

## Washington Journal of Law, Technology & Arts

---

Volume 5 | Issue 4

Article 5


---

3-1-2009

# Text Message Monitoring after *Quon v. Arch Wireless*: What Private Employers Need to Know about the Stored Communications Act and an Employee's Right to Privacy

Jennifer Heidt White

Follow this and additional works at: <https://digitalcommons.law.uw.edu/wjlta>

 Part of the [Communications Law Commons](#), and the [Labor and Employment Law Commons](#)

---

### Recommended Citation

Jennifer H. White, *Text Message Monitoring after Quon v. Arch Wireless: What Private Employers Need to Know about the Stored Communications Act and an Employee's Right to Privacy*, 5 SHIDLER J. L. COM. & TECH. 19 (2009).

Available at: <https://digitalcommons.law.uw.edu/wjlta/vol5/iss4/5>

This Article is brought to you for free and open access by UW Law Digital Commons. It has been accepted for inclusion in Washington Journal of Law, Technology & Arts by an authorized editor of UW Law Digital Commons. For more information, please contact [cnyberg@uw.edu](mailto:cnyberg@uw.edu).

## TEXT MESSAGE MONITORING AFTER QUON V. ARCH WIRELESS: WHAT PRIVATE EMPLOYERS NEED TO KNOW ABOUT THE STORED COMMUNICATIONS ACT AND AN EMPLOYEE'S RIGHT TO PRIVACY

Jennifer Heidt White<sup>1</sup>

©Jennifer Heidt White

### Abstract

In June 2008, the Ninth Circuit Court of Appeals held that public employees have a reasonable expectation of privacy in the content of text messages sent from employer-owned devices. The court concluded that the expectation of privacy arises vis-à-vis the text-message service provider, even where an employee has signed an explicit waiver of such an expectation. The decision, *Quon v. Arch Wireless*, raises difficult questions about the limitations placed on text-message service providers by the Stored Communications Act, and an employer's ability to regulate and monitor employee use of technology in the workplace. Although *Quon* only applies to public employers, the opinion also gives *private* employers a framework for creating technology-use policies that will protect employer access to text-message information. This Article will discuss statutory and constitutional limitations on accessing employee text messages, and what employers can do to reserve the right to review text-message communications.

### Table of Contents

[Introduction](#)

[Quon v. Arch Wireless](#)

[Text Message Monitoring Under the Stored Communications Act](#)

[Lessons for Private Employers Regarding Text-Message Service Providers and the Stored Communications Act](#)

[The Right to Privacy and Employment Privacy Waivers](#)

[Avoiding Inadvertent Waiver of Reserved Rights to Monitor Text Messages](#)

[Conclusion](#)

[Practice Pointers](#)

### INTRODUCTION

<1>Text messaging is an increasingly popular means of communication for working Americans. Eighty-nine percent of workers own a cell phone (up from 82% in 2006), and 19% own a personal digital assistant (PDA), such as a Blackberry.<sup>2</sup> Of those gadget owners, 59% use their cell phone or PDA for text messaging.<sup>3</sup>

<2>As one would expect, employers are attuned to this trend, and often include text-message services for employer-owned cell phones or PDAs.<sup>4</sup> However, employer-provided text-message services have made the drafting and enforcement of technology-use policies more complex. As the lines between private and business communication have blurred, it has become increasingly difficult for courts to determine who has the right to access text-message records, and what privacy rights should be afforded to the users of such technology.

Recently, in *Quon v. Arch Wireless*,<sup>5</sup> the Ninth Circuit held that a public employee

has a right to privacy in the content of text messages sent from an employer-owned pager vis-à-vis the text-messaging service provider, regardless of disclaimers or waivers signed by that employee.<sup>6</sup> Although the *Quon* decision involves a public employer, the court's legal reasoning offers important guidance for private employers as well, and this Article explores those lessons. First, this Article considers private employers' rights to text-message records, and how the Stored Communications Act specifically impacts those rights. This Article then outlines what private employers can do to protect themselves against state constitutional, statutory and common law claims for violations of privacy. In addition, this Article explores how private employers can avoid inadvertent waiver of reserved rights to review text-message transcripts. Finally, this Article closes with Practice Pointers to help private employers implement successful technology-use policies relating to text-message communications.

