WAS THAT "PIRACY" OR "PRIVACY"?

(Case 1031)

The Case:

Lawrence, the managing principal of NorthLink Consultants, is pleased at his firms' new information technology (IT) capabilities. Knowing that effective use of IT offers a strategic competitive advantage in the marketplace, Lawrence observes an increase in cooperation on projects and the office is using much less paper for memos and policy directives. The company web site is growing as staff, engineers and clients contribute to the site.

Lawrence, however, worries that several employees are spending an excessive amount of time on email. He suspects that much of this email activity is directed at family and friends on the Internet and outside the firm. He had reminded the employees of NorthLink's policy which states that email is for company business and emails are considered part of the firm's property.

Still, Lawrence feels that there is way too much time when employees are emailing in inappropriate ways. He approaches his systems engineer, Gwen, with a question. Since all the computers are connected on the computer network, could she access the employees' email files on their PCs? Gwen replies that such an examination of the files on the PC workstations is possible. Her own feelings, however, are that such an attempt to "reach out and touch" the users' PCs would be a breach of trust. In fact, some employees might be so offended with this intrusion of privacy that they would leave the firm.

Lawrence responds that company policy clearly informs employees that the email files are the property of the firm. They should understand that it is part of his supervisory responsibility to see that they use the email properly. Gwen argues that employees might well use the email to talk about issues that they do not want management to see. These may be legitimate company issues, but are not meant to be shared with the management. Adamant in his resolve, Lawrence states (as he walks out of Gwen's office) that, by tomorrow evening, he expects to be able to access all of the email files on each of the PCs.

Gwen is very disturbed. This policy will open up communications she feels should be regarded as private except when some formal legal decision requires them to be opened. However, since it is her job she knows she cannot refuse to perform a technical change in the system, and she feels she must allow Lawrence access by tomorrow evening.

Question: What should Gwen do?

NOTE:
This case is based on “Reach Out and Touch Someone” by the Public Administration at the University of Arkansas, and is used with permission.

Alternate Approaches and Survey Results for “Was That “Piracy” Or “Privacy”?” (Case 1031)

1. Comply, willingly. Gwen should do what she is told. NorthLink employees are using company equipment to make personal email transmittals and doing so on company time, despite having been informed that doing so is against company policy. They have no reason to complain, nor should Gwen complain or feel uncomfortable about following her supervisor’s orders.
   Percentage of votes agreeing: 10%

2. Comply, reluctantly. Gwen should stifle her conscience and abide by Lawrence’s request. She does not have the responsibility for strategic vision, running the company, or any other business decision, and should not insert herself into that process. Lawrence is in charge of this section and responsible for implementing company policy as it pertains to IT activities. Times are tough and she needs the job. After all, Gwen is not the one spending company time on private business.
   Percentage of votes agreeing: 6%

3. Refuse, flatly. Gwen should refuse to access the email files for Lawrence in the manner he has requested on the basis that his action is unethical. Further, she should inform Lawrence that she is prepared to resign if he forces the issue.
   Percentage of votes agreeing: 2%

4. Refuse, conditionally. Gwen should refuse to access the email files for Lawrence in the manner he has requested on the basis that his action may not be legal. Further, she should inform Lawrence that she will not access the files without express written approval from the human resources department, the employee union, and the firm's legal department.
   Percentage of votes agreeing: 13%

5. Analyze, carefully. Since she has access to the employee email files, Gwen should offer to do a confidential analysis for Lawrence of the email files to determine the apparent volume of personal messages, as well as which employees seem to be using the system the most for personal emails, but she will not review the nature or content of any of the messages.
   Percentage of votes agreeing: 7%

6. Document, clearly. Gwen should help Lawrence put together a brief agreement form for each employee to read and sign that reiterates the company’s policy regarding the use of its equipment and time for personal email communications,

and which clearly states that the employee agrees that the company has the right to review employee email communications on a random, unannounced basis, for compliance with the policy.
Percentage of votes agreeing: 28%

7. Monitor, quietly. Gwen should propose an option to Lawrence that instead of trying to read the emails, she can install a clandestine tracking system that keeps a daily log of internal and external email volume (sent and received) by individuals. This system will provide weekly reports of email activity to Lawrence, which he can use to manage IT resources and activities.
Percentage of votes agreeing: 13%

