Bloomberg Law Reports® Privacy & Information

Privacy of Email and Text Messages – Case Law Sprinting to Catch Up to Modern Technology

Robert D. Brownstone, Sheeva J. Ghassemi-Vanni, and Soo Cho, Fenwick & West LLP

Perhaps in an effort to sync up with technological mores, over the past year courts have been taking unprecedented stances that limit an individual's right to privacy in the workplace and elsewhere. This trend begs the question, what is the current state of privacy law, especially as to e-mail and text messages? This piece analyzes the most important decisions in this burgeoning area of the law, and the resultant lessons we can draw. Although many of the recent privacy cases involve a failed argument under the Fourth Amendment–inherently predicated on state or governmental action–some state constitutions, including the California constitution, contain similar protections that employees sometimes attempt to invoke as applicable to private organizations.

Is There a General Right to Privacy in E-mail?

Recently, the Eleventh Circuit attempted to deal with the question of whether individuals have a privacy right in e-mail–an issue the U.S. Supreme Court has yet to unambiguously address. The court ultimately declined to establish a definitive precedent, preferring to leave the question open for future decision.

In *Rehberg v. Paulk*,[1] an individual named Charles Rehberg sent anonymous faxes to administrators of a public hospital, criticizing their management and activities. Kenneth Hodges, then the District Attorney, and James Paulk, Chief Investigator at the District Attorney's office, investigated Rehberg's actions as a favor to the hospital. During the investigation, Paulk issued a subpoena to an Internet service provider ("ISP") for one of Rehberg's personal e-mail accounts, and obtained e-mails sent and received from Rehberg's personal computer. As a result of Hodges and Paulk's investigation, Rehberg was indicted on multiple counts of assault and harassment. Eventually, all the charges were ordered dismissed. Rehberg filed suit against Hodges and Paulk alleging that they invaded his privacy by illegally issuing the subpoena to his ISP. Rehberg claimed the subpoena violated his Fourth Amendment right to be free from unreasonable search and seizure.

Rather than decide whether Rehberg had a reasonable privacy expectation in the contents of his personal e-mails sent voluntarily through a third-party ISP, the court decided to resolve the case narrowly and leave the privacy issue for another day. Qualified immunity shields government officials who perform discretionary governmental functions from civil liability, so long as their conduct does not violate any clearly established constitutional rights. As no precedent had existed defining the bounds of privacy in e-mail, no clearly established constitutional right to privacy existed at the time Paulk is-

sued the subpoenas. The court thus declined to rule on the greater question of e-mail privacy and instead choose to grant Paulk qualified immunity on Rehberg's e-mail subpoena claim.

Unlike *Rehberg*, in the technologically groundbreaking decision of *United States v. Warshak*,[2] the Sixth Circuit dared to take a stance regarding the reasonable expectation of privacy in, and Fourth Amendment implications of, warrantless searches of e-mail. The criminal defendants in *Warshak* operated a company that distributed "nutraceuticals," including the male enhancement herbal supplement Enzyte. Defendants were the subject of a criminal indictment containing 112 counts, chief among them money laundering and fraud.

Prior to a jury trial, defendants moved to exclude approximately 27,000 incriminating e-mails, which the government had obtained by requesting prospective preservation of, and later subpoenaing, e-mail records from defendants' ISP. The government did not obtain a warrant for the e-mails, relying on the Stored Communications Act's provision permitting a "governmental entity" to require a service provider to disclose the contents of electronic communications under certain circumstances.

