under what standards.

B. Scope of Public Employees' Reasonable Expectation of Privacy During Workplace Searches

i. O'Connor v. Ortega*: The Standard of Reasonable Expectation in the Workplace*

The Supreme Court first examined the issue of employees' workplace privacy rights in *O'Connor v. Ortega*, which centered on

18. Sam Narisi, *Survey: BYOD Increases Profits, Productivity and Workplace Morale*, FINANCE|TECH NEWS (Feb. 4, 2013), http://www.financetechnews.com/survey-byod-increases-profits-productivity-and-workplace-morale/.

19. Dell Press Release, *supra* note 13.

20. GovPlace, *EEOC Counters Budget Cuts with BYOD Policy*, http://www.govplace.com/2012/08/eeoc-counters-budget-cuts-with-byod-policy/ (last visited Mar. 3, 2014).

21. Emily Jarvis, *DorobekINSIDER Live—Experts Weigh in on BYOD Lessons Learned*, GOVLOOP (Feb. 20, 2013), http://www.govloop.com/profiles/blogs/dorobek insider-live-experts-weigh-in-on-byod-lessons-learned.

22. *Id.*; GovPlace, *supra* note 20.

23. FORRESTER CONSULTING, BYOD IN GOVERNMENT: PREPARE FOR THE RISING TIDE (Sept. 3, 2012), *available at* http://www.cisco.com/web/offer/grs/101209/5/cisco_forrester_tlp_2.00.pdf.

24. *Id.* at 7.

the privacy rights of public employees during office searches.[25] Ortega, a physician and psychiatrist at a state hospital, was the subject of a workplace investigation concerning various allegations of inappropriate conduct.[26] While he was on administrative leave pending investigation of the charges, hospital officials allegedly searched his office and took personal items from his desk and filing cabinets in order to identify and secure the state property.[27] These items were then used in administrative proceedings that resulted in Ortega's discharge.[28]

The Court found that the employer's search may have been reasonable under the circumstances.[29] The Court adopted a standard to assess a public employer's intrusion on an employee's privacy that took into consideration the operational realities of the workplace.[30] Although, as a general matter, all nine Justices recognized that the employee had a reasonable expectation of privacy to his desk and file cabinets since he did not share these areas with other employees,[31] they were unable to agree on whether the search itself was reasonable.[32]

a. Plurality's Generalized Approach Ultimately Favors Employers by Failing to Consider the Distinction Between Investigatory and Non-investigatory Searches

The plurality, led by Justice Sandra Day O'Connor, noted that government employees retained their Fourth Amendment rights at work and that such expectations of privacy at one's workplace are based upon societal expectations that are reviewed on a "case-by-case" basis.[33] The plurality noted that the reasonableness of the search must be assessed by "balanc[ing] the nature and quality of the intrusion on the individual's Fourth Amendment interests against the importance of the governmental interests . . . ."[34] Thus, in a

25. O'Connor v. Ortega, 480 U.S. 709, 711–12 (1987).
26. *Id.* at 712.
27. *Id.* at 713.
28. *Id.*
29. *Id.* at 728–29.
30. *Id.* at 717.
31. *Id.* at 719, 31, 32–33.
32. *Id.* at 732 (Scalia, J., concurring), 732–33 (Blackmun, J., dissenting).
33. *Id.* at 717–18 (plurality opinion).
34. *Id.* at 719 (quoting United States v. Place, 462 U.S. 696, 703 (1983)).

workplace search conducted by a public employer, the "invasion of the employee's legitimate expectations of privacy" had to be balanced against the "government's need for supervision, control, and the efficient operation of the workplace."[35]

The plurality affirmed that a search without proper consent is unreasonable unless authorized by a valid search warrant based on probable cause.[36] The plurality also recognized exceptions, however, where "special needs" would make the warrant requirement impracticable.[37] The plurality noted that "[t]he operational realities of the workplace . . . may make some employees' expectations of privacy unreasonable when an intrusion is by a supervisor rather than a law enforcement official."[38] Requiring an employer to obtain a warrant in order to access an employee's office, desk, or file cabinets for work-related purposes would seriously disrupt routine business, interfere with the efficient operation of the agency, and impose intolerable burdens on public employers.[39] Supervisors and other employees may need to access a file or a report in an employee's office while the employee is away, and supervisors "may need to safeguard or identify state property or records in an office in connection with a pending investigation into suspected employee misfeasance."[40] In addition, the plurality reasoned that employers are less familiar with the subtleties of the probable cause standard than is law enforcement.[41]

Acknowledging that a factual dispute arose over whether the search of Ortega's office was a non-investigatory, work-related intrusion, or an investigatory search for evidence of suspected work-related employee misfeasance, the plurality attempted to outline a standard for reasonableness that allowed employers "wide latitude" to enter employee offices.[42] Consequently, the plurality held that the aforementioned types of workplace searches should be subject to a

35. *Id.* at 719–20.

36. *Id.* at 720.

37. *Id.* (citing New Jersey v. T.L.O., 469 U.S. 325, 351 (1985) (permitting school officials to conduct searches of students upon reasonable suspicion of contraband)); *see also* Terry v. Ohio, 392 U.S. 1, 28 (1968) (permitting an officer to conduct a limited search for his protection based on reasonable suspicion).