## QUON V. ARCH WIRELESS

<4>In 2001, the City of Ontario Police Department (the "Department") contracted with Arch Wireless to provide two-way alphanumeric pagers and text-message services to its officers, including Sergeant Jeff Quon.<sup>7</sup> Formally, the Department warned employees not to use the pagers for personal purposes. Furthermore, the Department required the officers to sign a waiver of their expectations of privacy in electronic communications, and notified its employees that the Department reserved the right to audit records of those communications.<sup>8</sup>

<5>Early on, when Sergeant Quon exceeded the allotted number of monthly text-message characters (presumably due to personal use), the administrator permitted Quon to pay for the excess messages in lieu of an audit. When the administrator "tired of being a bill collector," however, the Department decided to inspect Quon's text-message records to distinguish personal from professional communications.<sup>9</sup> As part of the investigation, the Department requested and received complete transcripts of Quon's text messages from Arch Wireless.<sup>10</sup> Quon brought suit against Arch Wireless for violation of the Stored Communication Act, and against the City of Ontario (the "City") for violation of the Fourth Amendment.

<6>The Ninth Circuit held that Arch Wireless had violated the Stored Communications Act (the "Act") by disclosing the contents of the text messages to the City without express consent of the addressee or intended recipient.<sup>11</sup> The *Quon* Court determined that the Act prohibited Arch Wireless from making content disclosures due to of the nature of the electronic services it rendered to the City.<sup>12</sup> The court of appeals also concluded that the City had violated Quon's Fourth Amendment right to privacy by reading the contents of his text messages, even though he had signed an express waiver of his privacy rights, and his pager was provided and owned by the City.<sup>13</sup>

<7>The *Quon* decision's relevance to private employers is not readily apparent because Sergeant Quon was a public employee; however, private employers would be wise to take heed. The Ninth Circuit's decision provides businesses with a framework for analyzing their technology-use policies, and aids in identifying appropriate measures to secure employer access to text-message information in light of constraints on third-party service providers by the Stored Communications Act. The following sections discuss these lessons and identify the ways in which employers can avoid the issues faced in *Quon*, including those arising under the Stored Communications Act.

## TEXT MESSAGE MONITORING UNDER THE STORED COMMUNICATIONS ACT

<8>Congress passed the Stored Communications Act in 1986, in part, to prevent electronic-communication service providers from disclosing the content of private communications to the government and other entities.<sup>14</sup> Through e-mail, businesses have largely been able to circumvent the Act by creating employer owned-and-operated e-mail networks, coupled with express technology-use policies. With text

messages, however, businesses typically depend on third-party cellular and text-message providers to facilitate message transmission. Because third-party providers are subject to the restrictions of the Stored Communications Act, employer access to text messages has been cabined by the statute.

<9> In relevant part, the Act distinguishes between providers that offer “electronic communication services” (ECS) and “remote computing services” (RCS). An ECS provider facilitates communication between a sender and receiver, and the Act prohibits the provider from “knowingly divulging . . . the contents of [that] communication” to any person except the addressee or intended recipient of the message without express consent of either party.<sup>16</sup> In contrast, RCS providers offer “computer storage or processing services by means of an electronic-communication system,” and may disclose communication to the “subscriber” as well as the addressee or intended recipient.<sup>17</sup> The legislative history clarifies that Congress intended the distinction to reflect the difference between providers that help parties send and receive messages, such as e-mail or telephone calls (i.e., ECS providers), and those providers who offer “offsite data banks” and “data processing services” (i.e., RCS providers).<sup>18</sup>

<10> In *Quon*, the Ninth Circuit determined that Arch Wireless was an ECS provider because it served as a mere “conduit for the transmission of electronic communications from one user to another, and stored those communications ‘as a backup for the user.’”<sup>19</sup> The “backup purposes” of Arch Wireless’ actions were in contrast to the “virtual filing cabinet” function of an RCS provider.<sup>20</sup> As such, when Arch Wireless disclosed Quon’s messages to the City-subscriber, it violated Stored Communications Act’s restrictions on ECS access.