Ultimately, the Sixth Circuit considered whether Warshak had an expectation of privacy in his e-mails. The court held: "a subscriber enjoys a reasonable expectation of privacy in the contents of emails"[3] sent through an ISP such that the government violates the Fourth Amendment by failing to obtain a warrant in advance of compelling the ISP to relinquish such e-mail records. But the court left open the possibility that an ISP's terms or conditions could alter such reasonable expectation of privacy by indicating an intention to "audit, inspect, and monitor" subscriber e-mail.[4] Further, the court held that the Stored Communications Act is unconstitutional to the extent it permits the government to obtain e-mails absent a warrant. However, the circuit court did not apply the exclusionary rule, and affirmed the trial court's admission into evidence of the 27,000 e-mails. The Sixth Circuit's rationale was that the government had relied in good faith on the Stored Communications Act to obtain the e-mails.

Throughout the *Warshak* opinion, the court emphasized the importance of e-mail in daily communication, the highly personal nature of e-mail, and the elevated level of protection e-mail should be afforded. The court noted that e-mail: "is the technological scion of tangible mail, and it plays an indispensable part in the Information Age," and indicated that e-mail should be provided the same level of Fourth Amendment protection as letters and telephone calls: "it would defy common sense to afford emails lesser… protection."[5] Moreover, the court urged: "the Fourth Amendment must keep pace with the inexorable march of technological progress, or its guarantees will wither and perish."[6]

Is There a Right to Privacy in Personal E-mails Sent on Work Computers?

While there has yet to be a high court ruling on whether there is a general right to privacy in e-mail, courts have provided some guidance on whether e-mail sent from work computers is private. Despite having access to both personal and work computers, most employees, at least on occasion, use work computers to send personal e-mails through company e-mail or personal web-based e-mail. Employees may be surprised to find out that depending on their employer's computer usage policies, the use of work computers to conduct personal business may defeat any expectation of privacy–even including the attorney-client privilege.

E-mails Sent from Work Accounts May Not Be Attorney-Client Privileged

In a recent California Court of Appeals decision, *Holmes v. Petrovich*,[7] the court found that e-mails sent by an employee to her attorney on a work computer were not protected by attorney-client privilege because they were sent from a work e-mail account. This opinion is now part of a group of

15 nationwide decisions since 2005 addressing whether an employer's No-Employee-Expectation-of-Privacy-Policy (NoEEP)/Technology-Acceptable-Use-Policy (TAUP) trumps an individual employee's attorney-client privilege rights.

In *Holmes*, the plaintiff was hired as an executive assistant to Paul Petrovich. Shortly thereafter, she informed Petrovich that she was pregnant. Petrovich became upset at this disclosure, and exchanged a series of e-mails with Holmes indicating that, while he did not intend to violate any laws, he felt taken advantage of. In response, Holmes used her work e-mail account to send e-mails to an outside attorney, indicating, among other things, her view that she was working in a hostile environment. Holmes eventually e-mailed Petrovich to inform him that his feelings regarding her pregnancy left her with no alternative but to end her employment.

Thereafter, Holmes filed a suit for sexual harassment, retaliation, wrongful termination, violation of right to privacy, and intentional infliction of emotional distress. At trial, the jury was shown several e-mails between Holmes and her attorney. Holmes had argued that these e-mails were privileged. However, the trial court had ruled that Holmes' e-mails, sent on a company computer and via the employer's e-mail system, were not protected by attorney-client privilege because they were not private. The trial court found support in the language of the company's detailed computer usage policy, which stated in unambiguous terms that:

- Company technology resources should be used only for company business and employees are prohibited from sending or receiving personal emails;
- Employees have no right to privacy for personal information created on company computers;
- Email is not private communication;
- The Company may inspect all files or messages at any time; and
- The Company would periodically monitor technology resources for compliance with Company policy.[8]

On appeal, the court affirmed the decision of the lower court, concluding that the pertinent e-mail messages did not constitute "confidential communications between client and lawyer" because Holmes knew of the company policy regarding no personal use, she had been warned that the company would monitor its computers for compliance with company policy, and she was warned that she had no right of privacy as to messages created on company computers. The court described the communications as "akin to consulting her lawyer in her employer's conference room, in a loud voice, with the door open, so that any reasonable person would expect that their discussion of her complaints about her employer would be overheard by him."[9]