38. *Id.* at 717 (emphasis omitted).

39. *Id.* at 720.

40. *Id.* at 722.

41. *Id.* at 724–25.

42. *Id.* at 723.

reasonableness standard.[43] This reasonableness standard entailed the following two-step analysis: (1) assessing whether the search itself was justified at its inception; and (2) assessing whether the search was actually conducted in a manner reasonably related in scope to the circumstances that justified the search initially.[44] However, both Justice Antonin Scalia's concurring opinion[45] and Justice Harry Blackmun's dissenting opinion[46] criticized this standard as being devoid of content and too abstract to provide clear guidance.

In creating this exception to the warrant requirement, the Court failed to provide boundaries regarding the power it inherently delegated to employers. By allowing the employer to search the employee's workspace, the Court allowed the employer to simultaneously gather evidence for its pending investigation against the employee.[47] The Court failed to recognize the fundamental conflict of interest inherent in a situation where the same employers who are responsible for verifying or safeguarding property are also those who are seeking to impose disciplinary action against an employee.[48] Justice Blackmun and the three Justices who joined him in his dissent were the only ones who recognized this pitfall.[49]

b. Justice Blackmun's Approach both Recognizes the Distinction Between Investigatory and Non-Investigatory Searches, and Takes into Consideration the Inevitable Convergence of Work and Personal Activities

In his dissent, Justice Blackmun shed light on the imbalance that lies between employers and employees in the context of work investigations. He properly characterized the employer's search as "investigatory in nature," because it was "aimed primarily at furthering investigative purposes."[50] There was no evidence to suggest the employee had removed property such that an inventory was needed, or that the employer had prepared a formal inventory of

43. *Id.*
44. *Id.*
45. *Id.* at 730 (Scalia, J., concurring).
46. *Id.* at 748 (Blackmun, J., dissenting).
47. *Id.* at 736.
48. *Id.* at 735–36.
49. *Id*.
50. *Id.* at 736.

what was found.[51] Rather, the dissent noted that the employers had rummaged through the employee's belongings and seized personal items, which were then used at a later termination proceeding.[52] Justice Blackmun concluded there was no special need to dispense with the warrant and probable cause standard since, based on these facts, requiring a warrant would not have been overly burdensome.[53]

Justice Blackmun noted that the extent of an employee's expectation of privacy often depends on the "nature of the search."[54] He emphasized that the plurality's balancing test was to be used only in "exceptional circumstances" *after* determining that special needs "[made] the warrant and probable-cause requirement impracticable," such that the government employer could not obtain a warrant "without sacrificing the ultimate goals to which a search would contribute."[55] While he acknowledged that such exceptions to the warrant requirement may be necessary, it did not justify dispensing with a warrant in *all* searches by the employer.[56] Justice Blackmun pointed out that the Court could still conclude that the traditional warrant requirement standard was nonetheless suitable, even in instances where a special need arose that called for balancing.[57] The plurality did expressly limit its proposed reasonableness standard to the two types of searches in dispute by the parties: the non-investigatory work-related search and the investigatory search for evidence of work-related employee misconduct.[58] Justice Blackmun noted, however, that this limitation was illusory because almost all searches fall under one of the two categories; furthermore, despite clear distinctions, the plurality applied the same standard to both categories.[59]

In addition, Justice Blackmun was cognizant of the realities of modern times.[60] He noted that the workplace has become "another

51. *Id.*

52. *Id.*

53. *Id.* at 745 & n.10.

54. *Id.* at 738.

55. *Id.* at 741.

56. *Id.* at 745 & n.9.

57. *Id.* at 745 (citing Camara v. S.F. Mun. Ct., 387 U.S. 523 (1967), which held administrative search in absence of warrant for possible violations of city's housing code violated Fourth Amendment requirement of probable cause).

58. *Id.* at 723.

59. *Id.* at 746.

60. *Id.* at 739–40.

home for most working Americans."[61] He further stated that the "tidy distinctions . . . between the workplace and professional affairs, on the one hand, and personal possessions and private activities, on the other, do not exist in reality," and the "operational realities of the workplace" were such that simply leaving one's personal belongings at home to avoid exposing them at work, as proposed by the plurality, is not practical.[62]

O'Connor laid the groundwork for assessing work-place searches by public employers. Though Justice Blackmun's dissent was more mindful of the distinction between the types of searches conducted by an employer and the need to safeguard employee privacy, the plurality's reasonableness standard prevailed. This framework, based on nonelectronic workplace items such as a desk and filing cabinet, would be extended over two decades later to electronic workplace devices in *City of Ontario v. Quon*.[63]

ii. City of Ontario v. Quon*: Electronic Workplace Devices*

In 2010, the Court first applied the *O'Connor* standard to an electronic communication device in *City of Ontario v. Quon*. In *Quon*, the Court addressed the issue of whether an employer's work-related review of a transcript of an employee's pager messages violated the employee's right to privacy.[64] Quon, a police officer, filed an action against the city, asserting a violation of his Fourth Amendment rights after the police department conducted a review of the text messages he transmitted through a pager provided to him by the city for work-related purposes.[65] The review was conducted after employers noticed the employee, along with other employees, were exceeding the allotted number of messages permitted under the department's contract with the carrier provider.[66] Upon review of Quon's messages, the department learned that many were not work related and some were sexually explicit.[67] Although the messages that the employee sent while off duty were redacted, the city subsequently

