Portfolio Media, Inc. | 648 Broadway, Suite 200 | New York, NY 10012 | www.law360.com
Phone: +1 212 537 6331 | Fax: +1 212 537 6371 | customerservice@portfoliomedia.com

No Privacy For Employee Info On Office Computers

By **Patrick T. Collins, Fernando M. Pinguelo and Keya C. Denner, Norris McLaughlin & Marcus PA**

Law360, New York (September 19, 2008) -- In a case of first impression in New Jersey that has potential ramifications for New Jersey employers and employees alike, an appellate court recently upheld the warrantless search of office computers used by an employee to store information relating to his theft of over $650,000 from the company.

Finding no controlling precedent in New Jersey, the appellate court applied federal rulings from other jurisdictions and held that the employee had no "legitimate expectation of privacy" in information he stored on office computers, even if that information was personal in nature and protected by confidential passwords erected by the employee.

The ruling stands as a reminder to employers of the importance of background checks, effective computer and e-discovery protocol and e-mail policies, and monitoring employee activity; and should make it easier for law enforcement and employers to work together to expeditiously gather useful evidence of employee theft.

By taking certain precautions outlined below, employers can help insulate themselves from dishonest employees.

The defendant-employee ("M.A.") in State of New Jersey, v. M.A., docket no. A-4922-06T4, was hired as a temporary bookkeeper in 1997 by Joseph Braun ("Braun"), a majority owner of Certified Data Products ("CDP").

At the time of his hiring at CDP, M.A. had already been convicted of forgery in connection with his theft of $221,871.05 from a former employer, and a civil judgment existed against him for the amount of this theft. Braun apparently failed to conduct a background search of M.A. prior to his hire.

At the time of his hiring, Braun advised M.A. "that the computers or anything in the office is company property." M.A. also signed a non-disclosure of confidential information and non-compete agreement.

Within a short time, M.A. became a trusted employee of CDP, and was promoted to a full-time

bookkeeper position. His job responsibilities included invoicing, order entries, payroll, and bank and payroll records; and later expanded to include a supervisory role.

M.A., who maintained a side-business known as Dynamic Data Solutions ("DDS") that specialized in the sale of used computers, represented to Braun that he also had expertise in computers, and Braun relied upon him for all of CDP's computer needs. Through DDS, M.A. sold CDP approximately ten used computers. M.A. installed these computers for CDP, upgraded CDP's computer system, and set up a computer network for CDP.

Employees of CDP could log into CDP's network system created by M.A. by using a common password and entering their name. CDP's network system had only two administrators, M.A. and Braun, who each shared access capabilities. Unbeknownst to Braun, M.A. also placed separate passwords in two computers, so that only he could access the stored information protected by these passwords.

One of these computers, a desktop tower, was purchased by CDP from DDS in 2001, and was located in M.A.'s private office located within CDP's offices. The other password-protected computer was a laptop that was previously owned by M.A., but was also purchased by CDP from M.A.

Subsequently, CDP's software and designs were installed on the laptop, and M.A. and another CDP salesperson used the laptop for business purposes. The laptop was kept primarily in CDP's offices.

It did not take long for M.A. to revert back to his criminal tendencies. In 2002, Braun discovered that M.A. called CDP's payroll company and increased M.A.'s salary by approximately $85,000 per year.

After confronting M.A., Braun immediately fired him. At no time after his firing did M.A. ask for the return of the two password-protected computers, or otherwise claim ownership of these computers.

Subsequent to his firing, Braun eventually learned that M.A. stole a substantial amount of money from CDP, and, therefore, involved the police. Braun informed the police that CDP owned the two password-protected computers, and signed two forms consenting to a search of the computers by the New Jersey State Police High Technology Crimes Investigation and Support. The search revealed evidence of M.A.'s theft of approximately $650,000 from CDP.

On appeal from a trial judge's ruling that the consensual search of the two computers was proper, M.A. argued that he had a reasonable expectation of privacy in the personal information stored on both computers because they were kept in his private office and he had placed confidential passwords on the computers to block access by others.

The appellate court, however, rejected this argument. Recognizing that no New Jersey court had directly addressed this issue, the appellate court relied upon federal caselaw from the 10th and 4th federal circuit courts of appeal and a Nebraska federal district court to conclude that M.A. had no reasonable expectation of privacy in the personal information stored on his workplace computers.

The important distinction for the appellate court between the circumstances of this case and other cases relied upon by M.A. to support his argument was the heightened expectation of privacy that a person enjoys while at home as opposed to while at work.

The appellate court relied upon several factors, outlined below, to uphold the search of the workplace computers that directly and indirectly relate to this key distinction. As these types of inquiries are undoubtedly highly fact sensitive, employers will be served well to consider these factors as guideposts to better protect themselves against employee theft, and ensure that warrantless consent searches of workplace computers by law enforcement will be upheld by the courts:

1. Employer Owned the Computers, and They Were Kept at the Workplace.

The appellate court upheld the finding that CDP owned both the desktop and laptop computers handed over to the State Police. Accordingly, to the extent possible, employers should strive to ensure that employees only use employer-owed computers, and employers should discourage employees' use of personal computers for work-related activities.

