# Somebody's Watching Me: Workplace Privacy Interests, Technology Surveillance, and the Ninth Circuit's Misapplication of the *Ortega* Test in *Quon v. Arch Wireless*

*Justin Conforti*[†]



[†] J.D. Candidate, 2010, Seton Hall University School of Law; B.A., Boston University, 2005. I would like to thank Professor Timothy Glynn for his insight, my fellow *Circuit Review* members for their diligent revisions, and my friends and family for their support.

## I. INTRODUCTION

*"The makers of our Constitution . . . sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men."*[1]

Most employees would probably jump at the chance for their employers to provide and pay for a BlackBerry.[2] The pocket-sized powerhouse keeps go-getters connected to work e-mails and the latest news via the Internet, and the deal seems even sweeter when the boss foots the bill. However, the circumstances surrounding this innocent little device are more insidious than employees may realize. While providing the opportunity to sneak out of work early and answer e-mails from the golf course, a piece of technology like the BlackBerry has further blurred already fuzzy lines separating the workplace from an individual's personal world outside the office. Despite the ostensible benefits of employer-provided technology, such as laptops, cell phones and BlackBerries, this blurring has serious implications for employee expectations regarding privacy in communications sent on employer-provided technology.

A 2001 American Management Association study shed some light on the stark reality that employers monitor workplace technology without employee awareness.[3] The study revealed that nearly 80 percent of surveyed large employers, who retain as much as a quarter of American workers, listened to employee phone conversations and voicemails, and read electronic files and e-mails.[4] Additionally, as of 2001, roughly 40 million American employees regularly use e-mail or access the Internet at work[5] and, as of 2004, 20.7 million American

---

[1] Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

[2] The BlackBerry is a wireless handheld device introduced in 1999 as a two-way pager. In 2002, the more commonly known smartphone BlackBerry was released, which supports push e-mail, mobile telephone, text messaging, internet, faxing, web browsing and other wireless information services as well as a multi-touch interface. *See generally* Jennifer Lane, Note, NTP, Inc. v. Research in Motion, Ltd.*: Inventions Are Global, But Politics Are Still Local-An Examination of the BlackBerry Case*, 21 BERKELEY TECH. L.J. 59 (2006).

[3] AMA, Survey: Workplace Monitoring & Surveillance, Summary of Key Findings 1 (2001).

[4] *Id*.

[5] Schulman, Andrew, *The Extent of Systematic Monitory of Employee E-mail and Internet Use*, Privacy Foundation July 9, 2001, *available at* http://diogenesllc.com/internetmonitoring.pdf.

employees "telecommute" from home.[6] When considered alongside a 1999 study showing that one in three workers surf the Internet for personal reasons during work hours,[7] these statistics suggest that perhaps employees do not realize their communications on employer-provided laptops, cell phones and BlackBerries may be monitored for their content.[8]

Indeed, these statistics indicate that employees may presume the Brandeis model of personal autonomy—the "right to be let alone"—extends to all aspects of their lives, including communications sent on employer-provided technology.[9] While employees may have an interest in maintaining some privacy at work, employers have conflicting interests in monitoring technology use to learn more about how employees utilize company time.[10] Employers need to learn about the character and personality of the employee they hire in addressing potential and ongoing performance issues and ensuring the physical security of their workplace.[11] Thus, employers may view electronic monitoring and other surveillance as necessary to ensure productivity, stop leaks of confidential information, and prevent workplace harassment.[12] Moreover, employers must worry about the ever-present

---

[6] Economic News Release: Work at Home in 2004, *available at* http://www.bls.gov/news.release/homey.nr0.htm. "Telecommuting" refers to when an "employee . . . works at home using telecommunications devices to provide a service." Katherine V.W. Stone, *Legal Protection for Workers in Atypical Employment Relationships in the United States*, 27 BERKELEY J. EMP. & LAB. L. 251, 270 (2006).

[7] Matthew W. Finkin, *Information Technology and Workers' Privacy: The United States Law*, 23 COMP. LAB. L. & POL'Y J. 471, 474 (2002).

[8] Matthew W. Finkin, *Information Technology and Workers' Privacy: The United States Law*, 23 COMP. LAB. L. & POL'Y J. 471, 474 (2002).

[9] Olmstead, 277 U.S. at 478 (Brandeis, J., dissenting). *See* RICHARD T. DE GEORGE, THE ETHICS OF INFORMATION TECHNOLOGY AND BUSINESS 102 (Blackwell Publishing, 2003).

[10] *See* Rachel Sweeney Green, Comment, *Privacy in the Government Workplace: Employees' Fourth Amendment and Statutory Rights to Privacy*, 35 CUMB. L. REV. 639 (2005).

[11] *See generally* Nicole Nyman, *What Must Employers Do To Shield Against Liability For Employee Wrongdoings In the Internet Age?*, 1 SHIDLER J. L. COM & TECH. 7 (2005).

[12] *See* TBG Ins. Services Corp. v. Superior Court, 96 Cal. App. 4th 443, 451 (Cal. Ct. App. 2002). These valid employer motives for surveillance comprise what a California Court of Appeals referred to as the "community norms" of the American business world, comprising an employer's responsibility regarding legal compliance in regulated industries, legal liability, performance review, productivity measures, and security concerns. *See also* Smythe v. Pillsbury Co., 914 F. Supp. 97 (E.D. Pa. 1996); Jarrod J. White, Comment, *E-Mail@Work.Com: Employer Monitoring of Employee E-Mail*, 48 ALA. L. REV. 1079, 1080 (1997).

specter of litigation that hangs over the modern workplace.[13] However invasive monitoring may seem, employers have legitimate motives to monitor employee conduct in the workplace.[14]

If employers monitor communications on workplace technology and employees inadvertently divulge personal information, employees will often struggle to find any legal protection, as the American legal regime does not provide any generally applicable, affirmative protection for employee privacy.[15] The Fourth Amendment to the United States Constitution does provide government employees some protection in the workplace,[16] based on the framework set forth by the Supreme Court in *O'Connor v. Ortega*.[17] However, the protections afforded to government employees by this framework are both limited and uncertain, in part due to the fact that the inquiry under the test for whether privacy exists is highly contextual. The test for whether a public-sector employee has a workplace privacy right hinges on whether he enjoyed "reasonable expectations" of privacy based on the circumstances of his workplace.[18] Upon finding such an expectation, a court will then examine whether an employer's search infringed upon that expectation, which depends on whether the search was reasonable in its inception and scope.[19] As this Comment will address, the Court's contextual methodology has allowed employers to alter workplace contexts with privacy policies that extinguish any employee privacy expectations in communications sent on workplace technology. Crucially, these doctrinal requirements for analyzing whether an employee has a privacy expectation in his workplace make the Fourth Amendment a poor fit for providing much

---

[13] *See, e.g.*, Erin M. Davis, Comment, *The Doctrine of Respondeat Superior: An Application to Employers' Liability for the Computer or Internet Crimes Committed By Their Employees*, 12 ALB. L.J. SCI. & TECH., 683, 689 (2002) (examining how the doctrine of respondeat superior, which generally holds employers liable for the acts of their employees, complicates the legal responsibilities an employer must consider when providing technology to employees).

[14] DE GEORGE, *supra* note 9, at 104.

[15] *See generally* TIMOTHY P. GLYNN, RACHEL S. ARNOW-RICHMAN & CHARLES A. SULLIVAN, EMPLOYMENT LAW: PRIVATE ORDERING AND ITS LIMITATIONS 273–342 (2007). *See also* Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477 (2006).

[16] U.S. CONST. amend. IV ("The 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, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.").

[17] O'Connor v. Ortega, 480 U.S. 709 (1987).

[18] *Id*. at 714.

[19] *Id*. at 724.

protection on technology such as computers, cell phones, and BlackBerries.[20]

Moreover, because the Fourth Amendment only applies when the government acts, private-sector employees have no statutory federal protection.[21] While the Electronic Communications Privacy Act of 1986 ("EPPA") protects against various kinds of electronic surveillance and interception of communications by public and private actors, including private-sector employers, this regime presents several potentially insurmountable hurdles for any employee who alleges his employer intercepted private communications on workplace technology.[22] It does not provide meaningful protection for most employees because the law does not protect against interceptions by a service provider, who often doubles as the employer; the protections do not apply to interception by certain devices of communications made in the "ordinary course of business," and the protections do not apply when one party to the communications consents to the interception.[23]

Potential state-based protections are also limited. A few state constitutions, including California's, provide potentially robust privacy rights for private-sector employees.[24] Moreover, some states recognize common-law causes of action and have adopted statutory regimes that might protect employee privacy interests in some communications.[25] Yet such protections are frequently limited and unavailable.

Both the concern and conflict about communication privacy in the modern workplace are on dramatic display in *Quon v. Arch Wireless*, a controversial case decided by a three-judge Ninth Circuit panel in June

---

[20] *See generally* Symposium, Orin Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1209 (2004).

[21] *See* United States v. Jacobsen, 466 U.S. 109, 113 (1984) ("This Court has . . . consistently construed [the Fourth Amendment] as proscribing only governmental action; it is wholly inapplicable 'to a search or seizure, even an unreasonable one, effected by a private individual not acting as an agent of the Government or with the participation or knowledge of any governmental official.") (internal citation omitted).

[22] 18 U.S.C. § 2510-2522 (2006).

[23] GLYNN, *supra* note 15, AT 294.

[24] CA. CONST. art. I, § 1 ("All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending . . . privacy."). *See also* Hill v. NCAA, 865 P.2d 633 (Ca. 1994) (applying California Constitution to private employee's claim of privacy invasion).

