Feds Creepy Use of Spyware to Monitor Employees Provides Privacy Lesson for Everyone

July 31, 2012 - Earlier this year, the New York Times ran a story detailing how the Food and Drug Administration had used computer spyware to monitor six scientists that had turned into whistleblowers. As it turned out, the FDA program started that way but it grew in scope. Now, the National Law Journal is reporting that both the VA and DEA are using exactly the same program. While both the VA and DEA are saying that they don't use the program for employee monitoring, they are not saying what they do use it for. And since the software they purchased is specifically marketed to employers for employee monitoring, those DEA and VA claims should be taken with a grain of salt. But the real story here is probably not about government monitoring at all. It is about the widespread use of spyware in the private sector and its ramifications on personal privacy, identity theft and potential loss of personally identifiable information.

Tweet

(function() {
var s = document.createElement('SCRIPT'), s1 = document.getElementsByTagName('SCRIPT')[0];
s.type = 'text/javascript';
s.src = 'http://widgets.digg.com/buttons.js';
s1.parentNode.insertBefore(s, s1);
})();

(function() {
var po = document.createElement('script'); po.type = 'text/javascript'; po.async = true;
po.src = 'https://apis.google.com/js/plusone.js';
var s = document.getElementsByTagName('script')[0]; s.parentNode.insertBefore(po, s);
})();

The DEA, FDA and VA all purchased a program named eBlaster from SpectorSoft Corp. The program is specifically marketed to employers and parents to monitor all computer activity on the machines which it is installed on. It does this by logging all key strokes, making a record of all websites visited and logging all instant messages sent or received. And it can be installed on virtually any computing device, including smart phones.

This is where the privacy ramifications of the software get very disturbing. First the software can be installed in "stealth mode". That means that even if you are tech-savvy, it would be nearly impossible for you to determine that the program was active on your computer.

Second, all of that information that the program is collecting is stored in a stealthy database. From what I can determine

by reading various reviews of eBlaster, that database can be accessed remotely by whoever installed the software. And if that's not bad enough, the software can be setup to send reports out via e-mail. Since email is normally unencrypted, that means that anyone can read it.

Anyone who follows stories about online privacy knows that information databases are very attractive targets for hackers. That means that if a hacker can determine that a particular employer is using this type of software, its employees could become very attractive targets.

Just think about this. With this type of software installed on your computer, if you do online banking, your account numbers, passwords and logon information could be vulnerable. If you do your taxes on the computer, even if your tax files are encrypted, if you have typed your social security number then your key strokes have been logged. If you have typed your address, the same holds true. Virtually everything required to steal your identity would be stored in a database on your computer and you would have no knowledge of it. And if you make online purchases, then all of your credit card information could be vulnerable too.

In fact, the eBlaster product page boasts that if you use their software, then you will be able to capture passwords.

There is absolutely no doubt that employers have a legitimate need to oversee employees. And many companies and government agencies have data privacy statements in place that specifically tell employees that they, a) have no right to privacy when they use company owned computers for personal reasons and, b) that all of the data accumulated on company owned machines belongs to the company. Simply put, that means that nobody should be recording highly personal information about themselves on computers that they don't own.

Whether or not companies leave themselves vulnerable to law suits for breach of privacy is a question that is still being worked out in the courts. It is a gray area. But I do suspect that if an employee's data is stolen and used by an identity thief, and if the employee can prove that they were vulnerable to identity theft or fraud due to their employer's actions, then the employer is probably liable. At some point, there is likely to be a court case on this issue and it will get ironed out.

And there is very little doubt that what the FDA did - monitoring whistleblowers and then firing them - was illegal. The Supreme Court has already said that whistleblowing is a protected activity under the First Amendment. It is very clear that some employers are taking liberties with their employees' rights.

byJim Malmberg
Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.
Follow me on Twitter:

Follow ACCESS