61. *Id.* at 740.
62. *Id.* at 739–40.
63. City of Ontario v. Quon, 130 S. Ct. 2619, 2624 (2010).
64. *Id.*
65. *Id.* at 2625.
66. *Id.*
67. *Id.* at 2626.

used a transcript of the remaining messages as a basis for disciplining Quon for violating department rules.[68]

In a unanimous decision, the Court held that the city's review of the employee's text messages was reasonable, even if the employee had a reasonable expectation of privacy.[69] The Court applied the same two-step analysis established in *O'Connor* for determining reasonableness: (1) examining whether the search was justified at its inception; and (2) whether it was reasonable in scope for its purpose without being excessively intrusive.[70] Under the first prong, the Court found that the search was justified at its inception because there were reasonable grounds to believe the search was necessary to determine if the character limit on the city's contract was sufficient to meet operational needs, thus furthering a non-investigatory work-related purpose.[71] Under the second prong, the Court held that the scope was reasonable because reviewing a transcript of the employee's messages was an efficient and expedient way to determine whether the overages were personal or work-related.[72] Furthermore, the search was not excessively intrusive because the employee's off-duty messages had been redacted, and the employer had only reviewed transcripts for two months, despite additional overages in other months.[73]

The Court came to a general consensus by concluding that there were reasonable grounds to believe the search was for a non-investigatory, work-related purpose.[74] In applying the same standard used in *O'Connor*, the Court declined to prescribe how technological devices might impact employee privacy expectations in the future.[75] This will be problematic as electronic devices continue to permeate the workplace environment with the advancement of technology. In addition, the Court failed to recognize the distinction between non-investigatory, work-related searches and investigatory searches for evidence of work-related employee misfeasance, or how the type of search would impact the standard established in *O'Connor*.

68. *Id.*
69. *Id.* at 2630.
70. *Id.* at 2631.
71. *Id.*
72. *Id.*
73. *Id.*
74. *Id.* at 2630.
75. *Id.*

II. Some Background on Workplace Investigation (and Issues Arising for Public Employees)

It is crucial to recognize the difference between non-investigatory, work-related searches (such as those conducted for inventory purposes), and investigatory searches for evidence of work-related employee misconduct because the type of search influences both the public employer's and the employee's interests when applying the *O'Connor* standard.[76] The investigatory process implemented in civil service employment places the employee and the employer in an adversarial situation, and it allows an employer wider latitude to gather evidence to be used against the employee, as this Note will discuss.

A. Typical Steps in a Workplace Investigation

A typical workplace investigation in the public sector may begin with an allegation of misconduct raised by an employee's supervisor, a co-worker, or a member of the public.[77] The investigator for the employer, typically someone designated from or by the personnel office, will usually begin a course of fact-finding that involves collecting information from witnesses and gathering other corroborating evidence.[78] The investigator will interview the initial complainant, other witnesses, and the accused employee, and will then also gather relevant documents and photographs.[79] An investigation involving the falsification of attendance records, for example, may include reviewing the employee's sign-in sheets, as well as other attendance documentation used by the employee's office such as attendance emails and time-off request forms. If the investigator determines that an employee did engage in workplace misconduct or failed to perform his or her duties, the employee may

76. *See* O'Connor v. Ortega, 480. U.S. 709, 723–24 (1987).

77. Louis Klein, *Viewpoint: The razor's edge: Public agency concerns when conducting a workplace investigation*, AM. CITY & CNTY (June 16, 2010), http://americancityandcounty.com/commentary/workplace-investigation-concerns-20100616.

78. *See, e.g.*, *Workplace Investigations – Basic Issues for Employers*, TEX. WORKFORCE COMM'N, http://www.twc.state.tx.us/news/efte/workplace_investigations_basics.html (last visited Mar. 3, 2014).

79. *See* The Human Equation, *Human Resource Procedure Guide: Conducting Workplace Investigations*, at 2 (1998), *available at* http://www.setnorbyer.com/pdf/HRProcedureGuideWorkplaceInvestigations.pdf.

be subject to corrective or adverse action.[80] Corrective actions include informal counseling and verbal instruction, which are intended to improve the employee's performance to an acceptable level or to prevent continued misconduct.[81] If a corrective action fails or the employee's conduct is egregious enough, the public employer may initiate a formal disciplinary action, also referred to as an adverse action.[82] Adverse actions are disciplinary legal actions, which include suspensions, reductions in salary, demotions, and terminations.[83]

B. Vulnerabilities of the Representation

In *National Labor Relations Board v. J. Weingarten, Inc.*, the Supreme Court held that an employee had a right to union representation during an investigatory interview and could refrain from participating in the interview in the absence of such representation.[84] In the case of a workplace investigation, a public employee is entitled to invoke these "*Weingarten* rights" by having a union representative present during an interview if the employee is the subject of the investigation, or if information from that meeting could be used against the employee in a disciplinary action.[85] An employee may invoke this protection if the employee reasonably believes disciplinary action might result from the meeting.[86]

80. *See, e.g.*, DEP'T OF PERS. ADMIN., A GUIDE TO EMPLOYEE. CONDUCT AND DISCIPLINE, at 4–5 (2004), *available at* http://www.documents.dgs.ca.gov/ohr/pom/supervisorshandbook.pdf.