[25] *See* Luedtke v. Nabors Alaska Drilling, Inc., 768 P.2d 1123 (Alaska 1989) (stating that public policy under the state constitution protects an employee's right to withhold private information from his employer and recognizing a cause of action for violations of that policy); Borse v. Piece Goods Shop, Inc., 963 F.2d 611 (3d Cir. 1992) (recognizing a cause of action for tortious "intrusion upon seclusion" in the workplace)

2008.[26] In *Quon*, a public-sector employee, Jeff Quon, filed suit against his employer, alleging that his employer violated his rights under the Fourth Amendment and the California Constitution by reading his personal text messages sent on his employer-provided pager.[27] In applying the *Ortega* test, the Ninth Circuit held that Quon had a reasonable privacy expectation in his pager messages.[28] The court found that his expectation of privacy in the messages was reasonable even though the employer provided the pager and had a formal anti-privacy policy warning employees about the possibility of surveillance and prohibiting the use of employer-provided technology for personal communications.[29] In spite of these warnings, the court found the expectation was reasonable because the employer had an informal practice of assuring Quon that he could maintain privacy in the messages if he personally paid all monthly overage fees on the pager.[30]

Having located a privacy right based on Quon's reasonable expectations, the court also held that the employer's review of the content of these messages was unreasonable in scope based on its failure to use less intrusive means in investigating whether the messages were work-related in nature.[31] The *Quon* court's treatment of this issue represents a split from several circuits and, as this Comment will conclude, a departure from Supreme Court precedent.

In January 2009, the employer petitioned the Ninth Circuit to rehear *Quon* en banc, which was denied by a majority of the Ninth Circuit judges. The denial of the rehearing, though, inspired an impassioned dissent, joined by seven judges and authored by Judge Ikuta, who

---

[26] Quon v. Arch Wireless Operating Co., Inc., 529 F.3d 892 (9th Cir. 2008).

[27] *Id*. Quon not only sued his employer under federal and state constitutions but also filed suit against Arch Wireless, the third-party service provider that released the content of the text messages to the city, claiming Arch violated the Stored Communications Act ("SCA"), codified as 18 U.S.C. § 2701 and part of the EPPA. 18 U.S.C. § 2701-2711. While this Comment focuses on the interplay between employer and employee interests regarding workplace technology, and therefore does not confront the Ninth Circuit's controversial SCA interpretation, it is worth noting how the SCA presents an equally important potential source of protection for private- and public-sector employees. The SCA expands the scope of liability to those outside the direct employment relationship and, as constitutional protections are often unavailable for private-sector employees, a statute such as the SCA becomes a critically important form of protection, despite its inherent limitations. *See generally* Kerr, *supra* note 20. It is also worth nothing that the Ninth Circuit has already been openly criticized for its reading and application of the SCA by a Michigan district court. *See* Flagg v. City of Detroit, 252 F.R.D. 346 (E.D. Mich. 2008).

[28] *Quon*, 529 F.3d at 908.

[29] *Id*. at 907.

[30] *Id*. at 908.

[31] *Id*. at 909.

directly criticized the panel's use of the "less intrusive means" standard that created the circuit split.[32]

In some regards, *Quon* represents valuable insight into the current state of workplace privacy jurisprudence and could signal the potential expansion of employee privacy. Its application also may be more expansive than it first appears, beyond its impact on public-sector employees in the Ninth Circuit. In addition to his Fourth Amendment claim, Quon filed suit that his employer violated his privacy under the California Constitution.[33] Because the court held that its application of *Ortega* governed its decision of Quon's federal *and* state constitutional claims, and because the California Constitution applies to private-sector employees, the panel's expansive inquiry into the reasonableness of the public-sector employer's search could have an impact on the privacy rights of *private*-sector employees in California, who, as of 2005, comprise 11.6% of the nation's total private-sector employment.[34]

Part II of this Comment sets forth the dramatic facts leading up to the *Quon* case, which stand as a prime example of the tension at play in the modern workplace between employer and employee interests regarding employer-provided communication devices. Part III discusses the framework set forth by the Supreme Court in *Ortega* for investigating claims of workplace privacy intrusion and continues with an exploration of how the two prongs of the *Ortega* test have generally been applied in the circuits. Part IV closely examines how the Ninth Circuit applied the *Ortega* test in *Quon*, as well as the potential ramifications of the panel's disregard of Supreme Court precedent and the court's split from several sister circuits in its analysis under the second *Ortega* prong. Finally, this comment concludes, in Part V, with a consideration of alternative means to address the privacy concerns inherent in the modern workplace and a proposal for potential legislative action to combat dwindling workplace privacy.

## II. TENSIONS BETWEEN EMPLOYER AND EMPLOYEE INTERESTS ON DISPLAY IN *QUON*

Before the Ninth Circuit could investigate the legal parameters of Quon's Fourth Amendment and state constitution claims, the trial court

---

[32] Quon v. Arch Wireless Operating Co., Inc., 554 F.3d 769, 774 (9th Cir. 2009) (Ikuta, J., dissenting from the denial to rehear en banc).

[33] CA. CONST. art. I, § 1. ("All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending . . . privacy.").

[34] Batelle Tech. P'ship Practice & SSTI, Laboratories of Innovation: State Bioscience Initiatives 2004, at 5, *available at* http://www.bio.org/local/battelle 2004/battelle2004.pdf (last updated July 15, 2005).

had to confront the sordid workplace that gave rise to the dispute.[35] Like many other workplaces, the Ontario Police Department ("OPD") had its fair share of melodrama. While all the facts in the background of Quon's workplace do not bear on the crucial doctrinal aspects of the Ninth Circuit's decision, the gritty realities of the OPD demonstrates the tensions at play between employer and employee interests in workplace technology.[36]

Prior to the audit of Quon's text messages at issue in the litigation, the OPD had to address a legitimate concern: its employees had used city-provided pagers to undermine a narcotics investigation.[37] In September 2002, one of the city's dispatchers, Sally Bors, realized her boyfriend, a member of the Hells Angels motorcycle gang, was under investigation by the police department.[38] Bors decided to warn her boyfriend, Mark Timbrell, that he was being followed, but she did not want to do the dirty work herself.[39] Accordingly, she paged her friend and fellow dispatcher Angela Santos, telling her to warn him.[40] Santos used her employer-provided pager to warn Timbrell and then quickly confessed her malfeasance to yet another dispatcher, April Florio.[41] Gossip apparently traveled like wildfire in the OPD, and Florio told Doreen Klein, another dispatcher, about the wrongdoing.[42] None of the aforesaid participants in the incident told their supervisors about what occurred.[43] The next day, somehow aware of what had transpired, internal affairs Sergeant Deborah Glenn spoke with Florio and Klein, first asking them to hand over their pagers so as to prevent them from corroborating their stories.[44] Both Florio and Klein feigned ignorance but Santos, when interviewed, confessed about the tip-off.[45]

When the dispatchers compromised the Hells Angels investigation by tipping off Bors' boyfriend, they acted in a manner that jeopardized the city's interests in covertly and efficiently battling crime.[46] The dispatchers' tip-off to the Hells Angels exemplifies employee misuse of workplace technology and demonstrates the motivations behind employer decisions to monitor employee actions, especially when public

---

[35] Quon v. Arch Wireless Operating Co., 445 F. Supp. 2d 1116 (C.D. Cal. 2006).
[36] *Id*. at 1149.
[37] *Id*. at 1121.
[38] *Id.*
[39] *Id.*
[40] *Quon*, 445 F. Supp. 2d. at 1149.
[41] *Id.* at 1122.
[42] *Id*.
[43] *Id.*
[44] *Id.*
[45] *Quon*, 445 F. Supp. 2d. at 1122.
[46] *Id*. at 1121.

safety may be negatively affected as a result of public-sector employees' misconduct.[47]

Around the same time, Jeff Quon was about to confront his own investigation.[48] Quon, like Florio, Bors and Santos, used a city-provided pager.[49] In October 2001, the OPD purchased pagers for its SWAT team members in order to facilitate their coordination with one another and increase their response time in emergency situations.[50] The city contracted with Arch Wireless for a usage plan in which the city paid a flat subscription rate for 25,000 characters per month per pager, with the city paying any overage fees incurred by the officers on a per-character basis.[51] Upon receiving the pagers, the SWAT team members, including Quon, were told orally that the pagers were subject to monitoring pursuant to the city's general anti-privacy policy.[52] When hiring, the OPD requires that all employees read and sign its formal general Computer Usage, Internet and E-mail Policy, which informs them that all network activity, including e-mail and Internet use, may be monitored, with or without notice, and that the city considered as its property all hard copy or electronic employee communications.[53] Furthermore, the city policy prohibited employee use of city property, including pagers and cell phones, for personal or confidential communication.[54] Under this policy, the city contended at trial that it considered pager messages sent by police officers as "e-mail," therefore subjecting any messages sent on city-provided alphanumeric pagers to potential auditing.[55]

Over the next few months, Police Chief Lloyd Scharf was concerned that "someone was wasting a lot of City time conversing with someone about non-related work issues" on the pagers, and asked Lieutenant Steven Duke ("Duke"), who managed the city's electronic equipment, to identify those responsible for the monthly character overages.[56] Upon realizing that officers were repeatedly sending pager messages in excess of the monthly limit, the OPD warned Quon, who was the main offender of exceeding the monthly character limit, not to exceed his monthly limit.[57] At the same time, Duke assured Quon that

---

[47] *Id.* at 1124.
[48] *Id.*
[49] *Id.*
[50] *Quon*, 445 F. Supp. 2d. at 1123.
[51] *Id*.
[52] *Id.*
[53] *Id.* at 1123.
[54] *Id.*
[55] *Quon*, 529 F.3d. at 897.
[56] *Id*. at 1126.
[57] *Quon*, 445 F. Supp. 2d. at 1124.

the city would not conduct an audit of his messages as long as he paid for the overage amount whenever he exceeded it.[58] While allowing Quon to pay for his overages, Duke claims he also reiterated several times that messages sent from and received on the pagers were subject to the city's usage policy and could be audited.[59] In April 2002, Quon received a memorandum from Scharf stating: "Reminder that two-way pagers are considered e-mail messages. This means that messages would fall under the City's policy as public information and eligible for auditing."[60] By August 2002, Quon continued to exceed his monthly allotment, and Duke had "grown tired of being a bill collector," so the department ordered an audit of Quon's messages to determine the necessity of a character-per-month increase.[61]

In order to carry out Scharf's orders for an investigation, Duke requested transcripts of the text messages from Arch Wireless, who held the messages in storage, in order to determine whether the messages were work-related in nature.[62] Duke and Scharf read the content of Quon's messages sent from August 1, 2002 to September 31, 2002.[63] Upon examination, the city determined that, in a month's total of 450 text messages, Quon had sent 57 work-related messages, while the rest were of a personal, and often sexually explicit, nature.[64] The sexually explicit text messages confirmed the water cooler gossip about Quon—while some of the racy messages were sent to his wife, Jerilynn, a fellow Ontario police officer, others were sent to his mistress and co-worker, Florio.[65]

As Sergeant Glenn conducted her investigation into the Hells Angels incident, she also wanted a peek at Quon's text messages to gauge just how inappropriate employees of the OPD were behaving, although no evidence at trial suggested that she actually read the messages.[66] After Duke and Scharf read the messages, the city demanded that Quon explain the sexually inappropriate messages, warned him about potential disciplinary action, and denied him a special assignment with the OPD.[67] Quon subsequently filed suit, alleging that the city violated Quon's privacy rights under the Fourth Amendment and

---

[58] *Id.* at 1124.
[59] *Id.*
[60] *Quon*, 529 F.3d. at 897.
[61] *Quon*, 445 F. Supp. 2d. at 1125.
[62] *Id.*
[63] *Id.*
[64] *Id.* at 1126.
[65] *Id.* at 1122.
[66] *Quon*, 445 F. Supp. 2d. at 1127.
[67] *Id.* at 1126.