<11> The Ninth Circuit, however, is not the only court to consider the distinction between ECS and RCS providers in the context of text message communications. One other court—the District Court for the Eastern District of Michigan—considered the service providers’ respective limitations under the Stored Communications Act post-*Quon*, and expressly rejected the Ninth Circuit’s interpretation. In *Flagg v. City of Detroit*, the district court considered the effect of the Stored Communications Act on text messages obtained through discovery in a civil case.<sup>21</sup> The court emphasized that the provider could fit both, or either, definition of a service provider under the statute because a text-message service provider facilitates communication between the sender and recipient, *and* usually offers some degree of temporary or permanent storage of the message incident to transmission.<sup>22</sup> The district court concluded that the service provider was acting as a RCS under the specific facts of the case because the text was the “only available record of the[] communications,” and, thus, was intended to provide permanent, rather than “back-up,” storage.<sup>23</sup> In so doing, the *Flagg* Court explicitly adopted the reasoning of the district court in *Quon* and, thereby, permitted the employer-subscriber access to the text message transcripts. <sup>24</sup>

#### Lessons for Private Employers Regarding Text-Message Service Providers and the Stored Communications Act

<12> Given the divergent conclusions found in *Quon* and *Flagg* on this issue, in addition to the arguably outdated statute, private employers should be prepared for uncertainty as to the classification of modern service providers under the Stored Communications Act.<sup>25</sup> To protect employer access to employee text messages, private employers should take certain preventative actions. First, private employers may want to contract for specific communication services, whether ECS, RCS, or both. An employer may be able to clarify its intent for a court by documenting *specific* contract provisions about how and what records are to be kept, and by informing employees about the relevant provisions of that contract.

<13> For example, in defining Arch Wireless’ activities, the court in *Quon* found

persuasive the absence of any "indication in the record that Arch Wireless retained a permanent copy of the text messages or stored them for the benefit of the City."<sup>26</sup> Without evidence to the contrary, the court assumed that the nature of the services provided would result in a temporary back-up—rather than permanent—copy.<sup>27</sup> Similarly, the district court in *Flagg* suggested that an employer's contract with its service provider *may* establish "control" over those messages.<sup>28</sup> Thus, more specific contract provisions or "control" over the messages, especially in the area of text-message storage, are recommended even given the divergent precedent.<sup>29</sup>

<14>In addition, the *Flagg* Court also suggested that businesses may be able to avoid the Stored Communications Act altogether by contracting for the retrieval of "text messages from an archive maintained at the behest of th[e] customer."<sup>30</sup> The court suggested that "to the extent that the contracts between the City and [the service provider] provide a mechanism for the City to request the retrieval of text messages from the archive maintained by [the service provider]," such a contract would be for services entirely outside the scope of the Stored Communications Act. For example, if such a contract were in place, the service provider would be "fulfilling a request from its customer, the City, to retrieve and forward communications from an archive . . . maintained at the customer's request, [and the service provider] cannot necessarily be characterized as having 'divulged' any information to anyone outside the scope of the confidential relationship . . . ." <sup>31</sup> Although this untested suggestion may not evade the Stored Communications Act, clear intent may help a court determine what type of relationship is at issue. As a result, the court may be less likely to define a text-message service provider as an ECS, which would require employee consent for access to records of text communications.