81. *Id.* at 5, 11.

82. *Id.* at 5, 16, 24.

83. *Id.* at 5.

84. Nat'l Labor Relations Bd. v. Weingarten, Inc., 420 U.S. 251, 259, 267 (1975).

85. *See* Robinson v. State Pers. Bd., 97 Cal. App. 3d 994, 1003 (1979) (stating that the plaintiff, a state employee, had the right to refuse a meeting with his supervisor without a union representative if the significant purpose of the meeting was to investigate facts in relation to a contemplated disciplinary action); *see also* Serv. Emps. Int'l Union, *Disputes and Grievances: Rights, Procedures and Best Practices,* SEIU.ORG, http://www.seiu.org/a/members/disputes-and-grievances-rights-procedures-and-best-practices.php (last visited Mar. 3, 2014) (holding union employees are entitled to *Weingarten* representation in circumstances where a supervisor asks for information that could be used as a basis for discipline).

86. *Weingarten, Inc.*, 420 U.S. at 267.

i. Weingarten *Rights Do Not Automatically Trigger*

An employee is not automatically entitled to *Weingarten* protections when called in for an investigatory interview with the employer. Two requirements must be met for an employee to invoke *Weingarten* rights: (1) the employee must have a belief that the interview may lead to discipline; and (2) the employee must demand a union representative.[87] This places the burden on the employee who must first either recognize the purpose of the interview[88] or make the initial inquiry as to the nature of the meeting.[89] The employee is also responsible for knowing his or her rights so that he or she can make such a request for representation.[90] This may be difficult in instances where an employee is approached by his or her supervisor who is inquiring about missing inventory or incomplete work. Not only may the employee be unaware that he or she is being questioned for misconduct until having already provided information that might later be used against the employee, but the employee may also feel pressured to comply because of the inherent supervisor-subordinate relationship. In addition, employees may fail to make the request simply because they are unaware of their right to representation. The supervisor or employee-relations designee conducting the questioning is not required to disclose that the questioning may be for disciplinary purposes, that the employee's answers may be used later against the employee in a disciplinary action, or that the employee may invoke his or her *Weingarten* rights during the interview.[91]

ii. Lax Qualification Requirements of Representatives

Another vulnerability lies in the representation afforded to the employee. Representation is not limited to union representation; it

87. AM. FED'N OF STATE, CNTY. & MUN. EMPS., STEWARD HANDBOOK 32 (Fall 2013), *available at* http://www.afscme.org/members/education-for-action/document/AFSCME-Steward-Handbook-1.pdf [hereinafter AFSCME].

88. *See* Penn-Dixie, 253 N.L.R.B. 91, 94 (1980) (holding employee who had "no inkling that he was being summoned for an interview which might result in discipline for him" and had no reason otherwise to request union representation is permitted to request union representation during the course of an investigation upon realizing he is the target of an investigation).

89. Serv. Emps. Int'l Union, *supra* note 85.

90. *Id*. Union representatives are advised to remind union members about their *Weingarten* rights by placing formalized requests on the back of their business cards, which employees may then read to their supervisor. *See also* AFSCME, *supra* note 87, at 40–41.

91. AFSCME, *supra* note 87, at 40–41.

may also include representation by a layperson such as a co-worker.[92] Furthermore, there are no specific eligibility or practical experience requirements in order to become a union representative, also known as a union steward, aside from being familiar with the union contract and work rules[93] and having certain general leadership qualities.[94] While it is preferred that applicants have knowledge of, or experience in, handling personnel issues in the civil service realm, one is not required to be an attorney or have any prior experience handling labor and employment issues.[95] It seems self-evident that it would be beneficial to have someone familiar with the workings of the public employment system present during a disciplinary investigation, even if that individual is not an attorney.

A familiarity with employment law would also help employees understand the long-term implications resulting from workplace investigations. A state employee, for example, may need to prepare for an administrative hearing before the State Personnel Board if a disciplinary action arises.[96] The employee may also face possible termination if the misconduct being investigated is severe,[97] giving way to post-employment concerns such as whether to pursue a claim

92. *See* Epilepsy Foundation of Northeast Ohio, 331 NLRB 676, 676 (2000) (extending the *Weingarten* right to have a co-worker present during investigatory interviews to the nonunionized setting); *but see* IBM Corp., 341 NLRB 1288, 1289 (2004) (expressly overruling *Epilepsy Foundation*, but preserving right of unionized employees to have a co–worker present).

93. AFSCME, *supra* note 87, at 8. *See also* Serv. Emps. Int'l Union, *Member Resources: Your Role as Steward*: *The Basics,* SEIU.ORG, http://www.seiu.org/a/members/your-role-as-a-steward-the-basics.php (last visited Mar. 3, 2014); Serv. Emps. Int'l Union, *Union Representatives/Organizers Job Description*, SEIU-UHW.ORG, http://www.seiu-uhw.org/archives/6908 (last visited Mar. 3, 2014).