E-mails Sent From Personal Accounts on Company Computers May Retain Attorney-Client Privilege

Last year, under slightly different circumstances, the New Jersey Supreme Court, in *Stengart v. Loving Care Agency, Inc.*,[10] came to the opposite conclusion, finding that an employee had a reasonable expectation of privacy in e-mails sent to and received from her attorney on her company laptop through a personal e-mail account. Marina Stengart worked as the Executive Director of Nursing for Loving Care and was provided a laptop to conduct company business. Stengart used her company-issued laptop to e-mail her attorney *through her personal Yahoo! e-mail account*, and later filed a discrimination lawsuit against her former employer. The former employer retrieved the e-mails through a forensic expert, and claimed that the employee had waived any privilege by using a company laptop to access the personal webmail account through which she had sent and received the e-mails.

The New Jersey Supreme Court disagreed, determining that due to the strong public policies underlying the attorney-client privilege, the communica-

tions remained protected from review by the employer. The court also noted that even if the company had explicitly informed the employee through its TAUP that the laptop could not be used for personal purposes and that it would retrieve and read all attorney-client communications, the policy would not be enforceable as to communications sent through personal, password-protected e-mail accounts.

The various privilege-vs-TAUP decisions, sometimes hinging on factual circumstances and other times on public policy, are refreshing recognitions of the role of e-mail in the workplace and in litigation today, and the need for the judicial system to further adjudicate privacy rights in this area. Employers should also seriously consider implementing an investigation manual that, among other protocols, red-flags an ostensibly privileged communication as a sensitive issue that an incident-response team should run up the flagpole to the employer's legal counsel.

What Protection Are Texts Afforded?

In addition to e-mail, there have been a few watershed cases regarding privacy in text messages. In *City of Ontario v. Quon*,[11] the U.S. Supreme Court held that a governmental employer conducted a legal search of its employee's text messages sent on employer-issued pagers. Although now pagers seem like they belong in medical television dramas or, possibly, a technological museum of antiquated electronic communication devices, back in 2001, when Quon received his pager, they constituted an innovative form of communication.

Quon was an officer with the city of Ontario Police Department. The city decided to issue pagers to its employees, including Quon. Years prior to receipt of the pagers, Quon and his coworkers had signed an "Employee Acknowledgment" of the city's "Computer Usage, Internet and E-mail Policy," which prohibited personal use of city-issued devices, including computers. Further, the policy stated "[employees] should have no expectation of privacy or confidentiality when using [city-issued electronic] resources."[12] The city never modified its policy to encompass pagers; however, it did orally notify its employees that that the policy would apply to pager use.

According to its service contract with Arch Wireless, the city had to pay any overage charges resulting from pager usage. Recognizing that many of the officers used the pagers for a mixture of personal and professional purposes, the city maintained an informal approach whereby if each officer paid the resulting overage charges, the city would not audit the text messages to determine if the overages were due to private, rather than business, use. Quon's pager usage resulted in multiple months in which he had overage charges. Even though he had paid for those charges, officials decided to audit his text messages. The city requested the transcripts of the text messages from Arch Wireless. While conducting the audit, the city found several sexually explicit text messages that Quon had sent to his wife, and to his girlfriend. Upon discovering these messages, the city terminated Quon. Quon then sued the city for violations of his right to privacy under the California Constitution and the Fourth Amendment to the United States Constitution, as well as Arch Wireless for violations of the Stored Communications Act.