8. Monitor, openly. Gwen, as administrator, should suggest that she monitor the email of those employees who are putting the most strain on the email system and, if the email is not related to company business, counsel them privately to cut it out or risk the loss of their job. Prior to setting her on this course of action, Lawrence should announce to the staff that, in accordance with the Company Policy, email will be read and individuals engaging in email correspondence unrelated to Company business will be subject to the written corrective action policy (counseling, warning, formal reprimand, suspension, termination). All discipline above counseling would be performed by Lawrence and/or his partners.
Percentage of votes agreeing: 15%

9. Inform, quickly. Gwen should quietly inform all employees of Lawrence's abrupt decision, immediately, and suggest that individuals clean out their email files so as to not face Lawrence's ire. She should note the date and time of Lawrence's remarks to her, and, for her own file only, reasons for her opposition.
Percentage of votes agreeing: 3%

10. Download, surreptitiously. Gwen should realize that this is the perfect opportunity to see how the firm's partners, including Lawrence, spend their email times. After making sure that her own email box is clean as a whistle, she should make a copy of each manager's inbox for perusal later, since you never know when this type of information might come in handy.
Percentage of votes agreeing: 2%

Forum Comments from Respondents

1. Comply, but it will not work and Lawrence will need to come up with an alternative. Gwen will do her job, and ultimately, Lawrence will NOT be satisfied. People will use other accounts like Yahoo, HotMail, MSN, and so on. People will only use the company account for related business; however, they will continue to use the network for personal business.

2. Similar to monitor openly, Gwen should do what Lawrence asks her to but only after informing all employees about the change in structure of the system. The goal is to make sure that employees aren't comitting "theft of payroll funds" by

using time inappropriately. In response to Gwen's privacy concerns, a system should be set up in which the employees can communicate to one another via emails specially marked as ones not to be viewed by management. A non-management employee (perhaps Gwen) should be given the authority to monitor these emails.

3. Combine Approach 6 and 8. First, the managing director should be counseled regarding the ethical and legal aspects of his decision. Specifically, he should understand that the review and disciplinary process must ensure the equal treatment of similarly positioned employees - if a star performer and a weak performer are both found to have abused the email system, the managing director must be prepared to treat the employees in a similar fashion to avoid a lawsuit by the poorly performing employee. (Of course, that information might diminish his desire to review the emails.) Second, if employees have not already signed an acknowledgement that they have read and agreed to the employee policies (including a clear statement of policy, including the company's right to review employee email communications on a random, unannounced basis, and the consequences of breaching the policy), then a signed acknowledgement should be obtained in order to help avoid misunderstanding or miscommunications. If employees have already signed such an acknowledgement (often done at the time of hire) then that step appears to be unnecessary. However, there should be an announcement that the review process has begun, who is involved in the process, how confidentiality is being protected, and that the email review will be prospective only. As for the process of review, an employee in a position of trust (perhaps the director of HR or legal counsel) should guide the process. Given Gwen's concerns with the directive, she might not be in the best position to adequately or properly manage the process. All discipline above counseling would be performed by Lawrence and/or his partners; however, accurate records should be kept of the disciplinary process and the reasons supporting the actions taken against an employee.

Comments from Board of Review Members

1. Whether or not the company has a "right" to review the email, doing so will generate a huge moral and morale problem within the firm, regardless of what information would be revealed. Employees have a right to some privacy, and this is a change in company policy that supercedes this right. Until now, the company has not performed email monitoring, nor stated it would. To institute this policy without warning is not appropriate. Gwen should try explaining this to Lawrence again (and other Partners), with an admonishment to notify the employees in advance of instituting this spying. She should let him know that he is opening himself, and the company, up to lawsuits and loss of good employees who will not tolerate this kind of behavior.

2. One key consideration is the sensitivity of the content of the emails even if they are all relevant company business. Inappropriate disclosure (even to Lawrence) of personnel decisions could cause serious (and unnecessary) personal and/or

professional embarrassment. For example, I am aware that the Department of Defense (DoD) does routinely screen emails sent through DoD email systems. They also have monitoring programs that automatically compile and report visits to "inappropriate" internet web sites. The most common inappropriate type of site is pornography, but that is not the only type of site prohibited. Service members have been tried and convicted of computer crimes based on their emails and website visitation histories.