94. AFSCME, *supra* note 87, at 5, 7, 9.

95. *See Your Role as Steward: The Basics*, *supra* note 93; *Union Representatives/Organizers Job Description*, *supra* note 93.

96. In California, the State Personnel Board is the administrative commission that handles disciplinary appeals for state employees. Dep't of Human Res., Cal. State Univ., Fresno, *Understanding Progressive Discipline*, at 19 (Aug. 1997), *available at* http://www.fresnostate.edu/mapp/VI/Understanding%20Discipline%20in%20one.pdf. The administrative commission that handles appeals varies depending on the state and jurisdiction, i.e., whether the employee is a city or state employee. For example, in New York, the Civil Service Commission handles appeals by city employees. N.Y. Civ. Serv. Comm'n, § 76 *Disciplinary Appeals*, http://www.nyc.gov/html/csc/html/appeals/ s76disciplinary.shtml (last visited Mar. 19, 2014). In Texas, a delegated representative in the employee's department handles such appeals for state employees. Univ. of Tex., *Rule 30601: Discipline and Dismissal of Classified Employees*, http://www.utsystem.edu/ board-of-regents/rules-regulations/rules/30601-discipline-and-dismissal-classified-employees (last visited Mar. 19, 2014).

97. DEP'T OF PERS. ADMIN., *supra* note 80, at 5.

for unemployment benefits or a wrongful termination suit.[98] Someone with practical experience in labor and employment law or with civil service personnel would be better equipped to anticipate these issues and advise the employee. In addition, having someone who is familiar with the legal implications of workplace investigations would provide continuity in representation from the initial investigatory interview to subsequent legal proceedings that may arise.

The Fourth Amendment is implicated when a public employer acts in an official capacity on behalf of the governmental organization and searches an employee-owned BYOD, which the employee has a reasonable expectation of privacy to. Thus, an employee may need to file a separate action regarding the violation of his or her Fourth Amendment rights. In this situation, having an attorney as a representative may be particularly helpful.

C. The Threat of Administrative Disciplinary Action Weakens the Protection of Public Employees' Privacy Rights

The issue of employee privacy in BYODs in the workplace implicates not only the Fourth Amendment, but it has Fifth Amendment ramifications as well. One vulnerability of an employee's privacy interest lies in the fact that employees have limited protection against self–incrimination in workplace investigations. The Fifth Amendment guards public employees from self-incrimination by providing that "[n]o person shall . . . be compelled in any criminal case to be a witness against himself."[99] However, this protection does not necessarily extend to administrative proceedings.[100] While a public employee has the right to remain silent and avoid self-incrimination if it appears that the employee could be charged with a criminal offense as a result of the employee's workplace misconduct,[101] the employee is not immune from discipline at work for failing to cooperate in a workplace investigation.[102]

98. U.S. Dep't of Labor, *Termination*, http://www.dol.gov/dol/topic/termination/ (last visited Mar. 19, 2014).

99. U.S. CONST. amend. V.

100. Spielbauer v. Cnty. of Santa Clara, 199 P.3d 1125, 1140–41 (2009); *see also* Lybarger v. City of Los Angeles, 710 P.2d 329, 334 (1985).

101. *Lybarger*, 710 P.2d at 334.

102. *Spielbauer*, 199 P.3d at 1140–41.

A public employer is prohibited from disciplining an employee solely because the employee invoked his or her right against self-incrimination under the Fifth Amendment,[103] but this does not mean the employee is in the clear. Even if the right is invoked an employer can still discipline the employee for his or her invocation.[104] In the course of an administrative investigation into an employee's work performance and conduct, a public employer may compel an employee to answer questions without any grant of testimonial immunity.[105] If an employee refuses to answer questions and invokes the Fifth Amendment's right against self-incrimination, the employer may deem that silence as insubordination and use it against the employee in a subsequent administrative proceeding or disciplinary action.[106] So while the Fifth Amendment protects the employee from self-incrimination in the criminal context, it does not protect an employee from being deemed insubordinate. If an employee refuses to incriminate herself, such refusal could result in disciplinary action; however, if the employee answers the employer's questions, she risks providing the employer with evidence that could be used against her in either a criminal or administrative action. Thus, a public employee's right to remain silent is largely illusory during a disciplinary investigation.

D. Relaxed Evidentiary Rules for Administrative Disciplinary Proceedings

Public employees who are ultimately disciplined are entitled to an appeal.[107] Unlike the evidentiary rules that govern proceedings in a court of law, however, the evidentiary rules governing disciplinary appeals permit admission of evidence obtained from an investigation or investigatory search.[108] For example, employees of the State of

103. Garrity v. New Jersey, 385 U.S. 493, 499–500 (1967).

104. *Spielbauer*, 199 P.3d at 1140–41.

105. *Id.*; *see also Garrity*, 385 U.S. at 499–500.

106. *Spielbauer*, 199 P.3d at 1140–41; *see also* James Baca, et al., *Public Employers' Right to Compel Answers in Employee Investigations Upheld by California Supreme Court* (Feb. 2009), *available at* http://www.aalrr.com/files/Alert_-_Public_Employers_Right_to_Compel_Answers-_February_2009(2).pdf.