California Constitution by viewing the text message content.[68] The other players in this melodrama—his wife, Florio, Klein and another officer—likewise filed suit, alleging their privacy rights had been violated due to the OPD reading their messages to Quon, although their suits were dismissed.[69]

While the trial court ultimately dismissed Florio's and Klein's claims, and the facts of their malfeasance do not bear on the doctrinal aspects of the *Quon* decision,[70] these facts demonstrate the tensions at play regarding workplace technology.[71] Like any savvy employer, the OPD upgraded its technology and provided pagers to its SWAT team members and dispatchers.[72] The city also knew enough to implement a formal technology anti-privacy policy, putting all employees on notice of possible surveillance.[73] Both of these administrative decisions exemplify employer interests in enhancing efficiency through communication-oriented technology and maintaining some control over the technology they provide to employees.[74] The OPD had an interest in managing the pager-use of an employee like Quon, whose consistent utilization of employer-provided technology for personal communications revealed his misuse of company time, for which he was earning a salary.[75] While the city may not have confronted the issue in a manner consistent with its own best interests, its decision to find out whether an employee used company time for his own personal communications reflects the concerns any employer has regarding employees wasting company time and resources.[76]

Conversely, the factual background of the *Quon* case reflects the realities that employees will follow managerial directives and, if given the impression that they will enjoy some sphere of privacy, they will continue to use workplace technology for private, sensitive communications. As demonstrated by the facts of the case, employees cheat on their spouses, have workplace affairs, and allow their personal problems to bleed into their professional lives—all the while potentially divulging this sensitive information to their employers by communicating about it on workplace computers, laptops and BlackBerries.

---

[68] *Quon*, 529 F.3d. at 898.
[69] *Id*.
[70] *Quon*, 445 F. Supp. 2d. at 1149.
[71] *Id*.
[72] *Id.* at 1123.
[73] *Id*.
[74] *Id*. at 1125.
[75] *Quon*, 445 F. Supp. 2d. at 1124.
[76] *Id.* at 1124.

Perhaps Quon should have known, on his own, not to send sexually explicit messages on his employer-provided pager, especially when the recipient was a fellow OPD employee who was not his co-worker/wife, but the realities of his workplace conveyed a mixed message. While the OPD had a general anti-privacy policy warning about surveillance, it also allowed another employee with supervisory power to lead Quon to believe he could avoid invasion into his text messages by paying his monthly overages. Many employees in Quon's position would likely have felt that his direct supervisor's actions trumped an anti-privacy policy, which he had probably skimmed, signed two years earlier and completely forgotten. Duke may have been trying to be a "nice guy" by allowing Quon to pay for his overages, but this informal practice stood contrary to all the OPD's formal written anti-privacy policies, and justified Quon's belief that he enjoyed some privacy in his text messages. These facts behind the OPD's policies and practices send a clear warning not only to employees, who should be aware of when their workplace communications will be monitored, but also employers, who may have supervisors sending contradictory and misleading messages about what when technology will be monitored and when communications will be kept private.

Although the *Quon* panel focused only on the facts regarding the OPD's anti-privacy policy and Quon's use of the pager, the general issues at the OPD embody the tension at play in the contemporary workplace. Both employers and employees have equally important stakes in the allocation of privacy rights regarding workplace privacy.

## III. THE *ORTEGA* FRAMEWORK: HOW THE SUPREME COURT AND THE CIRCUITS BALANCE EMPLOYER AND EMPLOYEE INTERESTS

After the OPD read his text messages, Quon filed suit alleging that the city violated Quon's Fourth Amendment rights, which protect individuals from unwarranted searches and seizures by the government.[77] In analyzing his Fourth Amendment claim, the Ninth Circuit applied the framework set forth by the Supreme Court in *O'Connor v. Ortega*.[78] With this seminal workplace privacy case, the Supreme Court confirmed that the Fourth Amendment protects one's reasonable expectation of privacy in the workplace.[79] In *Ortega*, the Supreme Court announced that public-sector employees may enjoy some privacy in the physical

---

[77] U.S. CONST. amend. IV.
[78] O'Connor v. Ortega, 480 U.S. 709 (1987).
[79] *Id*. at 716.

workplace, such as desks and file cabinets, based on whether the context of a particular workplace fosters within the employee a reasonable expectation of privacy.[80] The employer in *Ortega*, a state hospital, searched the office of one of its doctors as part of a sexual harassment investigation that eventually resulted in the employee's termination.[81] After his termination, Ortega claimed the search of his office violated his Fourth Amendment rights.[82] The plurality held that he enjoyed a reasonable privacy expectation in his physical workplace, and the government's search was unreasonable in its inception and scope.[83]

Justice O'Connor, writing for the plurality, set forth a contextual approach to examining whether employees have reasonable privacy expectations and employers conducted reasonable workplace searches.[84] To guide lower courts in investigating Fourth Amendment workplace privacy claims, the plurality applied a two-part inquiry.[85] First, in order to invoke Fourth Amendment workplace privacy protection, the employee must have enjoyed a reasonable privacy expectation in the area or thing intruded upon at work.[86] If the context of the employee's workplace fostered a reasonable privacy expectation, then some Fourth Amendment protection applies, requiring the employer to, at a minimum, provide some reasonable or legitimate reason for its intrusion into the employee's privacy.[87]

### *A. The First* Ortega *Test: Reasonable Employee Privacy Expectations*

Under the first *Ortega* inquiry, the Court focused its analysis on the particular context of a workplace in order to gauge the reasonableness of an employee's expectation of privacy.[88] According to the Court, this workplace includes "those areas and items that are related to work and are generally within the employer's control" and these "areas remain part of the workplace context even if the employee has placed personal items in them, such as a photograph placed in a desk or a letter posted on an employee bulletin board."[89] Mere access to an employee's items within the workplace—for example, personal items located in an employee's handbag, closed luggage or a briefcase—will not extinguish a reasonable

---

[80] *Id*. at 716.
[81] *Id*. at 712–14.
[82] *Id*. at 713.
[83] *Ortega*, 480 U.S. at 712–14.
[84] *Id.* at 726.
[85] *Id.* at 715–18.
[86] *Id.* at 716.
[87] *Id*.
[88] *Ortega*, 480 U.S. at 715.
[89] *Id*. at 715–16.

privacy expectation.[90] An employee's reasonable privacy expectation and subsequent Fourth Amendment protection hinge on the particular workplace structures and practices affecting the workplace in question.[91]

Justice Scalia wrote a concurrence in which he suggested an alternative test for Fourth Amendment application in the employment context.[92] Although he agreed that Ortega enjoyed a reasonable privacy expectation in his office, he expressed dissatisfaction with the plurality's contextual methodology and the Court's open invitation for employers to regulate privacy out of existence by manipulating the context of the workplace.[93] Accordingly, he feared that "[n]o clue is provided as to how open 'so open' must be" and that the plurality's standard is "so devoid of content that it produces rather than eliminates uncertainty in this field."[94] Justice Scalia instead proposed a categorical approach to workplace privacy invasions, insisting that his approach would more closely align with existing Fourth Amendment jurisprudence:

> Whatever the plurality's standard means . . . it must be wrong if it leads to the conclusion on the present facts that if Hospital officials had extensive work-related reasons to enter Dr. Ortega's office no Fourth Amendment protection existed. It is privacy that is protected by the Fourth Amendment, not solitude. A man enjoys Fourth Amendment protection in his home, for example, even though his wife and children have the run of the place—and indeed, even though his landlord has the right to conduct unannounced inspections at any time. Similarly, in my view, one's personal office is constitutionally protected against warrantless intrusions by the police, even though employer and co-workers are not excluded.[95]

Rather than determine whether workplace privacy exists on an ad hoc, case-by-case basis, as the plurality's test requires, Scalia would have created a categorical approach, in which "offices of government employees, and *a fortiori* the drawers and files within those offices, are covered by Fourth Amendment protections as a general matter."[96] Under his formulation, government employees would presumptively enjoy privacy protection in physical workspaces, and the inquiry as to whether

---

[90] *Id.* at 717.
[91] *Id*.
[92] *Id*. at 729 (Scalia, J., concurring).
[93] *Ortega*, 480 U.S. at 729 (Scalia, J., concurring).
[94] *Id*. at 729–30 (Scalia, J., concurring).
[95] *Id*. at 730–31 (Scalia, J., concurring) (internal quotes omitted).
[96] *Id*. (Scalia, J., concurring).

a privacy violation occurred would then turn on whether the government-employer's search was reasonable.[97] This categorical approach would have ensured a more predictable or consistent privacy protection for government employees than that afforded by the plurality's approach, which demonstrates a greater deference to employer interests in monitoring the workplace.[98]

Scalia's concerns seem prophetic considering how this portion of the *Ortega* test has been applied by the circuits, which routinely find that employer anti-privacy policies and other structural workplace manipulations by employers diminish employee expectations of privacy.[99] Regardless of Scalia's concerns and the incentives for employers created by the plurality's contextual methodology, a public-sector employee who alleges that his employer violated his privacy must demonstrate that his expectation of privacy is "reasonable under all the circumstances" of his particular workplace.[100]

### *B. The First* Ortega *Inquiry in the Circuits: Employer Privacy Policies Diminish Employee Privacy Expectations*

In the wake of *Ortega*, the circuits have applied the first *Ortega* prong by examining predictable factors in a given workplace, including an employee's "exclusive use" of a workspace, the degree to which the public has access to the workspace, and whether the employer disseminated an anti-privacy policy to place employees on notice for monitoring.[101] As a result of this contextual method, employers can alter the structure of the workplace by manipulating physical space and furniture and through general office practices that make spaces more open to the "public," in order to reduce or eliminate one's privacy expectation. Employers often achieve this result with regard to physical spaces and employee communications much more efficiently by simply using anti-privacy policies so as to render privacy expectations unreasonable.[102] For example, the Eighth Circuit has repeatedly held that when employers reserve the right to monitor workplace technology in a general policy, employees cannot have a reasonable expectation to

---

[97] *Id*. at 732 (Scalia, J., concurring).

