In Defense of the Hard Drive

James M. Rosenbaum

A new "legal principle" has emerged. It holds that if a corporation, business, or government entity owns a computer, and if an employee puts personal matter onto that computer, the author has neither a right nor an expectation of privacy in the computer-stored material.

This idea seems to have sprung forth spontaneously. There is, however, little evidence that it was inscribed on tablets or received atop a mountain. It seems to me, like many *a priori* truths, it ought to be further examined. This examination is essential, because a free society has a vital interest in preserving for its citizens a central core of privacy to protect their most personal thoughts. If this new principle is erroneous, the error is pernicious.

As an initial, but not quite trivial matter, it seems the idea is somehow related to two facts. First, computers are expensive, making the employer concerned about them. This contrasts with paper and pencils, which people have used for years. But paper and pencils are cheap; they are lost and nobody cares. Second, computers keep everything in one place – on their hard drives. With paper and pencil, chasing ideas is a messy, time consuming process, but a computer's hard drive is imaged[1] relatively easily.

A Cautionary Tale

Just a few months ago, this issue played out at the offices of the *New York Times,* of all places. Someone at the company's business office received an envelope containing photocopied material – one of those endlessly copied items which once circulated in offices everywhere. Whatever its content, the recipient clearly found it offensive. This probably-odious item came to a supervisor's attention. From there, it was doubtless conveyed to the legal staff.

If a company takes no action to remedy this situation, items such as these can engender a hostile work environment claim. And a simple corporate policy against sexual harassment is unavailing unless management makes the policy effective. What to do; particularly at an

Judge James M. Rosenbaum sits on the United States District Court for the District of Minnesota.

1 A trendy cyber-word for "copy."

organization which owes its very existence to the Constitution's protection of the right to freely express ideas?

The *Times* responded with a clandestine search of the infected division. No notice was given to the employees. The company reviewed the contents of every computer hard drive. It did so, even though the offending material was photocopied rather than computer-generated.

The search apparently unearthed[2] a number of nettlesome items, ranging from tasteless jokes to pornography – all on computers owned by the *Times*. In the aftermath, some 10% of the department's employees were summarily terminated; others were reprimanded and warned, which is unlikely to have a positive effect on the recipients' future careers with the *Times*.

Ensuing news reports were explicit: The employees had no rights in the face of this electronic rummage though their lives. They had no rights, because an employee should not expect privacy on material residing in a company-owned computer.

As a working judge, I know the *Times* has strengthened its defense against a hostile work environment lawsuit. But as a person, I wonder if I'd like to work there.

A Precept & Some Thoughts on Privacy

Americans harbor a deep-seated revulsion against "general searches." These are a kind of unregulated meander through an individual's papers and effects. In the years leading to the Revolutionary War, the British used general searches as a way to root out anti-English traitors and sympathizers. The citizens of the nascent Republic found these searches wholly unreasonable.

Their disgust led the Founders to draft the Constitution's Fourth Amendment. It protected their right "to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures." The Constitution protects individuals against actions by the government, but it embodies a higher principle: it expresses the concept that an individual retains a certain sphere of privacy which is inviolate.

An employee unquestionably owes a duty to perform services on the employer's behalf during the work day. And playing computer games, surfing the web, or collecting obscene material is probably not the service for which the employee is paid. But do the employee's idle acts permit the employer to more, beyond proof of the employee's breach of duty? After establishing its right to reimbursement, recompense, or even termination, the employer's right to wander through the employee's personal material does not seem self-evident.

A Book: Seventeen Years Too Early

In George Orwell's *1984*, each dwelling was equipped with a television camera and sound pick-up device which continuously sent the citizen's words to the government. The result was a cowed citizenry; afraid to think and afraid to express their thoughts, lest their ideas be overheard and punished.

The present concept permits – and even encourages – "Big Brother" searches. Most employers are not governmental entities, so constitutional search and seizure issues are not directly implicated. But just as an employee does not surrender all privacy rights on the company's premises, so they should not be automatically surrendered on the company's computer.

I have, happily, never sneaked around in the other computers in my building. But if the

2 Is "unearthed" a proper term when the burial environment is a computer hard drive?

others are anything like mine, each hard drive contains at least a bit of idle stuff. And if this is so, each employee stands subject to a search which goes, without restriction, far beyond any legitimate business interest.

A Proposal

There must be a balance between the employer's concerns for proper computer use and the employee's interest in personal privacy. I suggest the fulcrum of this balance lies in a "cyber time-out," coupled with reasonable notice to the worker. An employer with a definable reason to examine an employee's personal computer ought to be permitted to do so. But prior to undertaking its examination, the employer ought to give the employee reasonable notice of its concerns. For the sake of discussion, let us assume a reasonable time-out might be 72 hours.

It is easy to sequester a computer to preserve its content between the time of notice and examination. During this time-out period, the employer should be required to tell the employee its reason for examining the computer, and identify the files it proposes to examine. This notice minimizes the prospect of an employer's examination becoming a *de facto* general search.

This time-out, first, gives the employee notice of the employer's concerns. But secondly, and importantly, it gives the employee a chance to examine any options which may be available. Among the options available should be a chance, informally or by legal intervention, to limit or define the scope of the hard drive examination.

The time-out also gives the employee a chance to take some curative step or attempt to resolve matters without someone rooting about in his or her personal affairs. If the examination proceeds, either the employee or a representative should be permitted to attend. Once the employer's notice is refined, the examination must be restricted to the noticed subjects; stored information beyond its scope is off-limits.

I add one additional factor to this mix: an employer which fails to give the required notice, or violates the time-out, should be barred from taking any adverse employment action against the employee. Finally, in the event the employer fails to comply, the employee can seek damages resulting from the failure.[3]

This arrangement also accommodates any need to preserve evidence, should a civil or criminal dispute ensue. In a civil matter, the hard drive would be available for regular court discovery. Similarly, an employer suspecting illegal conduct can go to law enforcement – which is, after all, entrusted with the regular means to examine and prosecute crimes. In either case, orderly processes protect each party.

The present regime, giving employers a near-Orwellian power to spy and snoop into the lives of their employees, is not tenable. The use of an employer's computer should not be equated with the loss of its operator's rights. A society which values individual freedom cannot function this way. It seems to me a simple notice, coupled with a short cooling off period, can go a long way to protecting a citizen's essential right to think without fear.

3 There is another, perhaps not trivial, upshot of this proposal: In imposing a moderate restriction on the employer's access to the personal information residing in the employee's computer, it imposes a collateral restriction on *governmental* access at the same time. It does so, because if the employer must recognize a defined area of employee privacy, it cannot simply confer unfettered access to "its" computer to a government investigator. As a result, the government, along with the employer, is dissuaded from attempting a general search.