<15>Furthermore, companies should limit inquiries to transactional information, such as the "To" and "From" information, specific pin registers, or e-mail addresses, to avoid the "actual" content of text communications.<sup>32</sup> In so doing, employers may be able to properly regulate employee conduct by monitoring the parties to whom the messages are sent, rather than the content of the messages themselves. Indeed, the Stored Communications Act only limits access to the "contents" of the transmissions—defined as "any information concerning the substance, purport, or meaning of [the] communication . . . ." <sup>33</sup> regardless of how a court chooses to define the service provider.<sup>34</sup> Accordingly, service providers should be able to access and disclose basic transactional information about the text *without* consent of the originator, addressee or subscriber. Thus, by limiting the scope of their investigation, employers may be able to receive the information needed to assess the general propriety of text communications.

## THE RIGHT TO PRIVACY AND EMPLOYMENT PRIVACY WAIVERS

<16>In addition to asserting claims under the Stored Communications Act, Sergeant Quon also asserted two constitutional claims. Specifically, he contended that his government employer had violated his Fourth Amendment right to privacy, under both the United States Constitution and California state constitution, by accessing the content of his text messages without his permission.<sup>35</sup> The Ninth Circuit agreed, finding that Quon had a reasonable expectation of privacy in the content of his messages given the Department's informal policy of allowing personal text messaging as long as the employee paid for any overage.<sup>36</sup> The court also determined that the search was unreasonable in scope because the Department did not need to review the content of the messages "to verify the efficacy of the 25,000 character limit."<sup>37</sup>

<17>Although private employers are not subject to the same Fourth Amendment constraints at issue in *Quon*,<sup>38</sup> many states still protect private employees' rights to privacy. While California is the only state that extends a state constitutional right of privacy to all people, including private-sector employees,<sup>39</sup> nearly every state

provides for such privacy rights through statutes that often track the language of the Stored Communications Act or Federal Wiretap Act.<sup>40</sup> Moreover, even if a state's constitution or statutes fail to protect a private employee's right to privacy, common law may also provide redress for the violation of that right. Such common law protections include, but are not limited to, state law tort claims for intentional or negligent infliction of emotional distress, false light, and improper or unreasonable disclosure of private facts.<sup>41</sup> Employers should pay close attention to the state-specific constitutional, statutory and common law claims available to its employees, as such laws may open the door to claims against the employer for privacy violations.

#### Avoiding Inadvertent Waiver of Reserved Rights to Monitor Text Messages

<18> Given the pitfalls of state privacy protection, private employers must also avoid inadvertent waiver of the right to monitor an employee's text messages. The Ninth Circuit recognized Sergeant Quon's reasonable expectation of privacy in the content of his text messages and disregarded the signed employment privacy waiver because the Department had not acted in accordance with its own policy.<sup>42</sup> Indeed, even though the Department reserved the right to monitor all electronic communications and, by signature, Quon explicitly relinquished his expectation of privacy, the court found that his actual experience at work *increased* his expectation of privacy.<sup>43</sup> The "operational reality" of the workplace led employees to believe that if they paid their overages, their text messages would not be audited—a reasonable expectation that destroyed the effect of any notice to the contrary.<sup>44</sup>

<19> Similar precedent makes clear that an "operational reality" can either enhance or diminish the reasonableness of an employee's expectation of privacy.<sup>45</sup> In general, courts start at the plain language of the policy, but rarely end there.<sup>46</sup> Rather, many courts take a "policy-plus" approach by looking to the text of the policy itself, in addition to the relevant actions of both the employer and employees.<sup>47</sup> Rarely will a simple reservation of the right-to-review enough for employers survive this analysis; employers must also practice the procedures set forth in its technology-use policy. If an employer fails to do so, this inaction is likely to waive the employer's explicitly reserved rights, and negate an employee's consent to the terms of the technology policy.

