BusinessManagement DAILY

AUGUST 30, 2015

Personal data on business systems: The high cost of curiosity

by Niloy Ray, Esq., Littler Mendelson, Minneapolis

It's hardly shocking that many employees use work technology for personal matters—whether that's online shopping, catching up on social media or sending email to friends and family. Apart from the familiar issue of impermissible use by employees, this intermingling of personal and business computing creates less-obvious traps for employers.

As a recent New York case illustrates, ready access to personal information can lead a well-meaning but unwary employee into legal liability, even if the information accessed is properly discoverable in litigation.

An accidental discovery

In April 2008, an employee of Pure Power Boot Camp, a fitness center, decided to set up a personal Hotmail account using a work computer. On the Hotmail home page, she noticed something unusual—the user-name and password of a former employee. Apparently, the former employee had checked his personal email on the work computer, and saved his Hotmail log-in information on the machine.

The employee knew that Pure Power was having trouble with that former employee. He and another employee had recently quit to start a rival fitness center, Warrior Fitness. Talk around the office was that the two had been planning the move for months, and had allegedly stolen sensitive information, including Pure Power's business plans, customer lists and start-up and operations manuals.

So the current Pure Power employee logged into the former employee's personal Hotmail account using the credentials she had found. Once in, she noticed an email with the former employee's personal Gmail log-in information, so she logged into his Gmail account as well. She then figured out that the former employee used the same password for his Warrior Fitness email, so she accessed that account, too.

Compelling evidence, but …

From all three accounts, she found a trove of emails providing a detailed picture of two former employees' unlawful plans and actions. She printed them out for her superiors. That led Pure Power to sue.

The court found that the emails demonstrated ill intentions and disloyal conduct, and awarded $250,000 to Pure Power.

However, the court also held that the employee's actions, while well-intentioned, were unlawful. Even though

the court agreed that the two former instructors would otherwise have had to turn those personal emails over in the course of the lawsuit (and so Pure Power would have ultimately obtained this information), it allowed the defendants to countersue her, alleging that she had "stolen" the emails.

Following trial, the employee was ordered to pay $4,000 in damages for improperly accessing the emails.

What's off limits?

Where did the Pure Power employee go wrong? During civil litigation, businesses certainly can rely on information from their own systems to implement their legal strategy.

However, they cannot access personal email and other accounts (like social networking sites), even if they have the means to do so via information stored on their business systems.

Similar rulings against unauthorized access to information from personal accounts have been issued in many other cases, including when:

- An employee left her personal Gmail account open on a work computer and told colleagues her passwords.
- A manager asked an employee for the password to a personal MySpace group account and she felt pressured to comply.
- Temporary fragments of privileged email from a password-protected, personal Yahoo account were found on a work laptop.

Lessons learned

Employers should adhere to this simple principle: Unless the account-holder specifically gives authorization, never access—let alone print and use—information contained in password-protected, personal accounts. Asking for passwords or access is not foolproof either, as that could be coerced access if the employee felt pressured to comply.

Supervisors should not try to connect with employees through social media as a pretext to gain access to their private online statements.

Invasive methods, such as using keystroke loggers or password cracking tools, are even more inadvisable.

In sum, while some circumstances cut against the grain—such as when an employee voluntarily brings the information to a business's attention or where an IT policy lawfully authorizes its access—the best practice is to refrain from accessing and looking through anyone's personal email or other social-media accounts. That's true even if it is accessible via the company's business systems.

Instead, let your attorney seek this evidence through regular discovery channels in litigation. That protects the business—and your employees—from unintended consequences.

Niloy Ray advises clients out of Littler Mendelson's Minneapolis office. Contact him at nray@littler.com or (612) 313-7641.