107. *See* Cal. State Pers. Bd., Appeals Resource Guide, at 2 (2013), *available at* http://spb.ca.gov/content/appeals/Appeals_Resource_Guide.pdf.

108. *See* Cal. State Pers. Bd., 2 Evidentiary Hearing Process: SPB Statutes and Regulations § 59.1(c)(5) (Supp. 2013), *available at* http://spb.ca.gov/content/appeals/SPB_Hearing_Manual.pdf.

California who incur a disciplinary action may seek a hearing before the State Personnel Board to contest the action.[109] During these administrative hearings, the burden of proof rests on the public employer,[110] but that burden may be met with evidence, such as hearsay, which is generally inadmissible in a court of law.[111] The hearing officer is "not bound by common law/statutory rules of evidence or by technical or formal rules of procedure . . . but shall conduct the investigatory hearing in such a manner as necessary to reach a just and proper decision."[112] In California, the hearing officer has wide latitude to conduct the hearing. Any relevant evidence is admitted if it is evidence which "responsible persons are accustomed to relying on in the conduct of serious affairs."[113] This means that information obtained during the course of an investigation may be admitted so long as the evidence itself is reliable, even if it intrudes on an employee's privacy. Here, the employee could file a separate suit regarding the intrusion into his or her privacy, but that suit might not be resolved until after the administrative hearing is complete and the employee has been harmed by the results of the adversary action.

III. Application of the Reasonableness Standard Will Not Adequately Protect Employees During an Investigatory Search of a BYOD

The United States Supreme Court has held that the Fourth Amendment does not prohibit employers from conducting work-related searches, so long as those searches are reasonable.[114] While the Court has been careful to note the existence of two types of searches—non-investigatory, work-related searches and investigatory searches for evidence of an employee's work-related misfeasance—it essentially eviscerates any distinction by applying the same reasonableness standard to both situations when the potential of harm to the employee is significantly unequal.[115] Although a

109. *See* Dep't of Human Res., *supra* note 96, at 18–19. *See also* Cal. State Pers. Bd., *Appeals Division Appeal Hearing Procedures*, http://spb.ca.gov/appeals/faq.cfm (last visited Mar. 3, 2014).

110. CAL. STATE PERS. BD., EVIDENTIARY HEARING PROCESS, *supra* note 108.

111. Dep't of Human Res., *supra* note 96, at 19.

112. CAL. STATE PERS. BD., APPEALS RESOURCE GUIDE, *supra* note 107, at § 55.2(d).

113. *Id.*

114. O'Connor v. Ortega, 480 U.S. 709, 717 (1987) (plurality opinion).

115. *See supra* note 58 and accompanying text.

reasonableness standard may be appropriate when the workplace search is conducted for work-related, non-investigatory purposes, it is dangerous to apply this standard to searches conducted for investigatory purposes. This is especially true when the search involves an employee's personal property, such as an electronic personal BYOD.

The Court adheres to the reasonableness standard because it has concluded that the interests of public employers outweigh the privacy interests of employees.[116] This concern for the public employer's work mission may be justified during an inventory search of an employee's personal device. In such a search, the employer's primary interest should be ensuring that the agency is executing its duties, given that the public relies on government agencies to function properly and efficiently.[117] This motive changes, however, when the search is performed with an investigatory purpose, as recognized in Justice Blackmun's dissent in *O'Connor*.[118] Ultimately, the purpose of the search affects how the public employer's and employee's interests are weighed against each other.

A. The Solution: Adhering to the Warrant Requirement in Investigatory Searches

Courts should adopt a different standard for investigatory searches of BYODs that recognizes the distinction between the two kinds of searches. If the search is primarily for an investigatory purpose, a higher burden, in the form of a warrant and probable cause requirement, as Justice Blackmun advocated for in his dissent, should be imposed on employers.[119] Searches of BYODs pose a greater potential for intrusion into an employee's privacy.[120] Existing investigatory processes further jeopardize employee privacy, since they give employers great latitude in gathering evidence.[121] Collectively, these factors present a compelling employee interest, which outweighs the governmental interest in gathering evidence of

116. *O'Connor*, 480 U.S. at 720.

117. *Id.*

118. *See supra* Part I.B.i.b.

119. *O'Connor*, 480 U.S. at 745 & n.10.

120. See Fact Sheet 40: Bring Your Device . . . at Your Own Risk, PRIVACY RIGHTS CLEARINGHOUSE, https://www.privacyrights.org/bring-your-own-device-risks (last visited Mar. 19, 2014).

121. *See supra* Part II.D.

wrongdoing. In addition, searches of BOYDs do not present a special needs exception on which to justify a search based on less than probable cause.

i. The Special Needs Exception Does Not Apply to BYODs in an Investigatory Search

In some circumstances, searches based on less than probable cause may be constitutional where there is a special need.[122] The plurality in *O'Connor* based its decision on this special needs rationale.[123] However, such exceptions have been narrowly limited to apply only when there is a danger to the public or to someone's life.[124] In the context of BYODs, it is unlikely that such special need circumstances would ever arise. BYODs are electronic portable devices, and as such, can only produce certain limited types of evidence. Specifically, a search of a BYOD can only yield intangible or electronic information,[125] such as electronic documents, digital photos, and information about the device user's network access and internet usage. A search of a BYOD is unlikely to uncover actual weapons[126] or illegal substances.[127] Since a search of a BYOD would probably not uncover such items or anything else posing an immediate threat to public safety, an exception to the probable cause requirement is unjustified for searches of BYODs.