<20> Similar to the Ninth Circuit's decision in *Quon*, the Second Circuit in *Leventhal v. Knapek* for example, found that the government agency's mere "anti-theft" policy was insufficient to prohibit an employee from storing any personal items on his office computer because the terms of the policy were vague.<sup>48</sup> Moreover, the *Leventhal* Court emphasized that the agency's access to employee offices and computers for maintenance did not overcome the defendant's expectation of privacy in the contents of his computer where there was "no evidence that the[] searches were frequent, widespread, or extensive enough to constitute an atmosphere 'so open to fellow employees or the public that no expectation of privacy [wa]s reasonable.'"<sup>49</sup> Accordingly, the infrequency and inconsistency of the searches enhanced the defendant's expectation of privacy, and weakened the potency of the agency's policy.

<21> Employers should, in light the "policy-plus" approach, ensure that their policies are clear and specific both to the type of technology, as well as to the procedures used to track that technology. Furthermore, employers must explain their policies to their employees, and update their employees if the policies' terms change. Most importantly, employers must also actually enforce the rules or review processes set forth in the policies. Indeed, promises without follow-through will prove problematic in litigation. Thus, as *Quon* and others illustrate, "operational reality" has the chance to be the greatest help or harm to any employer's case.<sup>50</sup>

<22>Text messaging is changing the face, or at least the format, of workplace communication.<sup>51</sup> Washington Journal of Law, Technology & Arts, Vol. 5, Iss. 4 [2009], Art. 5

By understanding the laws that affect third-party service providers and the nature of an employee's potential privacy rights, private employers should be able to put new technology to use without placing business at risk. As such, private employers should be prepared to respond to the popularity of text messaging in the workplace with appropriate measures to protect their interests in employee monitoring. In this context, *Quon* provides important guidance and reminders.

<23>Specifically, employers should pay close attention to the type of text-message services provided in their contracts with third-party service providers. In addition, since case law is still developing in this area, it may be advantageous for employers to follow the *Flagg* Court's suggestion of contracting around the Stored Communications Act; however, the viability of this approach remains untested. Furthermore, *Quon* reminds us that privacy protection is not limited to government employees, and that it is important to practice what is preached. Employers must, therefore, make technology policies specific and up-to-date, and enforce those policies with care to avoid the "operational reality" penalty. Ultimately, attention to these lessons will help private employers guard against the problems addressed in *Quon*.

## PRACTICE POINTERS

- Carefully contract for specific communication services with the third-party service provider.
- Review relevant state and common law protections of privacy rights for private employees.
- Audit text-message communications regularly, and limit the scope of the audit to transactional information rather than content.
- Develop and update clear technology-use policies with specific provisions regarding text messaging. Regularly inform employees of any amendments to these policies.
- Once a technology-use policy is put into practice, take measures to carry out and enforce the policy.

[<< Top](#)

## Footnotes

1. Jennifer Heidt White, University of Washington School of Law, J.D. program Class of 2010. Thank you to Professors Jane K. Winn and Peter Winn of the University of Washington School of Law, Editor-in-Chief Alexander Casey, and Articles Editors C. Christine Porter and Nicole J. Lindquist for their valuable advice.
2. MARY MADDEN & SYDNEY JONES, PEW RESEARCH CTR.'S INTERNET & AM. LIFE PROJECT, NETWORKED WORKERS 17 (2008), [http://www.pewinternet.org/~media/Files/Reports/2008/PIP\\_Networked\\_Workers\\_FINAL.pdf](http://www.pewinternet.org/~media/Files/Reports/2008/PIP_Networked_Workers_FINAL.pdf).
3. *Id.* at 22.
4. See generally Symposium, *The Electronic Workforce*, 12 EMP. RTS. & EMP. POL'Y J. 1 (2008) (discussing technology in the workplace).
5. *Quon v. Arch Wireless Operating Co., Inc.*, 529 F.3d 892 (9th Cir. 2008), cert. granted sub nom. *City of Ontario v. Quon*, No. 08-1332, 2009 WL 1146443 (Dec. 14, 2009) (considering the Ninth Circuit's conclusions regarding the officers' expectations of privacy). In addition, the court also