The Ninth Circuit affirmed the trial court's decision in Quon's favor, finding that he had a reasonable expectation of privacy in his text messages, that the audit was constitutionally unreasonable in scope, and that Arch Wireless had violated the Stored Communications Act by turning over the text message transcripts to the city. The city appealed to the U.S. Supreme Court, which granted certiorari only as to the Fourth Amendment claim against the municipal employer. The Supreme Court held that even assuming Quon had a reasonable expectation of privacy, the search was reasonable because the city had a legitimate, work-related rationale for the search, and it was not overly intrusive. Unlike the

Sixth Circuit in *Warshak*, which clearly recognized that interpretation of the Fourth Amendment must change with the times and evolve into the new electronic communication era, the Supreme Court stated: "The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear."[13]

Nonetheless, significantly, the *Quon* Court did indicate that: "employer policies concerning communications will of course shape the reasonable expectations of their employees, especially to the extent that such policies are clearly communicated."[14] Thus, it would seem that a carefully crafted electronic use policy could eradicate, or at least considerably alter, an employee's reasonable expectation of privacy in the use of employer-issued electronic devices such as laptops and cell phones.

Search of Texts Incident to Arrest

A recent California Supreme Court case, *People v. Diaz*,[15] further contracted the Fourth Amendment protection afforded text messages in the context of a lawful arrest. There, a deputy sheriff witnessed Diaz participate in the sale of narcotics to a police informant. Once the sale was completed, the deputy stopped Diaz and arrested him for conspiracy in the sale of drugs. Incident to his arrest, the deputy conducted a search of Diaz's person and found drugs and his cell phone.

Upon arriving at the station, the deputy questioned Diaz to no avail. A full one and one half hours after arresting Diaz, the deputy searched Diaz's cell phone and found an incriminating text message. Once confronted with the text message, Diaz admitted to participating in the drug deal. Diaz later moved to suppress both the text message and his subsequent confession as fruits of an unlawful, warrantless search. The California Supreme Court affirmed the decisions of the appellate and lower courts, finding that the search was a lawful search incident to arrest because the cell phone was "'immediately associated with [Diaz's] person'" at the time of arrest,[16] which is an exception to the Fourth Amendment's warrant requirement.

The court did not seem to be overly concerned with the impact of developments in "modern technology" on searches incident to a lawful arrest, indicating: "If … the wisdom of the high court's decisions 'must be newly evaluated' in light of modern technology… then that reevaluation must be undertaken by the high court itself."[17] Moreover, the court echoed previous U.S. Supreme Court search and seizure cases, such as *United States v. Ross*,[18] in articulating that the character of the searched item should not influence the analysis of whether a warrantless search was lawful, despite the seemingly infinite storage capacity of cell phones. The *Diaz* court noted: "differing expectations of privacy based on the amount of information a particular item contains should… be irrelevant."[19]

What Lessons Can Be Learned from These Decisions?

Assuredly, this line of privacy decisions signals only the beginning of what will likely be an electronic-communication firestorm of appellate decisions over the next decade as the popularity of smartphones and social media rises. The take-away for employers is to be specific when drafting electronic use policies. Employers must decide whether, and under what parameters, to allow limited personal use of not only company computers, but also company e-mail and personal web-based e-mail. If employers intend to monitor employee use of company computers and e-mail, language should be included noting that the company may monitor, search, access, inspect and read computer contents and/or e-mail, and that electronic information created, stored, received or sent on company computers is not private. The lesson for individuals, whether in the workplace or otherwise, is that, even though personal, password-protected e-mail accounts are usually safe havens, privacy rights as

to cell phones and text messages, especially involving company-issued devices, are quite vulnerable.

Robert D. Brownstone is the Technology & eDiscovery Counsel and Electronic Information Management Group Co-Chair at Fenwick & West LLP. He is also a member of the Advisory Board of the National Employment Law Institute. He can be reached at (650) 335-7912 or RBrownstone@fenwick.com. Sheeva J. Ghassemi-Vanni and Soo Cho are associates in the Employment Practices Group at Fenwick & West. Each of their practices focuses on counseling as well as litigating a wide range of labor and employment issues. Ms. Ghassemi-Vanni can be reached at (650) 335-7191 or SGhassemi@fenwick.com. Ms. Cho can be reached at (415) 875-2485 or SCho@fenwick.com.