3. A very interesting question; we are addressing it at our firm right now but on a slightly larger scale. Our firm is networked with T1 lines between all offices and high-speed internet access from every desktop. Recently our MIS Manager noticed that the server hard drives were becoming filled up, which was surprising given their size and previous company history of hard drive capacity utilization. He checked and, lo and behold, there were gigabytes of totally inappropriate files that had been downloaded and saved to the company's servers. Virtually all of them were of a nature that would cause legal difficulties of one type or another (either with owners of intellectual property or, in some cases, with law enforcement personnel). After conferring with our Chief Operating Officer, he did a file wipe with no prior notification to those who had saved those files. At the next "all hands" company conference call, the announcement was made that our MIS Manager would be using his Network Administrator technical capabilities to, 1) identify who was embezzling company property (paid "on-the-job" time, PLUS bandwidth, PLUS file space) in this fashion, and 2) forward a copy of the offending file (including date, time, duration of time on line, and identity of the employee who did the download) to our CEO, who will not tolerate such activity. How does this story relate to your case history? In several ways. First, diversion of company property to employee personal use is theft. This includes the time the employee spends conducting personal business when they are at work. Consulting firms like mine sell their time to their clients; clients would not pay for time used by a consultant's employees who were taking a nap when they were supposedly conducting a field investigation. This situation is equivalent. Second, the problem is larger than simple inappropriate email use. Chat rooms and internet browsing are highly addictive activities. Employees who are not being properly supervised can literally spend hours in this fashion. Third, downloaded files offer the added risk of exposing the firm to significant adverse legal liability ("If you did not know that our intellectual property had been pirated and was resident on your server, you should have known and I'm sure the court will agree.").

4. Gwen is obviously sensitive to the employee's side of the issue. Lawrence should recognize that sensitivity and suggest a compromise. Gwen, as administrator, should monitor the email of those employees who are putting the most strain on the email system and, if the email is NOT related to company business, counsel them privately to cut it out or risk the loss of their job. Prior to setting her on this course of action, Lawrence should announce to the staff that, in accordance with the Company Policy, email will be read and individuals

engaging in email correspondence unrelated to Company business will be subject to the written corrective action policy (counseling, warning, formal reprimand, suspension, termination). All discipline above counseling would be performed by Lawrence and/or his partners.

5. When I worked as a consultant, my company, I believe, had a similar policy to NorthLink's. However, I don't ever recall being explicitly informed about it; the policy was just something you assumed was "out there," and I don't recall it ever being talked about. To my knowledge, the issue of invasion of employee privacy was never raised, probably because we had reason to believe that management was monitoring email, even though they never talked about it.

6. An interesting case, indeed. My company's policy is pretty much like NorthLink's. We have the capability to monitor email but we rarely do it. That is, we only monitor email if there is some evidence that it is being abused. We have a number of firewalls that prevent employees from visiting inappropriate sites, and we have not had any complaints about intruding into people's personal lives.

7. Gwen has two choices: (1) do what she is instructed to do, or (2) resign her position. Little would be gained by resigning since the next system engineers will be required to provide the information so the privacy of the employees would still be breached. Gwen might request a 30-day delay in carrying out the instructions so she can check with the firm's legal counsel to verify that no statues were being violated and also investigate what other firms are doing. She might also suggest that she review the emails (instead of Lawrence reviewing), and she would talk with those who are violating the firm's policy. She might also suggest that it would be better not to review past emails, but rather publish a notice that all emails henceforth are subject to review by management. The best procedure would have all employees sign an acknowledgement of the policy. Very likely Gwen's suggestions will fall on deaf ears. In that case she should proceed carrying out Lawrence's instructions.

8. This is a most difficult case. It is one that our firm has addressed in the past and we use a "signed acknowledgement" of the review policy. It should be noted that management has the responsibility to see that emails are used appropriately. Several lawsuits have been filed against firms due to inappropriate use of email. Also, emails should not be used to convey messages that the sender does not want management to see.