Westlaw Journal
COMPUTER & INTERNET
Litigation News and Analysis • Legislation • Regulation • Expert Commentary
VOLUME 33, ISSUE 23 / APRIL 22, 2016

EXPERT ANALYSIS

Reasonable Expectations of Privacy in a Not-So-Private Electronic World

By Jay Shapiro, Esq.
White and Williams

In this time of ubiquitous electronic communication, the boundaries of privacy rights in the workplace have become a moving target. Important issues have arisen concerning an employee's right to privacy in those communications when they occur in and around the workplace.

Searches of a public employee's workspace by an employer are governed by the Fourth Amendment's "reasonable expectation of privacy" standard along with a balancing of the need for the search and the reasonableness of the search itself.

This principle was reiterated in the U.S. Supreme Court's ruling in *City of Ontario v. Quon*, 560 U.S. 746 (2010), which addressed the legality of a public employer's review of an employee's text messages that were sent to and from his mobile pager.

Jeff Quon was a police sergeant in Ontario, California. In 2001 the department supplied Quon and others with pagers that could be used to send and receive text messages. The use was constrained by Ontario's "computer usage, internet and email policy." The policy gave the city "the right to monitor and log all network activity including email and Internet use, with or without notice." It also said "users should have no expectation of privacy or confidentiality when using these resources."

Quon agreed to the policy in writing, but his use exceeded what was anticipated by the department when it entered into its agreements with its cellular carrier. At first, the city told him that he was exceeding his monthly budget of messages and allowed him to pay for the excess usage. But after his excessive usage continued, the police department asked the wireless carrier for transcripts of his text messages over a two-month period.

The transcripts revealed many personal messages, including some that were sexually explicit. Quon's activities were referred to the department's internal affairs division, and he was disciplined.

Quon and three other employees who had been communicating with him sued the city, the department, the chief and the city's wireless provider. They alleged violations of their civil rights as well as federal and state laws protecting the privacy of electronic communications, including the federal Stored Communications Act, 18 U.S.C.A. § 2702(a)(1).

A jury found that the defendants did not violate the Fourth Amendment. The 9th U.S. Circuit Court of Appeals reversed, finding that Quon had a reasonable expectation of privacy in the communications and the search was not reasonable because the city could have utilized less intrusive means to conduct its investigation.

The Supreme Court acknowledged that "[i]ndividuals do not lose Fourth Amendment rights merely because they work for the government instead of a private employer," citing *O'Connor v. Ortega*, 480 U.S. 709, 717 (1987) (plurality opinion). But it also found "reasonable grounds" for supporting the search, which it said was performed "for a noninvestigatory work-related purpose."

The Supreme Court has acknowledged that the nature of the data kept on and accessible through cellphones has significant implications for privacy

The Supreme Court determined that there was no Fourth Amendment violation because the search of the text messages was reasonable. To support this conclusion, it found that the city had a "legitimate work-related rationale" and noted that the department limited its review to transcripts of messages outside of work hours over a period of just two months.

Justice Anthony Kennedy recognized the high court's precedents in the context of workplace searches of public employees when he wrote: "The Court must proceed with care when considering the whole concept of privacy expectations in communications made on electronic equipment owned by a government employer. The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear."

In a concurrence, Justice Antonin Scalia chose to bring private employee rights into the discussion. Justice Scalia said "the proper threshold inquiry should be not whether the Fourth Amendment applies to messages on public employees' employer-issued pagers, but whether it applies in general to such messages on employer-issued pagers."

How does the ruling apply in the private workplace?

Unless an employer is acting as an agent of law enforcement, the Fourth Amendment is not applicable to employee searches. Instead, an employee's reasonable expectation of privacy is generally circumscribed by employer policies and not the Constitution. However, some courts addressing searches involving nonpublic employees have demonstrated a willingness to apply Fourth Amendment precedent as it was used in fashioning the court's analysis in *Quon*.

Courts frequently use the framework set forth in *In re Asia Global Crossing Ltd.,* 322 B.R. 247, 256 (Bankr. S.D.N.Y. 2005). In general, that decision said courts should consider four questions:

- Does the corporation maintain a policy banning personal or other objectionable use?
- Does the company monitor the use of the employee's computer or email?
- Do third parties have a right of access to the computer or emails?
- Did the corporation notify the employee, or was the employee aware, of the use and monitoring policies?

The *Asia Global* decision drew from the 7th U.S. Circuit Court of Appeals' ruling in *Muick v. Glenayre Electronics,* 280 F.3d 741 (7th Cir. 2002). In *Muick* the court wrote that the employee "had no right of privacy in the computer" provided by his employer "for use in the workplace." Interestingly, although *Muick* considered the concept of right of privacy, it did not dress it in reasonableness.

Rather, the court maintained that because the laptops in question were the employer's property, "it could attach whatever conditions to their use it wanted to. They didn't have to be reasonable conditions; but the abuse of access to workplace computers is so common ... that reserving a right of inspection is so far from being unreasonable that the failure to do so might well be thought irresponsible."

Clearly, then, in the context of devices provided by employers, businesses commonly issue policies that announce the absence of privacy protections. For example, the following policy was found in *Mintz v. Mark Bartelstein & Associates,* 885 F. Supp. 2d 987 (C.D. Cal. 2012), to clearly provide notice that employees had only a limited expectation of privacy:

> The personal use of [the employer's] equipment or property should be kept to an absolute minimum. ... Any personal or other information placed on [the employer's] email, voice mail, telephones, blackberries, or any computer system shall be the property of [the employer], and shall not be considered the private or confidential property of the employee. Indeed, [the employer] has the ability and right to review email, voice mail, and telephone messages.