Employers should also prevent employees from installing company-related software on employees' personal computers to further discourage the use of personal computers for business purposes. Employers should memorialize these expectations through a written policy.

2. Employer Advised Employee Upon Hiring That all Workplace Computers Were Company Property.

Whether or not the employment relationship is documented, it is essential that the employee be made explicitly aware that workplace computers, including employer-issued laptops, are the sole property of the employer.

Employers are advised to keep track of company-issued hardware (including laptops, PDAs, memory sticks, cell phones, etc.) by maintaining a log of when company-issued hardware is provided to an employee and when the hardware is transferred or decommissioned.

Such detailed records also will help an employer with e-discovery related obligations including duties to preserve electronically stored information ("ESI").

3. Desktop Computer was Connected to the Employer's Network, and Laptop Contained Business Software.

These self-explanatory factors highlight the importance of drawing a clear line that company property is just that, and should be used only for company-related business.

In scenarios where it is difficult (if not impossible) for an employer to prevent an employee's use of personal computers for business-related activities, such use should be deterred through the use of a written policy prohibiting it.

4. Employer had Equal Access to the Computers, and a Co-Worker had Equal Access to the Laptop.

Whether or not someone's belief that his or her computer activities are private turns on who else has access to that computer.

Even if, for example, a particular company-issued laptop is used by only one employee, employers should make sure their network is set up so that more than one company administrator will be able to monitor others logged into the network at any time.

Moreover, employers should issue employee-specific login passwords and keep track of

employee computer activity.

5. Employee's Office was Never Closed or Locked.

This factor - access by others to an allegedly private space in the office - is analogous to the previous factor – access by others to alleged private information in "cyber space." Needless to say, employers should rarely give an employee the ability to completely lock others out of his or her work area.

Exceptions to the general rule include HR and benefits personnel who maintain sensitive employee files in their offices. While an argument can be made that an employee who holds the only key to his or her locked office enjoys some expectation of privacy in the contents of that office, one way to counter this argument is to include a written reminder in an employment manual that the office is to be used for business purposes only and that the employer has the absolute right to access the office and its contents at its discretion.

Cases in this area of the law are highly fact sensitive. The existence of one or all of the above factors might not necessarily guarantee that a consensual search of workplace computers will be upheld.

Following these guidelines, however, is a step in the right direction to both preventing employee theft, and ensuring that law enforcement will have access to one of the most important pieces to the forensic puzzle in the event a hi-tech theft occurs.

In addition to the factors specifically addressed by the appellate court, the court's ruling offers additional lessons to be learned (or reminded) in helping to shield employers from common pitfalls.

First, the most glaring gap in the factual recitation of the court's ruling is that the employer could have likely easily prevented this situation from occurring by conducting the appropriate background (criminal, credit, references) checks. This step in the employment hiring process should not be overlooked.

Second, nearly all of the information now being created and stored by businesses is being created and stored electronically; and court rules have been amended to recognize this trend.

These rules include new obligations on businesses regarding ESI, and require businesses to: (1) understand their technology and keep track of ESI and computer-related hardware; (2) suspend any routine ESI deletion policies when a lawsuit is anticipated, and (3) be aware of the new obligations imposed upon them.

Employers must understand their technology now and create procedures that demonstrate that they have a plan of action to segregate and preserve ESI if required to do so.

Third, employers are reminded that they should have written e-mail policies in place and enforced when it comes to employee use of email.

For example, these policies should outline what is and is not appropriate usage of e-mail (i.e., limit its use for business purposes only), remind employees that e-mail activity may be monitored at any time and at the sole discretion of the company, and address abuses as they are uncovered.

Fourth, with employment-related crimes on the rise (annual estimates top at $50 billion) and

technology advances enabling people to commit crime with relative ease and anonymity, employers should implement precautions to combat the occurrence of these crimes in the workplace.

For example, employers should (1) use password protected software, (2) allow only employees who need access to sensitive information to be given that access, (3) avoid centralizing responsibilities in one employee, (4) avoid exclusive contact with vendors by one employee, (5) review bank accounts periodically, (6) establish internal controls that randomly audit records and transactions, and (7) conduct an audit periodically.

Taking these relatively simple precautions will go a long way to help insulate your company from employee abuses and misconduct, and lend credence to the old adage that "an ounce of prevention is worth a pound of cure."

--By Patrick T. Collins, Fernando M. Pinguelo and Keya C. Denner, Norris McLaughlin & Marcus PA

Patrick Collins is a member of Norris McLaughlin & Marcus and chair of the firm's labor & employment group. Fernando Pinguelo, also a member of the firm, is chair of its entertainment law group and co-chair of its response to electronic discovery information group. Keya Denner is an associate with the firm.