[98] *Ortega*, 480 U.S. at 730.

[99] *See infra* Part III.B.

[100] *Ortega*, 480 U.S. at 721.

[101] *See* Am. Postal Workers Union v. United States Postal Service, 871 F.2d 566 (6th Cir. 1989); Schowengerdt v. Gen. Dynamics Corp., 823 F.2d 1328 (9th Cir. 1987); United States V. Taketa, 923 F.2d 665, 672 (9th Cir. 1991); McGregor v. Greer, 748 F.Supp. 881, 888 (D.D.C. 1990).

[102] *See* Heather L. Hanson, Note, *The Fourth Amendment in the Workplace: Are We Really Being Reasonable?*, 79 VA. L. REV. 243, 250 (1993).

privacy in communications sent on workplace computers and cell phones.[103]

Other circuit decisions demonstrate that anti-privacy policies can be dispositive as to whether an employee has a reasonable expectation to privacy. The Sixth Circuit, in *American Postal Workers Union v. United States Postal Service*, found that a postal worker had no reasonable expectation of privacy "in light of the clearly expressed provisions permitting random and unannounced locker inspections."[104] The court found that the employee's privacy expectation was unreasonable even though the employer had never actually conducted any unannounced locker inspection and therefore did not practice its policy.[105] Moreover, in *United States v. Angevine*, the Tenth Circuit found that an employee did not have a reasonable privacy expectation in his workplace computer when a "splash screen" warning discouraging employees from sending personal communications appeared every time he logged in to his computer.[106] In so holding, the court reasoned that the employer's "computer-use policy reserved the right to randomly audit Internet use and to monitor specific individuals suspected of misusing . . . computers," and the policy thereby placed the employee on notice as to monitoring, making his expectation of privacy unreasonable.[107] The Fourth, Seventh and Ninth Circuits have taken a similar approach in finding that anti-privacy policies defeat employee privacy expectations.[108]

---

[103] *See* Biby v. Bd. of Regents, 419 F.3d 845, 850–51 (8th Cir. 2005) (employee cannot have reasonable expectation of privacy when employment policy warned that employer could search employee computer for legitimate reason); United States v. Thorn, 375 F.3d 679, 683 (8th Cir. 2004) (employee denied any personal privacy right due to public agency's computer-use policy, which prohibited accessing sexual image and reserved the employer's right to access any computer in order to audit its use).

[104] American Postal Workers Union v. United States Postal Service, 871 F.2d 556, 560 (6th Cir. 1989).

[105] *Id*. at 560.

[106] United States v. Angevine, 281 F.3d 1130, 1133 (10th Cir. 2002). In this context, a "splash screen" refers to a page that is displayed when an employee turns on his computer or logs on to his e-mail system, warning that users are subject to possible criminal penalties and that information on the computer is not confidential. The screen may also reserve the employer's right to inspect computers to protect business-related concerns. *See* David Hricik & Chase Edward Scott, *Some Limits on Evidence Gathering in the Digital Age*, 25 GP Solo, 24, 26 (2008).

[107] *Angevine*, 281 F.3d at 1134.

[108] *See* United States v. Simons, 206 F.3d 392, 395 (4th Cir. 2000); Muick v. Glenayre Elecs., 280 F.3d 741, 743 (7th Cir. 2002) ("Glenayre had announced that it could inspect the laptops that it furnished for the use of its employees, and this destroyed any reasonable expectation of privacy . . . ."); United States v. Ziegler, 456 F.3d 1138, 1142 (9th Cir. 2006), *superceded by* United States v. Ziegler, 474 F.3d 1184 (9th Cir. 2007).

Conversely, the circuits have found that the absence of a general anti-privacy policy may foster a reasonable expectation of privacy in the workplace. In *McGregor v. Greer*, the United States District Court for the District of Columbia denied the employer-defendant's summary judgment motion because the workplace anti-privacy policy was unclear and the employee may have therefore had a reasonable privacy expectation.[109] The Second Circuit likewise found, in *Leventhal v. Knapek*, that an employee has a reasonable expectation of privacy in the contents of his office computer when the employer neither practiced routine searches on office computers nor disseminated a general anti-privacy policy.[110]

As demonstrated by these decisions, because an employee's privacy expectation must be reasonable before he has any Fourth Amendment protection, and because the *Ortega* framework works on a contextual rather than a categorical approach, private ordering has defined workplace privacy.[111] Therefore, employers may alter the context of a given workplace to eliminate employee privacy expectations so that they can conduct as much surveillance as desired.

*C: The Second Ortega Test*: *Reasonable Employer Searches*

Under the *Ortega* test, once an employee has established a reasonable expectation of privacy in a physical or Internet space, the inquiry turns to the second step, which is whether the employer's intrusion was justified. In creating this inquiry into the reasonableness of the employer's search, the Court carved out an exception for government-employers conducting workplace searches, allowing employers to circumvent historical Fourth Amendment requirements for probable cause and a search warrant.[112] The Court created an exception to these requirements mindful of employer interests in monitoring the workplace and the less-substantial privacy interests of government employees compared to the privacy interests of individuals in their homes.[113] The Court stated that a public-sector employer would not have

---

[109] McGregor v. Greer, 748 F. Supp. 881, 888 (D.D.C. 1990).

[110] Leventhal v. Knapek, 266 F.3d 64, 74 (2d Cir. 2001). *See also* United States v. Slanina, 283 F.3d 670, 676–77 (5th Cir. 2002).

[111] Professors Timothy Glynn, Rachel Arnow-Richman and Charles Sullivan define "private ordering" as "the rules the parties themselves establish to govern their relationship. Such ordering may occur by the parties' express agreement" or "implied from the circumstances" or even by "a 'default rule' establishing terms unless the parties 'opt out' by an agreement to the contrary." GLYNN, *supra* note 15, at XXV.

[112] *Ortega*, 480 U.S. at 737.

[113] *Id*.

to show the need for probable cause or obtain a warrant because "[t]he 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."[114]

Furthermore, the Court found that placing these normal Fourth Amendment burdens on public-sector employers would be unworkable in practice.[115] In so holding, the plurality relied on Justice Blackmun's concurrence in *New Jersey v. T.L.O.*, in which he stated that a public school teacher's search of a student's purse for cigarettes was reasonable because a "special needs" exception exists for teachers to respond to potential emergency situations.[116] Under such a "special needs" exception, a government employer is justified in not comporting with Fourth Amendment probable cause and search warrant requirements.[117] The *Ortega* plurality analogized public-sector employers to teachers, who have "neither the training nor the day-to-day experience in the complexities of probable cause that a law enforcement officer possesses, and [are] ill-equipped to make a quick judgment about the existence of probable cause."[118]

Similarly, the Court stated that "employers most frequently need to enter the offices and desks of their employees for legitimate work-related reasons wholly unrelated to illegal conduct" and that "requiring an employer to obtain a warrant whenever the employer wished to enter an employee's office, desk, or file cabinets for a work-related purpose would seriously disrupt the routine conduct of business and would be unduly burdensome."[119] Although Blackmun dissented from the plurality's application of the "special needs" exception in the public-sector context,[120] the plurality held that workplace searches would count as a "special needs" exception for normal Fourth Amendment probable cause and search warrant requirements.[121]

---

[114] *Id*. at 724.

[115] *Id*.

[116] The Court recognized "limited exceptions to the probable-cause requirement where a careful balancing of governmental and private interests suggests that the public interest is best served by a lesser standard." New Jersey v. T.L.O., 469 U.S. 325, 351 (1985) (Blackmun, J., concurring). In articulating this "special needs" exception, Justice Blackmun stated that, in such cases, the Court has "used such a balancing test, rather than strictly applying the Fourth Amendment's Warrant and Probable-Cause Clause, only when we were confronted with a special law enforcement need for greater flexibility." *Id*.

[117] *Id*.

[118] *Ortega*, 480 U.S. at 724. (quoting N.J. v. T.L.O., 469 U.S. 325, 353 (1985) (Blackmun, J., concurring)).

[119] *Id*. at 722.

[120] *Id*. at 742 (Blackmun, J., dissenting).

[121] *Id*. at 722.

Therefore, because workplace searches conducted by public-sector employers would fall under the "special needs" doctrine, the standard for determining whether an employer's search is justified is one of "reasonableness."[122] The Court acknowledged the interests of public-sector employers "in ensuring that their agencies operate in an effective and efficient manner."[123] The Court further stated that "the work of these agencies inevitably suffers from the inefficiency, incompetence, mismanagement, or other work-related misfeasance of its employees."[124] In providing this exception, the Court did not seem greatly concerned with employee privacy beyond whether the context of a given workplace makes the employee's expectation of privacy reasonable, stating that the burden to avoid privacy violations should be on employees, who "may avoid exposing personal belongings at work by simply leaving them at home."[125]

Then, to avoid a finding that its search violated this expectation of privacy, the government-employer must justify its intrusion as reasonable.[126] The reasonableness of an employer's search has two components.[127] First, the search must be reasonable at its inception, with the employer having some "reasonable grounds for suspecting that the search will turn up evidence that the employee is guilty of work-related misconduct."[128] Second, the search must be reasonable in scope, which requires the employer to adopt measures that are "reasonably related to the objectives of the search and not excessively intrusive in light of . . . the nature of the [misconduct]."[129] Again, this inquiry provides deference to employers in choosing the methods they employ in conducting workplace searches.