denied certiorari as to Arch Wireless' petition for review of the Ninth Circuit's *White, Pettit, Monaghan and Application of the Stored Communications Act*; Arch Wireless became USA Mobility Wireless, Inc. after the company's merger with Metrocall, Inc. *Quon v. Arch Wireless Operating Co., Inc.*, 529 F.3d 892 (9th Cir. 2008), *cert. denied sub nom. USA Mobility Wireless, Inc. v. Quon*, No. 08-1472, 2009 WL 1513112 (Dec. 14, 2009).

6. *Quon*, 529 F.3d at 903-904.
7. *Id.* at 895-96 (discussing how the text services operated in this instance). See generally USAMobility.com Products, [http://www.usamobility.com/products/messaging/2\\_way.html](http://www.usamobility.com/products/messaging/2_way.html) (last visited Jan. 3, 2010) (providing examples of two-way text message devices available to government agencies).
8. *Quon*, 529 F.3d at 896. The Department required employees to sign a general "Computer Usage, Internet and E-mail Policy," which indicated that "users should have no expectation of privacy or confidentiality when using th[o]se resources" and that "all network activity" could be "audited . . . with or without notice." *Id.* After receipt of the pagers, Quon and other employees were orally informed that pager messages were subject to the same policy. *Id.*
9. *Id.* at 897-98.
10. *Id.* at 898.
11. *Id.* at 903.
12. *Id.* at 900-901.
13. *Id.* at 904.
14. Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended at 18 U.S.C. §§ 2701-2711 (2006)). Primarily, the Stored Communications Act regulates the circumstances under which the government may require or request disclosure of the contents of a communication. See 18 U.S.C.A § 2703 (West 2009) (explaining the required disclosures of customer communications or records); see also 18 U.S.C § 2704 (2006) (describing government access to backup records); see also 18 U.S.C § 2705 (2006) (setting forth the option of delayed notice); see also 18 U.S.C § 2706 (2006) (providing for reimbursement for assembly of the communications); see also 18 U.S.C § 2707 (2006) (providing for civil action and relief). The Act also prohibits and provides punishment for hacking (unlawful and/or intentionally excessive access to an electronic communication service facility). 18 U.S.C. § 2701 (2006). See generally Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208 (2004); see also JANE K. WINN & BENJAMIN WRIGHT, *THE LAW OF ELECTRONIC COMMERCE* § 21 (4th ed. 2001 & Supp. 2008); see also RAYMOND T. NIMMER, *THE LAW OF COMPUTER TECHNOLOGY* § 16:32 (3d ed. 2006 & Supp. 2008).
15. See generally Kerr, *supra* note 14, at 1226-27 (explaining that the Stored Communications Act's voluntary disclosure limitations only apply to public service providers, like "America Online or Comcast," but not to non-public service providers, like "a company [that] provides corporate accounts to its employees"); see also CHRISTOPHER WOLF, *PROSKAUER ON PRIVACY: A GUIDE TO PRIVACY AND DATA SECURITY LAW IN THE INFORMATION AGE* § 6:3.2[A] (2d ed. 2008) (explaining that employers that act as service providers are not subject to the requirements of the Stored Communications Act).
16. 18 U.S.C.A. § 2702(a)(1), (b)(1) (West 2008).

17. 18 U.S.C.A. § 2711(2) (West 2008 & Supp. 2009). See 18 U.S.C.A. §



2702(a)(2), (b)(3) (West 2008).