There are other considerations relevant to the analysis. In particular, beyond the policies and procedures that are established in the workplace, it is important to add personal behaviors to the equation. Courts examine whether an employee claiming a privacy right to electronically stored communications has, by his conduct, undercut that assertion.

The concept of expectation of privacy has changed drastically since the Supreme Court wrote that a person who enters a telephone booth, "shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world." *Katz v. United States,* 389 U.S. 347 (1967).

Phone booths are largely relics of the past; we have now moved to the point where a federal appeals court has determined that a civil litigant had no expectation of privacy in a call that was inadvertently "butt-dialed." *Huff v. Spaw,* 794 F.3d 543 (6th Cir. 2015).

Certainly, mobile devices offer features that support greater privacy rights. The Supreme Court's decision in *Riley v. California,* 134 S. Ct. 2473 (2014), revealed its recognition of the vast breadth of data that may be accessed by a cellphone. The high court wrote that cellphones "are in fact microcomputers" that "could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps or newspapers."

The *Riley* court acknowledged that the nature of the data kept on and accessible through cellphones has significant implications for privacy. The court determined that the "search incident to arrest" doctrine, which provides an exception to the Fourth Amendment's warrant requirement, could not justify warrantless searches of cellphones absent exigent circumstances.

But *Riley,* decided under Fourth Amendment principles, analyzed the cellphone searches in criminal cases, with the attendant constitutional protections. The import of those concerns, save for analogizing the expectation of privacy, fade in the context of private employment.

In this arena, the question of whose device is it anyway is significant.

In *Mintz*, an employer argued that its former employee did not have any expectation of privacy in his cellphone because the employer paid the phone bills and its employee manual said the employer had "the right to review all email, voice mail and telephone messages." However, the question of ownership was not clear because the employee paid some of the phone fees and had used the cellphone number prior to his employment.

In *Riley,* the court turned its attention to the significant complication presented by cloud computing, which it described as "the capacity of Internet-connected devices to display data stored on remote servers rather on the device itself." When searches involving computers were isolated to hard drives, courts were comfortable applying the analogy of a file cabinet to document storage on a computer. *Trulock v. Freeh,* 275 F.3d 391 (4th Cir. 2001).

The Supreme Court in *Riley* pointed out that "officers searching a phone's data would not typically know whether the information they are viewing was stored locally at the time of the arrest or has been pulled from the cloud."

The critical point — that the device itself is no longer necessarily the focus of the expectation of privacy — can most certainly have implications in the private workplace.

A recent case that highlights these issues created by these technological developments is *Sunbelt Rentals Inc. v. Victor,* 43 F. Supp. 3d 1026 (N.D. Cal. 2014). Sunbelt employed Santiago Victor as a salesman. It provided him with a corporate iPhone and iPad for work and personal use. Not surprisingly, Victor created — at his own expense — an Apple account that was accessible and used on both devices. Victor returned the devices when he left Sunbelt to join a competitor. The new employer gave Victor a new iPad, and when he registered it he discovered that his Sunbelt phone was still linked to his account.

Sunbelt sued Victor, claiming that he stole trade secrets from it. Victor filed counterclaims against Sunbelt, charging that it had accessed his private communications, including those in the cloud, through his old device. Although the counterclaims were dismissed because Victor failed

The role of Fourth Amendment jurisprudence discussing reasonable expectation of privacy in electronic devices has become common in court decisions in the civil context.

to set forth factual allegations to support them, the potential for the loss of private information described in this case raises significant concerns.

Simply put, employees must be concerned about more than just the device because the accessible information and data will be the focus of any inquiry. The court in *Victor* specifically rejected the contention that in *Quon* the Supreme Court held an employee had a reasonable expectation of privacy in text messages sent on the employer-owned device.

The role of Fourth Amendment jurisprudence discussing reasonable expectation of privacy in electronic devices has become common in court decisions in the civil context. One of the key concepts is that a person who is aware of the potential to expose communications through an electronic device and intentionally or negligently disregards that risk undercuts his ability to assert a reasonable expectation of privacy.

For example, in *Huff*, the butt-dial case, the plaintiff acknowledged that he was aware of the possibility of accidental pocket-dialed calls and had, in fact, made calls inadvertently. The 6th U.S. Circuit Court of Appeals noted that the plaintiff could have locked his phone, set up a passcode or even downloaded an app that would have stopped such a call from occurring. Because the plaintiff did not take any of these steps, the court found he did not establish a reasonable expectation of privacy.

Huff demonstrates the potentially high stakes in this new area of electronic privacy. James H. Huff had been the chair of Kentucky's Kenton County Airport Board, which controls the Cincinnati/Northern Kentucky International Airport. His pocket-dial from a hotel balcony in Italy to the phone of an executive assistant who worked for him resulted in the overhearing of 90 minutes of conversation, including substantial discussions about sensitive personnel matters.

As methods of communication and data transfer continue to develop, more and more doors will open. Courts will be required to evaluate expectations of privacy, their reasonableness, and the intentional, reckless or negligent exposure of communications and information.

There is no single corporate policy approach that fits all. Businesses must carefully assess their particular operations to keep up with the times, technology and the law. WJ

Jay Shapiro co-chairs the cyberlaw and data protection practice of **White and Williams** in New York. A white-collar prosecutor for two decades, Shapiro was one of the first participants in the federal Electronic Crimes Task Force, which launched some of the earliest investigations into cybercrimes.