While the *Ortega* plurality merely instructed courts, in reviewing whether an employer's search was reasonable, to find whether a reasonable nexus existed between the objectives of the search and the actual search conducted, the Supreme Court later explicitly rejected examining whether an employer could have used less intrusive means to achieve its legitimate purposes. In *Skinner v. Railway Labor Executives' Association*, the Court analyzed a public-sector employee's claim that his employer's use of drug testing violated his Fourth Amendment privacy

---

122 *Id*.
123 *Ortega*, 480 U.S. at 724.
124 *Id*. at 724.
125 *Id*. at 725.
126 *Id*. at 723.
127 *Id*. at 725.
128 *Ortega*, 480 U.S. at 726.
129 *Id.* (citing N.J. v. T.L.O., 469 U.S. 325, 342 (1985)).

rights.[130] In holding that the employer had a legitimate interest in maintaining safety and efficiency and that its use of drug testing to ensure these interests was reasonable in its inception and scope, the Court rejected the employee's contention that the search was unreasonable because the government-employer could have used less invasive means to uncover whether employees used drugs.[131]

The *Skinner* Court affirmatively stated that, under an analysis of the second *Ortega* prong, it would not demand lower courts to inquire whether there were less intrusive means available when an employer conducts a workplace search.[132] The Court reasoned that using this standard to determine the nexus between the employer's interest in conducting a search and the reasonableness of the search would undermine the *Ortega* plurality's concern for respecting legitimate employer interests:

> We have repeatedly stated . . . that '[t]he reasonableness of any particular government activity does not necessarily or invariably turn on the existence of alternative 'less intrusive' means. It is obvious that '[t]he logic of such elaborate less-restrictive-alternative arguments could raise insuperable barriers to the exercise of virtually all search-and-seizure powers,' because judges engaged in *post hoc* evaluations of government conduct 'can almost always imagine some alternative means by which the objectives of the [government] might have been accomplished.'"[133]

Thus, the Supreme Court has clearly decided against a requirement that employers exhaust less-invasive workplace monitoring.[134]

---

[130] Skinner v. Ry. Labor Executives' Ass'n, 489 U.S. 602, 629 (1989).

[131] *Id*.

[132] *Id*. at 629, n.9.

[133] *Id*. (internal citations omitted).

[134] *See also* Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 663 (1995) ("We have repeatedly refused to declare that only the 'least intrusive' search practicable can be reasonable under the Fourth Amendment."); Bd. of Educ. v. Earls, 536 U.S. 822, 837 (2002) ("[T]his Court has repeatedly stated that reasonableness under the Fourth Amendment does not require employing the least intrusive means"); Illinois v. Lafayette, 462 U.S. 640, 647 (1983); Colorado v. Bertine, 479 U.S. 367, 373–74 (1987); United States v. Martinez-Fuerte, 428 U.S. 543, at 556–57 n. 12.

### *D. The Second Ortega Prong in the Circuits: Rejection of the "Least Intrusive Means" Test*

Similar to the first prong, the circuits have followed the Supreme Court's framework for analyzing whether an employer's search is reasonable in its inception and scope. For example, the Second Circuit, in *Leventhal v. Knapek*,[135] applied the second prong of *Ortega* to hold that, based on the fact that the employer reasonably suspected the employee was neglecting his duties, its searches of his computer were reasonable in light of the state's need to investigate the allegations of the employee's misconduct.[136] In so holding, the Second Circuit set forth the model analysis under this prong: a court will identify the employer's interest at stake in the search and then determine whether the actual search conducted is reasonable in comparison.[137] If the search proves to be excessive, it is unreasonable and the employee will succeed on his Fourth Amendment claim.[138]

After the Supreme Court announced its unwillingness to analyze an employer's searched based on an analysis of less-intrusive means when an employer conducted a workplace search, seven circuits likewise rejected the "least intrusive means" test.[139] However, in a case that

---

[135] *Levanthal*, 266 F.3d 64 (2d Cir. 2001).

[136] *Id*.

[137] *Id.*

[138] *But see* Rossi v. Town of Pelham, 35 F. Supp. 2d 58 (D.N.H. 1997) (local government employee enjoyed a reasonable expectation of privacy to her office, and a warrantless search by a police officer infringed upon this privacy expectation because the search could have been conducted less intrusively by a non-officer); United States v. Taketa, 923 F.2d 665 (9th Cir. 1991) (police officers did have a reasonable expectation of privacy in their office that they would not be videotaped, and probable cause was required for such videotape surveillance).

[139] *See* Lockhart-Bembery v. Sauro, 498 F.3d 69, 76 (1st Cir. 2007) ("To the extent Lockhart-Bembery argues that Sauro acted unreasonably [under the Fourth Amendment] because there were other, less intrusive ways to reduce the safety hazard, that argument fails as a matter of law. There is no requirement that officers must select the least intrusive means of fulfilling community caretaking responsibilities."); Cassidy v. Chertoff, 471 F.3d 67, 79 (2d Cir. 2006) ("The Supreme Court has repeatedly stated that reasonableness under the Fourth Amendment does not require employing the least intrusive means to accomplish the government's ends.") (internal quotation marks omitted)); Davenport v. Causey, 521 F.3d 544, 552 (6th Cir. 2008) ("The Fourth Amendment does not require officers to use the best technique available as long as their method is reasonable under the circumstances."); Shell v. United States, 448 F.3d 951, 956 (7th Cir. 2006) ("As an initial matter, we note that a search does not need to be the least intrusive alternative to be constitutionally valid, it simply has to be reasonable."); Shade v. City of Farmington, 309 F.3d 1054, 1061 (8th Cir. 2002) ("The Fourth Amendment does not require officers to use the least intrusive or less intrusive means to effectuate a search but instead permits a range of objectively reasonable conduct."); United States v. Melendez-Garcia, 28 F.3d 1046, 1052 (10th Cir. 1994) (stating that the Fourth Amendment does not require police "to use the least intrusive means in the course

predates *Skinner*, the Ninth Circuit applied this rejected standard in its analysis of the second *Ortega* prong in *Schowengerdt v. Gen. Dynamics Corp*.[140] In *Schowengerdt*, the court held that if the employer could have used less intrusive means to conduct the search to further its legitimate interest, the search would be unreasonable.[141] In that case, an employee's locked desk was searched for sexual materials, and he filed suit alleging that the search violated his privacy expectation.[142] In remanding to the lower court to find whether the employer's search was reasonable at its inception and in scope, the Ninth Circuit stated that "[i]f less intrusive methods were feasible, or if the depth of the inquiry or extent of the seizure exceeded that necessary for the government's legitimate purposes, such as its interest in security, the search would be unreasonable and Schowengerdt's Fourth Amendment rights and right to privacy would have been violated."[143]

The *Skinner* Court explicitly rejected this inquiry into less-intrusive searches as too onerous a burden on employers conducting workplace searches.[144] The *Quon* panel directly justified its result in finding the OPD's search to be unreasonable on this "less intrusive means" language in the *Schowengerdt* decision.[145] As discussed in the next section, this Comment posits that by citing a pre-*Skinner* decision that is no longer good law as part of its analysis under the second *Ortega* prong, the *Quon* panel not only departed from Supreme Court precedent and split from seven sister circuits but also upset the balance struck by the *Ortega* plurality between the conflicting privacy interests of employers and employees.

## IV. THE NINTH CIRCUIT'S APPLICATION OF THE *ORTEGA* FRAMEWORK IN *QUON*

Quon succeeded in arguing that the city violated his Fourth Amendment rights by reading his text messages and defying his reasonable expectation of privacy.[146] In so holding, the *Quon* panel correctly applied the first *Ortega* prong to find he had a reasonable

---

of a [Terry] detention, only reasonable ones"); United States v. Prevo, 435 F.3d 1343, 1348 (11th Cir. 2006) ("Suffice it to say that the Fourth Amendment does not require the least intrusive alternative; it only requires a reasonable alternative.").

[140] Schowengerdt v. General Dynamics Corp., 823 F.2d 1328 (9th Cir. 1987).

[141] *Id*. at 1336.

[142] *Id*.

[143] *Id*.

[144] *Skinner*, 489 U.S. at 629, n.9.

[145] *Quon*, 529 F.3d at 909.

[146] *Id*. at 908.

expectation of privacy.[147] However, the panel mistakenly used language from the *Schowengerdt* decision and found the OPD's search to be unreasonable based on an analysis of less intrusive means the city could have used when conducting the search of Quon's text messages.[148]

Under its analysis of the first *Ortega* prong, the panel correctly applied the contextual *Ortega* methodology and based its conclusion that Quon had a reasonable expectation of privacy on the fact that the OPD had an informal practice of allowing Quon to pay his overages, despite the formal anti-privacy policy.[149] The court found that Quon's expectation of privacy was reasonable due to his employer's conflict between a general anti-privacy policy and an informal practice of allowing Quon to maintain his privacy in his text messages.

Therefore, regarding the panel's analysis of the first *Ortega* prong, the *Quon* court's conclusion is important because it instructs employers on how to structure and enforce workplace anti-privacy policies. This portion of the holding stands as a lesson for employers who want to maximize workplace surveillance by not only creating an anti-privacy policy but strictly enforcing it in order to render unreasonable any workplace expectation of privacy.

Regarding the analysis under the second prong, the panel applied the rejected "less intrusive means" standard and shifted the balance struck by the *Ortega* plurality.[150] In finding that the OPD's search was unreasonable, the court adduced that it could have used several less intrusive hypothetical means to achieve its goal of monitoring the pagers.[151] As part of its analysis, the panel quoted from its decision in *Schowengerdt*, despite the fact that *Skinner* Court superceded the *Schowengerdt* decision when it rejected the "least intrusive means" test.[152]

In the wake of this controversial finding, the OPD petitioned for the Ninth Circuit to rehear the case en banc.[153] This effort split the Ninth

---

[147] *Id*.