- Washington Journal of Law, Technology & Arts*, Vol. 5, Iss. 4 [2009], Art. 5
18. S. REP. NO. 99-541, at 3 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3357. See generally Kerr, *supra* note 14, at 1213-14.
  19. *Quon*, 529 F.3d at 902 (quoting *Theofel v. Farey-Jones*, 359 F.3d 1066, 1075 (9th Cir. 2004)).
  20. Cf. *Theofel*, 359 F.3d at 1072-76 (finding provider to be an ECS provider of e-mail services when the provider retained e-mails on its server for back-up protection).
  21. *Flagg v. City of Detroit*, 252 F.R.D. 346 (E.D. Mich. 2008).
  22. *Id.* at 362.
  23. *Id.* at 362-63.
  24. *Id.* See *Quon v. Arch Wireless*, 445 F.Supp.2d 1116, 1137 (C.D. Cal. 2006) (calling Arch Wireless an RCS provider because the action was "retrieval of the contents of those text messages kept in long-term storage on its computer network after they had been received" (original emphasis)), *rev'd*, 529 F.3d 892 (9th Cir. 2008).
  25. See *Quon*, 445 F.Supp.2d at 1132 ("It is . . . obvious . . . that Congress had no conception of the type of communication/storage system at issue in this case when it drafted the statute.").
  26. *Quon*, 529 F.3d at 902-903.
  27. *Id.*
  28. *Flagg*, 252 F.R.D. at 354 (emphasizing that the "specific nature and extent of the services provided by [the service provider] to the City during the course of their contractual relationship" is unclear, and, therefore, "impossible to make any definitive pronouncement about the degree of control granted to the City under its agreement with [the service provider].").
  29. *Id.* at 355.
  30. *Id.* at 359.
  31. *Id.* at 358.
  32. See generally Kerr, *supra* note 14, at 1214-16; see also WOLF, *supra* note 15, at § 6:3.2[A].
  33. 18 U.S.C. § 2510(8) (2006).
  34. See, e.g., *Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107 (3d Cir. 2003) (concluding that the employer's search of an employee's e-mail was appropriate since the information was stored on a system was administered by the employer as the service provider).
  35. *Quon*, 529 F.3d at 903-906.
  36. *Id.* at 907.
  37. *Id.* at 908-909.
  38. S. Elizabeth Wilborn, *Revisiting the Public/Private Distinction: Employee Monitoring in the Workplace*, 32 GA. L. REV. 825, 828 (1998) ("Because constitutional rights operate primarily to protect citizens from the government, 'state action' is required before a citizen can invoke a constitutional right. . . . Private-sector employees . . . do not enjoy the same level of privacy protection [as public-sector employees] because employer action rarely constitutes state action."). See generally Robin

Miller, *Expectation of Privacy in Text Transmissions to or from Pager, Cellular Telephone, or Other Wireless Personal Communication Device*, 25 A.L.R. 6th 201 (2007) (collecting cases); see also Erwin Chemerinsky, *Rethinking State Action*, 80 NW. U. L. Rev. 503, 517-19 (1985) (discussing the public/private distinction).

