New Liabilities and Policies for Incidental Private Use of Company Electronic Systems and PDA

Winter 2009

Incidental personal use of company supplied computer devices and services, including Blackberries, often supported or hosted by third party providers, is commonplace. With it comes new risks and liabilities for companies and third party providers that are only beginning to be understood and managed. The trend of outsourcing service functions suggests that these problems will likely increase.

Allowing employees to use company electronic communication systems and personal digital assistants (PDAs) for incidental personal use, but retaining the right to monitor and audit the content of emails, messages and web traffic, is standard practice. But reviewing "personal messages" can be problematic. A recent unexpected case, finding that a public employer had violated employees' privacy rights and that its text messaging provider had breached federal privacy law, provides a sobering example of why companies should be alert to this problem so they can adjust their strategies accordingly.

The *Quon* Case

In *Quon v. Arch Wireless Operating Company, Inc.*, 529 F.3d 892 (9th Cir. 2008), the court found that a police department had violated the Fourth Amendment and state constitutional rights of several employees and those with whom they exchanged text messages by reviewing "personal" text messages created on pagers owned and issued by the employer. It also found that the text messaging provider, Arch Wireless, violated the Stored Communications Act (SCA), 18 U.S.C. §§2701-2711, by providing transcripts of these messages to the employer. Although the case involves the public sector, it is still instructive for private sector employers.

The employer in *Quon* had issued a written policy clearly notifying employees that any use of department computers for email or other internet access must be strictly limited to official business, and that employee communications using the department's computers or internet service provider would be monitored by the department. The policy stated unequivocally that internet and email systems were not to be used for personal or confidential communications, and that pagers were covered by the employer's policy with respect to monitoring or auditing.

Despite these formal policies, however, the department had an informal practice of allowing employees to use their pagers for personal text messaging as long as they did not exceed the 25,000 characters allotted to each pager by the employer's contract with its text messaging provider. When employees exceeded this limit, they paid for the excess usage from their personal funds. After the employer decided that the bookkeeping for these transactions was too time-consuming, it reviewed the employees' text messages to ascertain the proportion of business-related to personal messages. When the employees learned that their personal messages had been provided by the text messaging provider, they sued both their employer and the provider.

Although the trial court ruled for the defendants, the Ninth Circuit reversed, finding that the text messaging provider was an "Electronic Communication Service" (ECS) within the meaning of the SCA, and therefore could not release the messages without the permission of either the sender or the recipient. Addressing the privacy issues, the court ruled that the informal practice of permitting personal use created an expectation of privacy, despite the clarity of the written policy.

The court explained that the department could have given the plaintiffs advance notice that henceforth their text messages would be audited to determine whether any were personal, or could have given the employees an opportunity to redact the content of their personal messages if the intent of the "search" was to ascertain the relative amounts of personal and official

use of the pagers. Because the police chief had testified that the object of the search had been to ascertain whether the character limits on pager texting should be increased, reviewing the content of the text messages was ruled broader in scope than necessary.

Lessons from *Quon*

It is not clear that *Quon* can or should be extrapolated to claims by employees of private companies, as there are significant distinctions and different defenses. Yet the practical lessons are clear. Among them are:

- Even if some personal use is permitted, policies regarding employee use of email, internet access, and PDAs should be 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.
- Employers should require employees to expressly confirm that they have read, understood, and agree to the policy (i.e., they consent) by a signed acknowledgement, a "click through" link on the company's site or intranet, and/or annual reminders. The consent, in whatever form, should be tracked, stored and recoverable.
- There should be no informal practice or mechanism by managers or superiors for avoiding, overriding or "opting out" of this policy, and it should be enforced consistently. Staff should be trained about the importance of uniform oversight and should be reminded periodically of the policy.
- Carefully draft or "push back" on service agreements with outsourced or third party providers, where possible. This may include (a) contractual attempts to comply in advance with the SCA or other "wiretap" type statutes, such as by definitions (e.g., the employer is both the "sender" and "recipient" in this third party context) or other "consent" language; and (b) robust indemnity provisions , including coverage for any data breach or improper disclosure by the provider, to encompass data breach notices, forensic computer services, investigation costs, credit monitoring and related attorneys fees.
- Regardless of past practices, companies and their third-party vendors will need to check rigorously and, if necessary, update their standard subpoena and document response policies and protocols to comport with the SCA and possibly foreign laws if the company operates internationally. Consider privacy or cyber risk insurance, now offered by a number of carriers. These products have increased in sophistication and scope, and frequently provide useful cover for a variety of data disclosures, intrusion and breach event expenses and fees.

With proactive and protective procedures such as these, adverse results such as in the *Quon* case may be avoided or minimized.