[148] *Id.* at 909.

[149] *Id.* at 908.

[150] *Quon*, 529 F.3d at 909.

[151] *Id.*

[152] *Quon*, 554 F.3d at 777–78 (Ikuta, J., dissenting from the denial of rehearing en banc).

[153] *Id.* at 774. The Ninth Circuit en banc procedure has complexities that other circuits do not. The Ninth Circuit has the distinction of being the largest circuit court in the country, with 28 authorized judgeships. *Final Report of the Commission on Structural Alternatives for the Federal Courts of Appeals Before the S. Comm. on Courts and Intellectual Property of the H. Comm. on the Judiciary.* 106th Cong. 220 (1999) (prepared statement of Hon. Byron R. White, Chair, White Commission). This makes traditional en banc petitions, which require all the judges in a circuit to rehear the case,

Circuit: the original three-judge panel and a majority of active Ninth Circuit judges voted to deny the petition to rehear the case, with Judge Wardlaw writing a concurrence defending the denial, while seven judges dissented from the denial of a rehearing, led by Judge Ikuta's impassioned dissent.[154] In his dissent, Ikuta correctly maintained that the panel's analysis of whether the OPD could have used less intrusive means to investigate employee pager use and protect its interest in workplace efficiency runs contrary to the *Ortega* plurality's concerns with placing too great a burden on employers.[155]

In her concurrence to the rehearing denial, Judge Wardlaw insisted that the panel did not employ the rejected test and instead merely ensured the reasonableness of the nexus between the interest and the search.[156] As part of this rationale, Wardlaw tried to justify the panel's analysis of the less-intrusive means the OPD could have used by distinguishing the cases in which the Supreme Court rejected the "least intrusive means" test.[157] However, the test was explicitly rejected by the Supreme Court and seven sister circuits, and Wardlaw and the panel ultimately ignored the *Ortega* plurality's edict that all workplace searches by public-sector employers fall under the "special needs" exception, and the employer, upon conducting a search, must only demonstrate some justification for conducting the search.[158] As a result of the use of this test, the Ninth Circuit split from sister circuits and potentially upset the *Ortega* balance between employer and employee interests.[159]

---

impracticable. Due to its unruly size, the Ninth Circuit availed itself of Congress's modified en banc procedure, allowing any circuit with more than 15 authorized judgeships to designate its own rule for how many judges will hear a case en banc. *See* 28 U.S.C. § 46(c) and Pub. L. No 95-486, § 6. Accordingly, the Ninth Circuit requires that the chief judge, along with at least 10 of the 28 judges, sit for a petition to rehear en banc, and that this 11-judge panel will rehear the case if they unanimously agree. USCS Ct App 9th Cir., Circuit R 35–3. Regarding the OPD's petition, because Judges Pregerson, Wardlaw, and Leighton, comprising the original three-judge *Quon* panel, voted to deny the petition to rehear the case en banc. Furthermore, when the full court was advised of the petition for rehearing en banc, a majority of the votes of the nonrecused active judges in favor of en banc reconsideration. Fed. R. App. P. 35. For an in-depth exploration of how the Ninth Circuit's size, and the resulting inefficiencies, harms "nearly 20 percent of the nation's population," see *Examining the Proposal to Restructure the Ninth Circuit: Hearing on S. 1845 Before the S. Comm. on the Judiciary*, 109th Cong. 2 (2006) (statement of Rachel L. Brand, Asst. Att'y Gen. for the Office of Legal Policy), *available at* http://www.usdoj.gov/olp/pdf/ninth_circuit_split_aag_brand_testimony.pdf.

[154] *Quon*, 554 F.3d at 769.

[155] *Id*. (Ikuta, J., dissenting from the denial of rehearing en banc).

[156] *Id.* (Wardlaw, J., concurring in the denial of rehearing en banc).

[157] *See infra* Part IV.B.

[158] *Ortega*, 480 U.S. at 724. *See also supra* Part III.C. and D.

[159] *Quon*, 529 F.3d at 777–78 (Ikuta, J., dissenting from the denial of rehearing en banc). *See also supra* Part III.D.

*A. Quon's Reasonable Expectation of Privacy: Conflict Between an Informal Practice and a Formal Anti-Privacy Policy*

Despite the city's formal anti-privacy policy warning employees about the possibility of surveillance, the Ninth Circuit applied the *Ortega* contextual methodology to find that Quon had a reasonable expectation of privacy based on Duke's informal practice of allowing Quon to pay for personal character overages to avoid an audit.[160] Accordingly, the Ninth Circuit determined that the OPD had created a reasonable privacy expectation because it had a contrary informal practice of allowing the officers to pay for overages to avoid audits.[161]

In the denial to rehear *Quon* en banc, Judges Wardlaw and Ikuta agreed on the standard under the first *Ortega* prong but haggled over the factual realities of the OPD and whether the informal practice actually created a reasonable privacy expectation for Quon.[162] Ikuta argued that the mixed messages sent by the OPD should be trumped by the formal written policy, while Wardlaw maintained that the informal practice negated the written anti-privacy policy and gave Quon a reasonable expectation of privacy in the content of his text messages.[163] Essentially, Wardlaw correctly stated that Quon's expectation was reasonable because any employee who would have been told that he could avoid an audit of his messages if he paid the overages himself would expect his messages to remain private if he kept paying. Therefore, this portion of the panel's decision is correct based on the operational realities of Quon's workplace.

This holding is important because it sends a message to employers that they could potentially be held liable for workplace privacy invasions if they allow an informal practice to foster a reasonable expectation of privacy within employees. Therefore, *Quon* instructs employers on how they can structure workplace practices and conduct surveillance without making the OPD's same mistake of creating and then violating employee expectations of privacy. In order to discourage employee expectations of privacy, employers now know that they must not only disseminate a general anti-privacy policy but also that they must take measures to strictly practice that policy to avoid the creation of reasonable privacy expectations.[164]

---

[160] *Quon*, 529 F.3d at 897.
[161] *Id.*
[162] *Quon*, 554 F.3d at 770, 774.
[163] *Id.* at 770, 774.
[164] *See* Mark E. Schreiber and Barbara A. Lee, *Practice Tips: New Liabilities and Policies for Incidental Private Use of Company Electronic Systems and PDAs*, 52 BOSTON BAR JOURNAL 11 (2008). ("[*Quon*] . . . provides a sobering example of why

At its most extreme, the court's holding under the first *Ortega* prong provides a perverse incentive for employers to routinely intrude into employee privacy, to ensure that no informal practices on surveillance reverse the presumption that employees do not enjoy a privacy expectation under general privacy policies. If an Information Technology specialist or general manager gives employees the impression that the company will not actually conduct surveillance, then the employee may be found to have enjoyed a reasonable expectation of privacy that then limits how the employer may conduct a workplace search.[165]

At the same time, the holding is important for employees because of the potential downstream effects it could have on how employers structure workplaces. At first glance, the panel's result—finding that an employee enjoyed a reasonable expectation of privacy on his employer-provided pager, used under a general anti-privacy policy—seems to provide some increased privacy protection for employees. Although the court found that Quon had a reasonable privacy expectation, and this seems like a victory for employees who want greater workplace privacy protection, this decision may result in enhanced protection only in a narrow set of cases in which an employer failed to enforce its formal policy. Indeed, the *Quon* decision itself is a warning signal that this decision provides for subsequent employers, who now know that they must practice what they preach in terms of privacy and surveillance.[166]

Practically speaking, if employers really do pick up on the cues of the *Quon* decision and regularly enforce their surveillance policies, the context of a given workplace will place employees on notice that their employers are looking over their shoulders when they communicate on workplace computers, laptops, and cell phones. In this regard, the decision could result in fewer mixed messages like the ones the OPD

---

companies should be alert to this problem so they can adjust their strategies accordingly.").

[165] *Ortega*, 480 U.S. at 730.

[166] *See* Schreiber, *supra* note 164 (describing *Quon* and setting forth explicit lessons employers should learn from the case, including drafting "policies regarding employee use of email, internet access, and PDAs" that are "clear that employees have no expectation of privacy and can expect their use of these systems and devices, including personal use and messages, to be subject to monitoring and access by the employer with or without notice."); CALIFORNIA EMPLOYER'S GUIDE TO EMPLOYEE HANDBOOKS AND PERSONNEL POLICY MANUALS, 1-2 CA Guide to Employee Handbooks § 2.16 ("The Quon decision serves as a reminder that employers must avoid statements and actions that might be construed as giving employees a reasonable expectation of privacy in electronic messages or other data created or transmitted using Company equipment. In this regard, it is important that all managers in an organization stay 'on message' where surveillance of employee communications is concerned.").

sent to its employees and will instead encourage full disclosure when surveillance occurs. Ironically then, the contextual methodology espoused by the *Ortega* plurality and underlying the *Quon* decision ultimately creates an equilibrium in which employers have an incentive to maximize surveillance to reduce employee expectations of privacy. Accordingly, employees can trust they are being watched at all times and are less likely to share personal correspondence on employer-provided technology.

