

<p>The 18th Annual GENERAL COUNSEL CONFERENCE</p>	<p>June 12-13, 2006 The St. Regis Hotel New York City</p>	<p>www.almevents.com 866.526.6955</p>	<p>ALMEVENTS™</p>
--	---	---	--------------------------

LEGALTECHNOLOGY

Select '**Print**' in your browser menu to print this document.

©2005 Law.com Legal Technology

Page printed from: <http://www.law.com/tech>

[Back to Article](#)

Easy to Use, Easy to Lose

Wayne Smith
Law Technology News
May 24, 2006

Today's mobile devices provide instant, real-time access to firm information: e-mail, Web, contacts, documents, voice messages and even multimedia.

Each new iteration of a smartphone, Research In Motion's BlackBerry, Palm's Treo or Microsoft's mobile device drives ever-increasing capability, richer applications and new options for accessing information inside your firm's security perimeter. Today's handhelds typically come loaded with a variety of connectivity options: USB, Bluetooth, Wi-Fi and now even broadband wireless.

But among legal professionals, there is a tendency to think of PDAs differently than laptops in terms of security and risks to privacy and client confidentiality. We misplace our cell phones all the time right? What's the big deal? The big deal, of course, is that as PDAs become more like notebooks in terms of the ability to access and store firm information, security risks can only increase.

The sheer popularity and portability of such devices make them highly prone to being lost, stolen or compromised. Many people routinely keep personal information on these devices, such as name, address, phone number and possibly even bank account numbers, Social Security number and even private PINs or passwords. The risk of identity theft for the owner of the device becomes a stark reality. Then there is the threat that sensitive client information can also be exposed. This can include e-mail and voice messages, contact lists, appointment information and even electronic documents stored either in memory or on storage cards. As pocket-sized and fully connected mobile devices increasingly adopt all of the capabilities and computing power of laptops, even more of your firm's data can travel outside its walls.

Clients need to know that their private information remains safe and secure, wherever it goes, and we in the legal industry have a responsibility to ensure that this is so.

<p>The 18th Annual GENERAL COUNSEL CONFERENCE</p>
<p>June 12-13, 2006 The St. Regis Hotel ■ New York City</p>
<p>www.almevents.com 866.526.6955</p>

ALMEVENTS™

<p>25th Anniversary</p>	<p>LEGALTECH™</p>
<p>JUNE 5-6, 2006 THE WESTIN BONAVENTURE HOTEL ■ LOS ANGELES</p>	
<p>REGISTER TODAY</p>	
<p>www.almevents.com 800.955.2719</p>	
<p>WEST COAST 2006</p>	

In addition to the risk of PDAs getting into the hands of strangers, there are also the inherent security issues related to PDAs functioning as wireless network clients, either via cellular data service or Wi-Fi connectivity. The challenge of keeping viruses, spyware, hackers and potential data pirates from infiltrating the PDA space can only grow.

So what can be done to secure these devices and to minimize the risk of compromised information? Although data security involves many contexts and variables, and is seldom quick and easy, there are some practical things that firm administrators and users can do to address these inherent risks.

- **Limits and restrictions.** Firms should determine what type of information should never find its way onto a handheld device. This could include such data as social security numbers, passwords and other types of sensitive information. Once protocols have been determined, steps will need to be established to prevent information of this kind from either being synchronized to the handheld or stored by other means.
- **Passwords and locks.** Your firm should require power-on passwords for all handheld devices, and also adhere to prescribed device-locking settings. Although some devices offer auto-locking features, the good news is that all current device platforms provide the ability to secure access to the device itself in some form or another. For example, our current BlackBerry policy sets a password on all devices, locks the device after 10 incorrect login attempts and locks the device whenever it is holstered and after 15 minutes of inactivity. Additionally, a device password is required when a user connects with his/her desktop to synchronize data.
- **Third-party utilities.** In addition to built-in password and auto-lock features, consider purchasing third-party utilities. For example, SureWave Mobile Defense, from JP Mobile, provides basic security options for both the Palm Inc. and Microsoft PocketPC operating systems. One feature, called the "bitwiping bomb," defends against brute force attacks, by wiping all data from memory when a user exceeds the allowed number of login attempts.

Larger firms can take advantage of new products that enforce PDA security policies firm-wide. For example, the latest version of Microsoft Exchange includes tools for administration of mobile devices and connections, and can remotely wipe a Windows PDA if it is lost or stolen.

- **Standardize.** Firms, both large and small, should standardize on a PDA system so that security issues can be addressed in a concerted manner without the added complexity of dealing with disparate systems. Only firm-provided devices should be permitted to access firm data.
- **External threats.** Protecting wireless and Wi-Fi capable handhelds from external threats and attacks is essential. Although viruses targeted specifically at PDAs are rare, under certain circumstances, they can act as carriers that can wreak havoc on connected systems. All of the major anti-virus vendors now have products designed for mobile platforms. In addition, all desktops that are used to synchronize with devices should maintain up-to-date antivirus systems.

Consider installing a firewall on your PDA to prevent unwanted external access. If the device has Wi-Fi capability and you never use it, disable it completely. If you do use it, then protect it with a packet-filtering firewall, such as [Airscanner Mobile Firewall](#) for Windows Mobile Pocket PC from AirScanner Corp.

- **Biometrics.** You may want to consider some form of biometric utility that takes user authentication to the next level. [Safeguard PDA](#) from Utimaco Safeware is one such example. Utimaco's products for Palm Inc., Windows Mobile and Symbian operating systems provide encryption capabilities for stored data and network connections.

Wayne Smith, a member of the Law Technology News editorial advisory board, is manager of information systems at Chester, Willcox & Saxbe, in Columbus, Ohio.