

JULY 2010

Questions?

If you have any questions about this update, please contact:



Gary S. Starr, Partner
gstarr@goodwin.com
(860) 251-5501



Henry J. Zaccardi, Counsel
hzaccardi@goodwin.com
(860) 251-5737

One Constitution Plaza
Hartford, CT 06103-1919
860-251-5000

300 Atlantic Street
Stamford, CT 06901-3522
203-324-8100

1133 Connecticut Avenue NW
Washington, DC 20036-4305
202-469-7750

289 Greenwich Avenue
Greenwich, CT 06830-6595
203-869-5600

12 Porter Street
Lakeville, CT 06039-1809
860-435-2539

www.shipmangoodwin.com

Supreme Court Clears Way to Monitor Electronic Messages - Sort Of

The Supreme Court announced that an employer may review electronic messages if and when that review is motivated by a work-related purpose and carried out in a reasonable way. To do otherwise would infringe on an employee's privacy rights – rights protected under federal and state constitutions. Thus, employers must proceed with caution when monitoring electronic messages.

While uncertainty still exists in this area, the Supreme Court has provided some guidance for balancing the privacy rights of employees when sending and receiving electronic messages, and the interests of employers in avoiding abuse. Although the case outlines several principles for employers to follow, it leaves some unanswered questions.

The case before the Supreme Court involved a California police department that provided text messaging pagers to its employees. At the time that the pagers were distributed, the City made clear that its existing computer and Internet usage policy applied to pager use. That usage policy provided that the pagers were for business related purposes, and that pager messages were not private.

The City's contract with the pager company allotted a limited number of messages that could be sent and received each month. When messages exceeded that limit, an additional fee was imposed. When employees continually exceeded the monthly limit, the City required employees to reimburse it for the overage fees.

After months of incurring these extra fees, the Police Chief decided to review the pager usage to determine whether the monthly limit was either too low or too high. The City contacted the pager service provider and obtained transcripts of the messages of two employees who had repeatedly exceeded the limit. Upon review, the City found that the majority of the messages were not work related, and that one employee's messages

were sexually explicit between himself and his wife, and between himself and his girlfriend. The employees sued the City arguing that their right to be free from unreasonable searches and seizures was violated. The Supreme Court disagreed and found in favor of the City. In its decision, the Court was mindful of the special needs of an employer, which may be sufficient to justify searches for work related misconduct.

The Court found that the search was reasonable for two main reasons. First, the search was motivated by a legitimate work related purpose: the desire to assess the monthly usage limit. Second, the search was not overly intrusive. The court noted that rather than searching through personal e-mails or devices, the pagers had been provided by the employer and were not private.

Despite the outcome in favor of this employer, it is uncertain how employee privacy cases will be decided in the future. The Supreme Court emphasized that the reasonableness of searches and seizures turns on the specific facts of each case. The court noted, for example, that the plaintiffs were police officers who could have anticipated that their messages would be monitored for investigatory purposes. This leaves the issue unresolved in other cases where the employees may not be so informed or have jobs that would not normally be subject to such review.

While the challenge based on search and seizure law applies explicitly to governmental agencies, private sector employees also have privacy rights. Therefore, employers need to have in place usage policies that should be signed by employees, and the policy should make clear that messages sent and received are subject to inspection and are not private. When new technologies are introduced, the usage policy should be quickly updated to include the new device.