*B. The Quon Court's Use of the "Least Intrusive Means" Test*

Pro-employee advocates in search of expanded workplace privacy rights should instead look to the *Quon* panel's analysis under the second *Ortega* prong, in which the panel inquired into less-intrusive means the OPD could have used to conduct its search. Upon finding Quon had a reasonable expectation of privacy in his text messages, the panel investigated the reasonableness of the OPD's search of his messages and held that the search was unreasonable in its scope.[167] As any court must first determine when examining the reasonableness of a workplace search, the Ninth Circuit panel identified what objective the OPD actually had in conducting the search.[168] The panel reiterated that, at the trial level, the jury determined that the purpose of the search was to determine the "efficacy of the existing character limits to ensure that officers were not paying hidden work-related costs."[169] The trial court instructed the jury that if it found this to be the purpose of the search then they must find that the search was reasonable as a matter of law, and the OPD was not found liable as a result. However, on appeal, the Ninth Circuit panel determined that the "search was nevertheless unconstitutional" because it found that the search, for Scharf's intended purpose, "was not reasonable in scope."[170]

As part of its determination that the search conducted was unreasonable in scope, the panel quoted *Schowengerdt*, stating that "if less intrusive methods [to investigate Quon's overages] were feasible, or if the depth of the inquiry or extent of the seizure exceeded that necessary for the government's legitimate purposes . . . the search would be unreasonable . . . ."[171] Then, the Ninth Circuit inquired into the reasonableness of the city's investigation based not on the actual search

---

[167] *Quon*, 529 F.3d at 908.
[168] *Id*.
[169] *Quon*, 445 F. Supp. 2d at 1146.
[170] *Quon*, 529 F.3d at 908.
[171] *Id.* (quoting Schowengerdt v. General Dynamics Corp., 823 F.2d 1328, 1336 (9th Cir. 1987)).

conducted, but rather on a litany of hypothetical less-intrusive means the city could have used when conducting the search:

> There were a host of simple ways to verify the efficacy of the 25,000 character limit (if that, indeed, was the intended purpose) without intruding on [Quon's] Fourth Amendment rights. For example, the Department could have warned Quon that for the month of September he was forbidden from using his pager for personal communications, and that the contents of all of his messages would be reviewed to ensure the pager was used only for work-related purposes during that time frame. Alternatively, if the Department wanted to review past usage, it could have asked Quon to count the characters himself, or asked him to redact personal messages and grant permission to the Department to review the redacted transcript.[172]

Based on these alternative, potentially burdensome methods the OPD could have utilized to discover the reason for Quon's regular monthly overages, the Ninth Circuit found that reading his messages "was excessively intrusive in light of the noninvestigatory object of the search."[173]

The issue as to whether the Ninth Circuit panel actually used the rejected "least intrusive means" test stands at the center of the disagreement between Judge Ikuta, writing for the dissent to rehear *Quon* en banc, and Judge Wardlaw, who concurred in the denial and wrote the original panel opinion. Ikuta outright accused the panel of applying the rejected test when it concluded that, as a matter of law, the search was unreasonable in scope because the city could have used several less intrusive means of investigating the efficacy of increasing the monthly character limit.[174] In Ikuta's estimation, the use of the *Schowengerdt* "less intrusive means" language, after the Supreme Court explicitly

---

[172] *Id.* at 909. Like any appellate court, the Ninth Circuit *Quon* panel was confined to the jury's factual findings on the record on appeal and therefore had to assume that Scharf's purpose in conducting the search was to determine whether to increase the monthly character allotment, as opposed to the alternative theory that they wanted to determine whether Quon was misusing company time by using his pager for personal communications. However, the panel's analysis of the less-intrusive means the OPD could have used, as well as it's insinuation that the monthly character increase was not his actual intended purpose, signals that perhaps the panel did not agree with the jury's finding, and the use of this rejected test allowed them a back door to ultimately finding the search unreasonable.

[173] *Id.*

[174] *Quon*, 554 F.3d at 777 (Ikuta, J., dissenting from the denial to rehear en banc).

rejected this standard in *Skinner*, places too great a burden on the government-employer when it conducts a workplace searches.[175] According to Ikuta, the Ninth Circuit's application of the rejected test violates the instruction set forth in *Skinner* and also ignores the underlying spirit of the *Ortega* plurality's concern for balancing employee and employer interests.[176]

Judge Ikuta has the better argument regarding the *Quon* panel's analysis of the OPD's search because it is rooted in Supreme Court precedent and decisions of the majority of sister circuits. Arguing against Ikuta, Wardlaw contended that the panel used the *Schowengerdt* language because it "relate[d] to the jury's finding that Chief Scharf conducted the search for noninvestigatory purposes."[177] Wardlaw justified the presence of this "least intrusive means" language in the court's decision by stating that the panel "mentioned other ways the [OPD] could have verified the efficacy of the 25,000-character limit merely to illustrate our conclusion that the search was 'excessively intrusive' under *Ortega*, when measured against the purpose of the search as found by the jury."[178] Wardlaw also sought to defend the panel's use of the "least intrusive means" test by stating that the "cases in which the Supreme Court has cautioned against employing a 'least intrusive means' test have often involved circumstances in which the government had engaged in years of investigation and study that resulted in reasonable conclusions that the government conduct was necessary."[179] Furthermore, Wardlaw stated that, unlike cases relied upon by the dissent, *Quon* did "*not* involve a 'special needs' search," making, she argued, the panel's use of the least intrusive means test acceptable.[180]

Both of these arguments do not justify the panel's use of the rejected test. First, while some of the cases in which the Supreme Court

---

[175] Judge Ikuta used the language of the *Skinner* Court to explain why "the panel's approach fits squarely within the Supreme Court's explanation of why the least intrusive means test is *not* appropriate: '[i]t is obvious that the logic of . . . elaborate less-restrictive-alternative arguments could raise insuperable barriers to the exercise of virtually all search-and-seizure powers, because judges engaged in *post hoc* evaluations of government conduct can almost always imagine some alternative means by which the objectives of the government might have been accomplished.'" *Quon*, 554 F.3d at 778 (Ikuta, J., dissenting from the denial to rehear en banc) (quoting Skinner v. Railway Labor Executives' Ass'n, 489 U.S. at 629 n.9).

[176] *Id*. at 778.

[177] *Id*. at 772.

[178] *Id.* at 771.

[179] *Id*. at 773 (citing Skinner v. Railway Labor Executives' Ass'n, 489 U.S. 602, 629 n.9 (1989)).

[180] *Quon*, 554 F.3d. at 773.

explicitly rejected the test did feature "years of investigation and study," the Court never explicitly stated that, in cases in which no long-term study occurs, an employer must use the least intrusive means possible when conducting a search.[181] Furthermore, Wardlaw erred in stating this was not a "special needs" context because, as the *Ortega* plurality made clear, searches conducted by public-sector employers count as "special needs" searches that circumvent the normal Fourth Amendment requirements for probable cause and search warrants.[182] Then, despite Wardlaw's characterizations to the contrary, the panel utilized the rejected test. The *Quon* decision therefore reflects a departure from Supreme Court jurisprudence and the Fourth Amendment jurisprudence in the other circuits.[183]

Underlying Ikuta's concerns—and the central issue at the heart of this circuit split—is the potential shift in the balance between employer and employee interests embodied by the use of the "least intrusive means" test. By employing this reasoning, the Ninth Circuit placed the burden on the OPD to exhaust alternative investigations into employee conduct before infringing on reasonable privacy expectations.[184] The Ninth Circuit's application of the rejected test violates the instruction set forth in *Skinner* and also ignores the concern underlying the *Ortega* plurality's balance of employee and employer interests. While the Ninth Circuit was correct in its reasoning under the first *Ortega* prong, its litany of "less intrusive means" undercuts the warrantless search purpose of the *Ortega* decision and Justice O'Connor's concerns that "government offices could not function if every employment decision became a constitutional matter."[185] While an expansion of workplace privacy rights may be beneficial for employees, the use of a least intrusive means test and its resulting burdens on employers could negatively impact an employer's ability to monitor workplace efficiency, productivity, and safety.[186]

Despite the theoretical burden the Ninth Circuit has placed on employers by utilizing the "least intrusive means" test, this split may not

---

[181] While the factual scenarios in the background of many of the decisions in which the Supreme Court has rejected the "least intrusive means" test do feature "years of investigation and study," the Court has never explicitly stated that it has rejected the use of this burdensome standard based on the fact that general studies have been conducted. *Skinner*, 489 U.S. at 629. The Court did not base its rejection of the test on that, and its subsequent decisions rejecting the "least intrusive means" test feature factual scenarios that do not center on "years of investigation and study." *See supra* Part III.C.

[182] *Ortega*, 480 U.S. at 722. *See also supra* Part III.C.

[183] *See supra* Part III.

[184] Green, *supra* note 10, at 369.

[185] *Ortega*, 480 U.S. at 722 (quoting Connick v. Myers, 461 U.S. 138, 143 (1983)).

[186] *See Quon*, 554 F.3d at 778 (Ikuta, J., dissenting from the denial to rehear en banc).

have any lasting implications for employee privacy rights. Before inquiring into the reasonableness of an employer's search, a court must always first locate a reasonable privacy interest on the part of the employee.[187] As discussed above, while the Ninth Circuit found the employee's expectation to be reasonable in the context of his workplace, the decision stands as an example of a careless employer who did not practice its anti-privacy policy, and future employers now have notice to avoiding a similar result.[188] If employers now have notice to conduct routine surveillance and render unreasonable employee expectations of privacy, the *Quon* decision suggests that employees may rarely have a reasonable privacy expectation in the future. If employees do not have a reasonable expectation of privacy in the workplace, then employers may conduct whatever searches they want, regardless of whether they use the least intrusive means possible. *Quon*, then, may ultimately represent the limitations inherent in the current workplace privacy framework and perhaps signals that the tension between employer and employee privacy interests must be confronted not by judge-made law but by legislators.

## V. SHOULD WORKPLACE PRIVACY BE LEFT TO PRIVATE ORDERING?

The impassioned disagreement raised by the en banc denial, sparking debate between Judges Ikuta and Wardlaw, demonstrates that the *Ortega* contextual methodology, as Justice Scalia predicted, leads to uncertainty and confusion.[189] Additionally, the *Ortega* test's focus on the context of a given workplace has provided the opportunity for employers, who structure how an office operates, to diminish employee privacy expectations.[190] Several commentators suggest that these flaws in the *Ortega* framework present insurmountable obstacles to ensuring substantive workplace privacy protection and that judges should find alternative means to analyze Fourth Amendment workplace privacy violations.[191]

---

[187] *Ortega*, 480 U.S. at 716.

[188] Schreiber, *supra* note 164.

[189] *Ortega*, 480 U.S. at 729–30 (Scalia, J., concurring).