The Court has also noted that the reasonableness of a search depends on the context of the search.[128] Though courts have upheld searches based on less than probable cause in schools,[129] the

122. *See, e.g.*, Terry v. Ohio, 392 U.S. 1, 28 (1968) (permitting limited "stop and frisk" searches based on less than probable cause when reasonably necessary for officer to safeguard against concealed weapons); New Jersey v. T.L.O., 469 U.S. 325, 342 (1985) (permitting school officials to conduct searches of students upon reasonable suspicion); Griffin v. Wisconsin, 483 U.S. 868, 872 (1987) (permitting searches of probationer's home upon reasonable suspicion).

123. *O'Connor*, 480 U.S. at 720.

124. *See, e.g.*, *Terry*, 392 U.S. at 28 (permitting police officer to conduct limited search of suspect he reasonably believed that suspect would be armed); Skinner v. Ry. Labor Execs. Ass'n, 489 U.S. 602, 633 (1989).

125. Randolph S. Sergent, Note, *A Fourth Amendment Model for Computer Networks and Data Privacy*, 81 VA. L. REV. 1181, 1195–96 (1995) (recognizing that the Fourth Amendment has been applied where intangible information is the subject of the search).

126. *Terry*, 392 U.S. at 28.

127. *T.L.O.*, 469 U.S. at 342.

128. *O'Connor*, 480 U.S. at 719.

129. *See, e.g., T.L.O.*, 469 U.S. at 339–40 (noting school officials require flexibility to supervise students and maintain security and order to curb disciplinary problems and

workplace is different. Unlike a school, where attendance is typically compulsory, in most cases, employers do not owe an equal duty of care to supervise and educate their employees. The government's interest is therefore limited because employers and employees are on more equal footing. They do not owe each other any constitutionally significant duties to justify unwarranted searches.

It remains unclear whether a warrant based on probable cause is required for searches that are primarily investigatory in nature because the reasonableness standard has not been tested on an investigatory search. *O'Connor* and *Quon* involved inventory searches of employer-owned property,[130] and in *Quon* the Court found the search to be reasonable.[131] The Court has not yet had the opportunity to apply the reasonableness standard to an investigatory search of a BYOD because BYOD workplace policies are relatively new.

In the absence of any special need and in light of the investigatory nature of the search, an employer's justification for a warrantless investigatory search of an employee's personal BYOD is weak. The substantial privacy interest that an employee has in his or her BYOD further reduces this justification.

Until Congress develops laws that specifically address BYODs, public employers, such as government agencies, will be in the best position to implement clear policies regarding BYODs. Government agencies should proactively develop their own BYOD policies because individual agencies may use BYODs differently or have varying concerns regarding their use in the workplace.[132] Agencies can easily incorporate BYOD policies into their existing electronic communications or network user agreements.[133] By implementing

preserve a proper educational environment); In re William G., 709 P.2d 1287, 1294 (1985) (noting "the unique characteristics of the school setting require that the applicable standard be reasonable suspicion"); Marner ex rel. Marner v. Eufala City Sch. Bd., 204 F. Supp. 2d 1318, 1325 (1993) (noting search by school officials is justified if there are "reasonable grounds for suspecting that the search will turn up evidence that the student has violated or is violating either the law or the rules of the school").

130. *O'Connor*, 480 U.S. at 728; City of Ontario v. Quon, 130 S. Ct. 2619, 2632 (2010).

131. *Quon*, 130 S. Ct. at 2630.

132. Adam Santucci, BYOD Lessons From Jersey's Bridge Scandal, PENNSYLVANIA LABOR & EMPLOYMENT BLOG (posted Jan. 21, 2014), http://www.palaborandemploymentblog.com/2014/01/articles/workplace-trends/byod-lessons-from-jerseys-bridge-scandal/.

133. Tracy L. Glanton, *When was the Last Time You Updated Your BYOD Policy?*, ELARBEE THOMPSON (Oct. 29, 2013), http://www.elarbeethompson.com/media/elerts/when-was-last-time-you-updated-your-byod-policy.

their own departmental policies, agencies will protect themselves and provide notice to their employees about privacy considerations.[134] In addition to implementing such policies, government agencies may also control BYODs by providing employer-owned devices in lieu of BYODs used by employees. No matter what specific steps government agencies take regarding BYODs, they are in the best position to protect themselves and their employees through proactive policy development and implementation.

ii. Employees Have a Strong Property Interest in Their BYODs and Employment

An investigatory search of an employee's personal device highlights two compelling employee property interests: (1) the property interest in the BYOD itself; and (2) the property interest in the employee's employment.[135] Under a Fourth Amendment analysis, employees should be given greater consideration when their BYODs are searched in the workplace, given that these two property interests are at stake.

