



Truly Unlimited Calling.
Anyone in the U.S. One flat rate.
Just \$99.99 monthly access*
* ACTIVATION, TAXES & OTHER CHARGES APPLY

verizonwireless

Learn More

post-gazette **NOW**
 Pittsburgh Post-Gazette

Smart phones, big worries

Monday, February 25, 2008

By Elwin Green, Pittsburgh Post-Gazette



Manu Fernandez / Associated Press

Mobile phone handsets are displayed at the Mobile World Congress, in Barcelona, Spain earlier this month. The congress, the largest wireless industry conference, is expected to bring together more than 50,000 industry executives from some 1,300 companies.

You just bought a new smart phone, and it makes you feel so much smarter just for owning it that you can't stand yourself. It does everything, and does it so well, that the PDA your company gave you three years ago seems clunky. Your life would be so much more cool if you could use your smart phone for company business as well as for personal stuff, so you decide to talk to your supervisor first thing Monday morning and offer to return the PDA.

Not so fast, pilgrim.

If your supervisor allows you to conduct company business on your personal smart phone, she could open a Pandora's box of legal and technical issues.

For starters, there is the matter of security. To what extent could company e-mails on your smart phone be accessible to others?

"If you send an e-mail, you're really transmitting an electronic copy of what you type over

the Internet," said Zach Hummel, an employment law attorney and partner in New York-based Bryan Cave LLP. "Usually there is a copy of what you type retained on the phone. There's also a copy that will be on the server of the employer, and then there's a copy that shows up in the inbox of whoever receives it."

There is room for mischief there.

"No system that allows access by a remote device is 100 percent secure, and never will be," said Kim Marcille, who spent 18 years doing IT work for the Miami Herald before forming Possibilities Amplified Inc., a business consulting firm.

The need for security makes Ms. Marcille prefer the BlackBerry to Apple's new iPhone. With the former, she said, "there are security policies that you can set," such as a password, and a timeout setting that will lock the device when it remains idle after a certain period of time. The iPhone, she said, is not "remotely as secure." But its huge popularity almost guarantees that at some point, some employee will ask for, and receive, permission to use it for company business.

"For small businesses, this is a big issue," she said, "because they don't have corporate IT departments" to help make remote devices more secure.

The possibility of intrusion by a third party is not the only security concern that might make a company decide against allowing employees to access company files or e-mails from a personal device. A second issue is the trustworthiness of the employee himself -- especially if something happens to give that employee a reason to do mischief. For instance, an employee who has been laid off could realize later that when he walked out the company's doors for the last time, he brought a large chunk of company information with him, with which he could do considerable harm.

In that regard, a smart phone "is no different than a very, very large briefcase," said Mr. Hummel.

Then there is the issue of privacy. Courts have held that an employee has little or no expectation of privacy in an employer-provided e-mail account, and most employers have policies in place that declare their right to monitor employees use of employer-provided equipment. What happens when the equipment is employee-owned?

Employees are still subject to confidentiality agreements, said Elaine Diedrich of Schnader Harrison Segal & Lewis. Even after an employee leaves, the company can seek legal action to conduct "electronic discovery," a search of his or her smart phone, to make sure that it does not contain confidential information.

E-mails are not the only threat to corporate security. The new devices also can be used to send instant messages, to which large files can be attached. And of course they allow text messaging, or texting.

Texting is especially problematic because text messages, unlike e-mails, do not show up on company servers. By default, they are invisible to the company, so the people sending them could be saying anything, from sharing company information to sending torrid love notes.

Texting also presents a cultural challenge, said John Rostern, a specialist in technology risk management for Milwaukee-based accounting and consulting firm Jefferson Wells.

"The 25-year-olds coming out of college want everything to be available, not on a laptop, but on a cell phone or PDA."

This puts them at odds with the culture of companies in which "most of the regulations and policies and things like that have not kept up with technology."

Referring specifically to such industries as health care and financial services, he said, "The more tightly regulated the environment, the worse the gap becomes."

So when will corporate policies catch up with technology?

Mr. Rostern laughed.

"After the first major breach happens. Unfortunately, we haven't demonstrated, as a species, the ability to look ahead very well."

Mr. Hummel does not see corporate policies ever catching up completely.

"As the technology goes forward, all of us, I don't care where you are, all of us are behind the curve."

Elwin Green can be reached at egreen@post-gazette.com or 412-263-1969.

First published on February 25, 2008 at 12:00 am