[190] *See* Hanson, *supra* note 102. Hanson describes the *Ortega* framework as presenting two insurmountable limitations for employees. *Id.* at 245–46. First, the framework, originally meant as an exception to the probable cause warrant requirement, allows employers to conduct searches instead of police officers, who are constrained by societal norms and formal procedural restrictions. *Id.* Second, Hanson sees the requirement that, upon a finding of a privacy expectation, the government's search be "reasonable" as overly deferential to the government. *Id.*

[191] Hanson suggests that courts should apply a property-based analysis to Fourth Amendment workplace privacy claims. Under this approach, she suggests that courts would have a "bright-line, objective definition of Fourth Amendment protection largely beyond an employer's control" and "the property rights focus functions as a fairly good

Ultimately, by allowing a workplace context to define the privacy right an employee may enjoy in a society in which "[t]echnological and communication advances mean that much of everyday life is now recorded by someone somewhere," the Court has perhaps diminished Brandeis' conception of the essential "right to be left alone."[192] Scalia's categorical approach may have ensured a more dependable or predictable privacy protection for employees, but the Supreme Court has made clear that the context of a workplace will define what an employee can expect regarding his right to workplace privacy, and that is simply the current state of the law.

Despite the fact that the *Ortega* framework allows employers to have their cake and eat it too, perhaps the *Ortega* plurality had it right all along and private ordering should rule the day, with employers dictating the terms of a workplace context and that context defining the limits of what privacy employees can expect to enjoy. The concept of allowing private ordering to ultimately dictate the parameters of workplace privacy finds a basis in what Professor Scott Sundby refers to as the true underlying metaphor or guiding principle of the Fourth Amendment:

---

proxy for what the government does not legitimately need and should not be able to get, clearly delineating what should fall outside of 'legitimate' internal governance concerns." Hanson, *supra* note 102, at 264. This approach, while delineating clearer distinctions between precisely what is protected would prove problematic when applied to laptops, cell phones and BlackBerries, which are owned by employers but used outside the office, making them even more likely to contain personal information.

Professor Stephen Schulhofer argues that workplace searches should be allowed without probable cause or a warrant only if pressing health and safety concerns are at issue, or if there are "internal governance imperatives," a standard similar to the noninvestigatory, work-related searches allowed to ferret out misconduct by the *Ortega* plurality. Schulhofer is concerned primarily with workplace drug tests, and, while his standard would provide more rigorous protection of employee bodily integrity, the standard would still provide great deference to government-employer interests and would therefore not differ greatly from the *Ortega* approach. Stephen J. Schulhofer, *On the Fourth Amendment Rights of the Law-Abiding Public*, 1989 SUP. CT. REV. 87, 90–123 (1989).

In examining the general values at stake when the government seeks to obtain information or conduct a search, Professor Christopher Slobogin has re-imagined what privacy jurisprudence would look like without the Fourth Amendment. In its place, Slobogin proposes a new federal scheme, developed on the basis of various state and individual interests that inform the regulation of government searches and seizures. At the heart of Slobogin's theoretical proposal lies some sort of *ex ante* review of searches and seizures. Pertinent to the "special needs" exception of workplace searches, Slobogin bases his proposal of this *ex ante* review on an "exigency principle," requiring the government to obtain third party authorization from a lay decision maker prior to any nonemergency search or seizure (the "exigency principle"). As part of the substantive component of this hypothetical replacement scheme, Slobogin would mandate that the level of certainty required to authorize a particular search or seizure should be roughly proportional to the level of its intrusiveness. Christopher Slobogin, *The World Without a Fourth Amendment*, 39 UCLA L. REV. 1, 11–47 (1991).

[192] Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

trust between the government and private citizens.[193] Although the "the notion of trust sounds, and is in many ways, so simple, so nonlegalistic, and so nonphilosophical, that it risks being dismissed as not sufficiently grounded in legal-political theory," Sundby argues that this metaphor asks the one essential question concerning government intrusions into the individual's sphere of privacy: "is the government's action inconsistent with trusting the citizenry to behave in a lawful and responsible fashion?"[194]

While Sundby focuses his exploration of trust-as-metaphor on all aspects of government intrusions and Fourth Amendment jurisprudence, it finds strong echoes in the dilemma of balancing employer and employee interests, as exemplified by the *Quon* decision. Sundby focuses on the government's need for implicit trust of the citizenry, but this metaphor should be turned on its head in the workplace context: as the *Quon* decision demonstrates, employers and employees have ample reasons for mutual distrust, with employers suspecting employees of laziness and wrongdoing, and employees suspecting employers invade personal communications on workplace technology.

Perhaps *Quon* can teach the lesson that workplaces *should* be based on mutual distrust. If employers distrust employees to some degree and assume they require some amount of monitoring, then employees should likewise distrust that employers deserve to know their personal information. If employees then know that that they are being watched due to ample notice about technology surveillance, they can accordingly structure their behavior and refrain from divulging personal information on workplace technology. Regardless, the *Ortega* framework, and its deference to employer interests in monitoring, indicates that, despite being watched, perhaps employees should trust employers anyway. While employers do conduct surveillance on workplace technology, in most cases they will not necessarily indulge in unreasonable searches, as creating an Orwellian workplace will negatively impact employee morale.[195]

If the goal is to ensure healthy workplace relationships between employers and employees, one compromise to the problem of satisfying both parties' interests and expectations could center on workplace

---

[193] *Id*.

[194] *Id*. at 1791.

[195] *See* David Smith, Case Note, *Search and Seizure*: O'Connor v. Ortega*, "He Hit Me First!,"* 56 UMKC L. REV. 411, 418–19 (1988) (noting that employers would refrain from most objectionable searches because "[a]n environment which makes an employee feel that he or she has no privacy would be counter-productive. Therefore, it stands to reason that employers only search an office on official business since ad hoc searches would destroy the healthy work environment employers strive so hard to attain.").

privacy legislation requiring disclosure. Because the current state of the law allows employers to conduct any surveillance depending on the context of the workplace, employers should place employees on meaningful notice when conducting workplace surveillance. As Quon's workplace demonstrated, sometimes a workplace context can send mixed messages, and employers should bear the responsibility of sending a clear, unmistakable signal that employees may be monitored and all employees should refrain from sending private communications on employer-provided technology. If employees are provided with such notice, then they will at least have a meaningful choice as to whether they will only use employer-provided technology for work-related purposes or whether they will risk sending personal communications on workplace laptops or BlackBerries despite the possibility of being watched by their employers.

Fairness dictates, for example, that employers who provide laptops, cell phones or BlackBerries should provide general and ongoing surveillance warnings to employees in order to constantly discourage any personal use of technology.[196] This not only reserves for the employer the right to keep track of its own technology but also puts the employee on reasonable notice as to monitoring. Collection, use, or disclosure of personal information should normally be done only with an employee's knowledge and consent, with a warning screen acknowledging surveillance every time an employee signs on to a computer or laptop.[197] Employers should give employees access to the personal information held about them, so that they can verify and, if necessary, challenge its accuracy and completeness.[198]

Employees like Quon must be provided with meaningful notice, so they have awareness that they are being watched and will therefore keep

---

[196] One commentator suggests that legislators should create laws that "provide clarity on notice and consent requirements, delineate appropriate use and lifetime of data, and afford an employee the capacity to correct false data," Laura Evans, *Monitoring Technology in the American Workplace: Would Adopting English Privacy Standards Better Balance Employee Privacy and Productivity?*, 95 CALIF. L. REV. 1115, 1144 (2007). Another commentator suggests that potential solutions include providing meaningful remedies against the misuse or abuse of electronic surveillance by employers, and additionally requiring employers to advise employees each time the employer accesses their computer system, giving written notice to employees prior to instituting a monitoring program, articulating a legitimate business reason for implementation of a policy, or only getting information on a "need to know" basis. Michael L. Rustad & Sandra R. Paulsson, *Monitoring Employee E-Mail and Internet Usage: Avoiding the Omniscient Electronic Sweatshop: Insights from Europe*, 7 U. PA. J. LAB. & EMPL. 829, 899–900 (2005).

[197] *See* 10-272 Matthew Bender & Company Inc., Labor and Employment Law § 272.06. (2008).

[198] *Id*.

personal information private. If both players know the rules of the game, and each can mutually distrust the other enough so that employers routinely conduct surveillance and employees know enough to refrain from communicating personal information on workplace technology, then employers and employees will reach an imperfect solution to the quandary of serving both their interests concerning workplace privacy.[199] On the one hand, employers will be able to continue monitoring employee productivity, efficiency and compliance. On the other, by having meaningful notice not to divulge all that juicy information about their adulterous relationships and general bad behavior on those insidious, employer-provided BlackBerries, employees will retain a Brandeis-quality sphere of privacy and autonomy in which their employers cannot intrude.

---

[199] *See* William J. Stuntz, *Implicit Bargains, Government Power, and the Fourth Amendment*, 44 STAN. L. REV. 553, 555 (1992). This proposed model, based on both sides being on the same page, for notice regarding monitoring to prevent workplace privacy violations has echoes of the Fourth Amendment theories of Professor William Stuntz, who posits that the Court's use of the "special needs" exception should be analogized to the law of contracts, indicating that an implicit bargain between government-employers and public-sector employees exists in the background of workplace searches. *Id*. at 554. Viewing the Fourth Amendment through the lens of contract law, Stuntz believes the "Court's 'special needs' decisions have it about right" because, in the context of "special needs" searches, the government and the citizen have a relationship independent of the search; the government has alternative options it could pursue if a search would violate the Fourth Amendment, such as punishment or discharge; and these searches spread benefits to innocent search targets by ferreting out wrongdoing and streamlining inefficiencies. *Id*. at 555. Basically, Stuntz believes that an implicit bargain between citizens and the government exists in the background of any search conducted in the "special needs" exceptions contexts of government workplaces, public schools and regulated businesses. *Id*. He believes this because "rational people in the position of these search targets would likely agree to such a regime," as they "get something in return: a reduced likelihood that the government will exercise other, worse alternatives." *Id*. He explains that if the government and the public-sector worker were to negotiate a rule for workplace searches in advance, this type of negotiation "would reflect the parties' understanding of the whole relationship, and their mutual awareness that the government often has alternatives to searching. *Id.*