

Pseudo-private data and workplace sensitivity

© 2004 Andrew Seely

University of Maryland University College, European Division

[aseely@faculty.ed.umuc.edu](mailto:aseely@faculty.ed.umuc.edu)

## Pseudo-private data and workplace sensitivity

Your cubicle mate quietly hangs a poster on his side of the partition. The poster is a photograph of a woman with large breasts, wearing a string bikini and a provocative smile. Another colleague sends an email to select friends at work, including you, discussing how the blacks on staff probably don't work as hard as their slave ancestors. Yet a third has a screen saver on her computer that scrolls a message stating that all Jews and Muslims are sinners who will burn in Hell. A fourth takes frequent visits to other cubicles to talk about his wife, who is home, barefoot and pregnant, "just the way all women should be."

In all four cases, your action is likely to be guided by any reasonable, modern corporate Equal Employment Opportunity (EEO) policy. Such policies clearly prohibit activities that create a hostile work environment, especially when those activities are sexually charged or target employees on a basis of race, creed, or gender as defined by the Civil Rights Act of 1964. Penalties for such transgressions may even be more severe when the perpetrator is in a leadership position or has in some way made acceptance of the behavior a condition of employment.

No one in the modern American work force would question that a clearly hostile work environment exists when an employee must listen to unwelcome sexist jokes told by the boss in the workplace during business hours. There is no such problem, however, if the

boss kept his jokes in a private file – unless looking at the contents of that file were a requirement of the employee’s job.

In the modern information technology (IT) workplace, EEO policies and feelings of individual empowerment have made overt problems more and more infrequent. An area of work that is IT-centric, though not necessarily IT-specific, is the use, storage, and access of what may be termed “pseudo-private” data.

What is pseudo-private data? Are there occasions in a corporate computing environment where there may be a reasonable assumption of privacy as opposed to an expectation of privacy? A network password, for example, is by definition private. Corporate security policies frequently and explicitly specify that a user’s password should be known only by the user, should be memorized, and should never be written down. Based on such a policy, the user has a reasonable assumption that no one will ever see his password.

Similarly, browser caches and temporary system files are temporary, scratch files that are not intended as products in themselves. A worker creating a report would not expect to be held accountable for the intermittent “save-files” a word processor may make every so often, especially when the word processor is designed to delete such files when the program is closed. Thus, intermediate, working copies of files that are stored as temporary systems files may be assumed to be for the use of and consumption by the software only during a small window of time. There is a number of variables that may be joined in such a way as to create a hostile workplace situation that is not explicitly

defined in standard corporate policies. This possibility exists almost exclusively with the positions of security and systems analysts and may result in the analyst having to view, as a function of employment, material defined as offensive by EEO policy. What must be determined is if the assumption of privacy with respect to pseudo-private data outweighs the protection of workplace sensitivities in the very small percentage of employees that actually work in system analyst positions. The following scenarios help to illustrate this problem.

#### Scenario One

Bob is a model employee with respect to EEO policy. He is polite, does not display offensive materials, and treats all coworkers equally. Betty is the corporate security analyst. Betty's job description includes the task of regularly cracking the authentication server's ciphertext password list. To accomplish this task, she has access to appropriately powered equipment; i.e. she can crack long passwords in less time than password policies dictate they be changed. Thus, as condition of Betty's employment she must view the pseudo-private data contained in any users' password. Does the corporate EEO policy define Bob as creating a hostile work environment if Betty cracks his password and finds that it is "f\*\*kmebetty"? Or does Bob have a reasonable expectation of privacy based on the company's password policy guidelines?

#### Scenario Two

Becky is outwardly a model employee with respect to EEO issues, as is Bob above. Bill is a support technician and subordinate to Becky in the organizational chart. Becky is white, Bill is black. Becky has been working for many days on a document that will eventually be a report to shareholders, but her computer crashes. She had the auto-save feature of her word processor turned on, but the files became corrupted. Bill is called in to recover what he can from the corrupted files and finds that Becky had inserted – and deleted – racial slurs in front of every non-white person’s name mentioned in the report, including Bill’s. The auto-save feature has tracked the deletions to facilitate in recovery of damaged files. Thus, to perform his job, Bill must view racially disparaging remarks written about him by his boss. Becky obviously had no intention of making these comments public and she has never acted in a disparaging fashion to any employee, but her temporary system files stored her activity in progress. Does Bill have the right to report this? Or is Becky above prosecution with respect to EEO policy because she had an assumption of privacy for her system’s temporary files?

### Conclusions and Recommendations

Typical EEO policies do not explicitly address this issue. While a company may decide to discipline Bob and Becky on general principle, they may not have acted against any specific policy. “Consent to monitoring” notices and user agreement forms may act as a catch-all; if you type it into your keyboard then its fair-game for monitoring and thus has no assumption of privacy. But rigorous enforcement of this is philosophically opposed to

typical password protection policies and may create an atmosphere of distrust in the workplace.

This paper has demonstrated a special case where disruptive behavior can exist outside of typical policy. The window of possibility for workplace offense is small; how many outwardly nice people are hateful in these ways? How many lewd passwords are really cracked? Is it even worth thinking about enough to create or modify a policy? If policy is changed, a fine line must be tread between allowing employees to work freely and giving the appearance of attempting to micromanage their thoughts. Policy should provide for retroactive penalties but should stop short of preventative monitoring. Considering the highly litigious nature of the United States, it may be wise for companies to expend some effort to address this issue.