Employees have a heightened privacy interest in BYODs because these devices are used for work and non-work related purposes.[136] A BYOD may contain personal data, ranging from vacation photos to a favorite "90s hits" music file to financial documents, all of which an employee may not wish to share with his employer. Unlike BYODs, employees have a limited reasonable expectation of privacy[137] in employer-owned devices because they are not intended for either personal use or the storage of personal data, and they may be further restricted by departmental policies reserving an employer's right to conduct a reasonable search of employer-owned devices.[138] Furthermore, the "workplace" has been defined as "those areas and items that are related to work and are generally within the employer's control."[139] A BYOD does not fall within this definition because it is generally under the employee's sole control and ownership. Therefore, the possibility of intrusion into an

134. Santucci, *supra* note 132.

135. Bd. of Regents v. Roth, 408 U.S. 564, 577–78 (1972) (recognizing that the Fourteenth Amendment's due process requirements apply when one has a valid property interest in continued public employment).

136. *See supra* note 16.

137. City of Ontario v. Quon, 130 S. Ct. 2619, 2631 (2010).

138. *Id*.

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

employee's privacy increases significantly if an employer conducts a warrantless search of a BYOD.

Aside from owning a BYOD, an employee also has a property interest in his employment.[140] This second property interest entitles an employee to due process before the government can deprive the employee of that interest.[141] The administrative procedures for investigatory processes that exist, however, function in a way that make the employee vulnerable to disclosure of private information.[142] An employer may require an employee to disclose private information by threatening the employee with disciplinary action.[143]

Requiring employers to obtain a warrant and establish probable cause that the employee is engaging in illegal conduct or work-related misfeasance before conducting an investigatory search of an employee's BYOD would help protect employees' privacy rights. A warrant requirement would deter employers from using inventory searches as "fishing expeditions," and it would ensure that employers take reasonable steps to obtain evidence and corroborating information through alternative means before conducting a search of an employee's BYOD. Requiring that a neutral magistrate review an employer's assertion of probable cause would also safeguard employees' privacy interests. Neutral magistrates, and the warrant process, can prevent unjustified intrusions on employee privacy, which is more meaningful protection than the remedial measure of seeking a Fourth Amendment violation claim after an employee's privacy interests have already been infringed. Requiring a warrant and probable cause would not significantly interfere with an employer's ability to conduct an investigation, because the employer would still be able to interview witnesses and gather evidence through other means.[144] In such circumstances, the employee could even consent to a search of his BYOD, eliminating any need to obtain a warrant.

Applying the reasonableness standard to all searches—whether the search is for inventory or for investigatory purposes—does not adequately protect the privacy interests of employees. The compelling private interests at stake outweigh the less compelling

140. *Roth*, 408 U.S. at 577–78.

141. *Id.*

142. *See supra* Part II.

143. *See supra* notes 98–106 and accompanying text.

144. *See, e.g.,* Dep't of Human Res., *supra* note 96, at 17.

governmental interests demonstrating the necessity of adopting the traditional warrant requirement in investigatory searches of employees' BYODs.

Conclusion

As technology continues to advance, and new technology permeates the workplace in the form of BYODs, it is imperative that the law must also evolve; such evolution is necessary to protect employee privacy interests. However, twenty-five years after its adoption in *O'Connor*, the test for assessing the reasonableness of employer-conducted searches remains unchanged.[145] Though the Court's jurisprudence in this area is clear regarding the reasonableness of inventory searches, the application of this standard to investigatory searches remains unresolved. Furthermore, neither *O'Connor* nor *Quon* addressed the application of such a standard to employee-owned personal devices or BYODs, as used in the workplace.

In order to adequately protect employee expectations of privacy in the workplace, where existing employer policies fail to outline clear expectations, the courts should adopt a new test for BYODs. Courts should take into account the nature of a search in determining which standard to apply. Inventory searches may be best handled with the existing standard, but investigatory searches should be subject to the traditional warrant requirement and probable cause standard.

The existing reasonableness standard would inadequately protect employee privacy expectations in an investigatory search of his or her BYOD because BYODs present heightened privacy interests. A search of an employee's BYOD creates greater potential for an intrusion on an employee's privacy, because the device's dual use means it is more likely to contain personal information than an employer-owned device used by an employee for only work-related purposes. Furthermore, an investigatory search may impact an employee's employment by triggering administrative processes that may result in disciplinary action. These existing processes grant public employers wide latitude in questioning employees and gathering evidence that may be used against an employee in a disciplinary action, thereby providing limited protection to employees in safeguarding their privacy.

145. O'Connor v. Ortega, 480 U.S. 709, 713–14 (1987); City of Ontario v. Quon, 130 S. Ct. 2619, 2625 (2010).

Though employers may have a legitimate interest in ensuring the efficient operations of the workplace, this alone is not enough to justify an exception to the probable cause standard in the context of an investigatory search. Because BYODs only disclose a limited type of information and the employer is still free to explore other investigatory tactics, a warrant requirement would impose a minor burden on the employer. Thus, the significant harm to the employee outweighs the minimal harm to the employer in imposing a warrant requirement. As people begin to rely more and more on their BYODs and these devices become extensions of ourselves, it is necessary to safeguard public employees' privacy rights in their BYODs as they navigate the uncharted waters of this new technological workplace transformation.

* * *