

Another case has been decided that should put employees on notice – there is no special privacy protection for email sent using your employer’s devices.

On December 13, 2012, the U.S. Court of Appeals for the Fourth Circuit upheld the conviction of Phillip Hamilton, a former member of the Virginia House of Delegates. Hamilton had been sentenced last year to over 9 years in prison for using his political position for his personal enrichment.

The source of some of the evidence used to convict him was an office email account from which he communicated his criminal intentions to his wife.

Hamilton appealed the conviction and sentence on many grounds, including the assertion that the use of the messages violated his right to privacy as well as his marital communication privilege.

The court demurred, finding that Hamilton waived the privilege because he sent the messages in question using his work computer and his work e-mail account. The court came to this decision even though the office where he worked instituted and communicated its computer use policy after most of the incriminating email had been sent.

Fourth Circuit Judge Diana Gribbon Motz wrote, "...(T)he district court found that Hamilton did not take any steps to protect the emails in question, even after he was on notice of his employer's policy permitting inspection of emails stored on the system at the employer's discretion."

As upset as privacy advocates might be about this case, the decision follows a long line of rulings where employee privacy rights related to communications emanating from office equipment have been severely restricted or denied by the courts.

One of the most prominent cases was *Quon v. the City of Ontario (California)*. Here, a police officer sued over the review of what turned out to be embarrassing, sexually-explicit messages that he had sent to his wife and his mistress using a department-provided pager. In its ruling, the court found that, due to the nature of Quon’s position and the reason for providing him with the device, he had no reasonable expectation of privacy. Although the issue was not raised specifically, presumably an argument as to marital communications privilege would have also failed for the same reason.

Quon was not a unique decision – it was preceded by a number of cases that reinforced the right of employers to monitor the information that passes through the equipment that they provide to their employees.

In 1996, in the matter of *Bohach v. the City of Reno*, the court dismissed a challenge to an employer’s stated intention to review the communications that passed between two employees as part of an internal investigation. The court found that the objecting plaintiff had not established that he had an objectively reasonable expectation of privacy in the messages at issue.

The unique aspect about the Bohach case is that the communications system through which the messages were sent was a proprietary system purchased by the city around 1995 for sending missives to its employees. This was not an unusual internal communication strategy for the time when considering that Microsoft Outlook was only introduced in 1997. Because this system was a municipal installation, the court determined that the city was the system administrator, giving the city special rights as to the data. As the system administrator, the court ultimately ruled that the city of Reno was "...free to access the stored messages as it pleased."

In 2000, CIA agent Mark L. Simon lost the appeal of his conviction for possessing pornography, which had been downloaded to his office computer. The court found that Simon had no reasonable expectation of privacy. Not only did the Foreign Bureau of Information Services have a well-communicated policy that prohibited the use of its computers for personal browsing, but it also gave its employees notice that the department might perform computer investigations to ensure compliance with this policy.

However, using the office computer for personal purposes does not automatically result in a waiver of privacy and privilege. There have been cases where employee email has been protected from perusal.

One of the most prominent of these cases is *Stengart v. Loving Care Agency, Inc.* In this matter, an employee filed suit against her former employer for discrimination. However, before she quit, she used her company-provided computer to send information she felt she could use to her advantage to her attorneys. After the litigation process began, it became clear to Stengart that her former employer had gained access to the legal strategies and documents that had been communicated with her attorneys. It was later determined that the defendants had copied Stengart's hard drive and used the material they found therein.

The court decided that because Stengart had taken steps to protect her privacy by using a personal email account that was password-protected, she had a reasonable expectation of privacy that preserved her attorney/client privilege.

The takeaway from these decisions:

It is important to establish and communicate a policy regarding the personal use of business property, updating the employee personnel manual so that it clearly indicates that employees should have no expectation of privacy as to communications to or from their office computer.