39. Hill v. Nat'l Collegiate Athletic Ass'n, 865 P.2d 633 (Cal. 1994) (concluding that the "Privacy Initiative" referendum, which was absorbed into the first article of the California constitution, created a right of action against private parties as well as government actors for violation of privacy). See Cal. Penal Code §§ 630-637.9 (West 2009). See generally William R. Corbett, *The Need for a Revitalized Common Law of the Workplace*, 69 BROOK. L. REV. 91, 108-109 (2003).
40. See Richard E. Kaye, *Cause of Action to Recover Damages for Invasion of Privacy of Private Sector Employees' Privacy by Intrusion upon Seclusion*, in 42 CAUSES OF ACTION 2D 255, § 46 (2009) (collecting statutes).
41. See *id.* § 2 (discussing state tort law claims). See generally Kevin J. Baum, Comment, *E-Mail in the Workplace and the Right of Privacy*, 42 VILL. L. REV. 1011 (1997); see also L. Camille Hébert, *Electronic Monitoring and Surveillance as Invasion of Privacy*, in 1 EMPL. PRIVACY LAW § 8A:31 (2009); see also L. Camille Hébert, *Employer Searches as Invasion of Privacy*, in 1 EMPL. PRIVACY LAW § 8:13 (2009).
42. *Quon*, 529 F.3d at 904-906.
43. *Id.* at 906-907.
44. *Id.*
45. See *O'Connor v. Ortega*, 480 U.S. 709, 717 (1987) (concluding that the "operational reality" of a public-employer workplace can make an expectation of privacy unreasonable); see also *Muick v. Glenayre Elec.*, 280 F.3d 741 (7th Cir. 2002) (determining that conditioned use of private-employer property destroyed any reasonable expectation of privacy in the employer-issued laptop, and that the employer's reservation of the right to inspect was prudent).
46. See *United States v. Thorn*, 375 F.3d 679 (8th Cir. 2004) (concluding that there was no reasonable expectation of privacy where government employee signed policy expressly forbidding personal use and employer reserved the right to randomly audit), *vacated on other grounds*, 543 U.S. 1112 (2005); see also *Adams v. City of Battle Creek*, 15 IER Cases 254 (W.D. Mich. 1999) (finding pager technology intended to be included as part of electronics-use policy and that pervasive personal use of pagers in violation of that policy did not justify perception of privacy), *aff'd in part, rev'd in part*, 250 F.3d 980 (6th Cir. 2001) (not reaching Fourth Amendment claim); *TBG Ins. Servs. Corp. v. Superior Ct.*, 96 Cal. App. 4th 443 (Cal. Ct. App. 2002) (finding that signed computer-use policy offered notice that eliminated the employee's reasonable expectation of privacy under state constitutional privacy claim).
47. Compare *United States v. Angevine*, 281 F.3d 1130 (10th Cir. 2002) (concluding no reasonable expectation of privacy in data downloaded to state university computers, when university had a policy that reserved the right to audit Internet use and defendant did not take actions consistent with the desire to maintain privacy) and *United States v. Simons*, 206 F.3d 392 (4th Cir. 2000) (determining no reasonable expectation of privacy in files downloaded from Internet by government employee when policy limited use to official government business, permitted random audits, and the employer had reason for suspecting misconduct as impetus for search) with *United States v. Slanina*, 283 F.3d 670 (5th Cir. 2002),

*vacated*, 537 U.S. 802 (2002) (determining legitimate expectation of privacy where policy was not disseminated to employees and documents on the computer were password-protected), and *Leventhal v. Knapek*, 266 F.3d 64 (2d Cir. 2001) (concluding legitimate expectation of privacy where there was a lack of a clear and consistently enforced policy, though ultimately finding scope of search properly limited).

48. *Leventhal*, 266 F.3d at 74 (citing *O'Connor v. Ortega*, 480 U.S. 709, 718 (1987)).
49. *Id.*
50. See generally Nicole J. Nyman, Comment, *Risky Business: What Must Employers Do to Shield Against Liability for Employee Wrongdoings in the Internet Age?*, 1 SHIDLER J. L. COM. & TECH. 7 (2005), available at <http://www.lctjournal.washington.edu/Vol1/a007Nyman.html>.
51. See Symposium, *supra* note 4; see also Katie Fretland, *U.K. Store Worker Fired by Text Message*, USA TODAY, Aug. 7, 2006, [http://www.usatoday.com/tech/news/2006-08-07-text-message-fired\\_x.htm](http://www.usatoday.com/tech/news/2006-08-07-text-message-fired_x.htm); see also Amy Joyce, *Fired via Email, And Other Tales of Poor Exits*, WASH. POST, Sept. 10, 2006, at F01, available at <http://www.washingtonpost.com/wp-dyn/content/article/2006/09/09/AR2006090900103.html>.