

WIRELESS TECHNOLOGY: LAW PRACTICE WITH “NO STRINGS ATTACHED”

ROSS L. KODNER, ESQ.

©2004 ALL RIGHTS RESERVED

April 14, 2004

It's easy to get tangled in cables, cords, and wires in our high-tech world. Newer equipment lets you unplug and build an efficient, wireless law practice.

Those frustrating cables: They're everywhere! Intertwining and connecting seemingly plug-incompatible gadgets; tangling purses and briefcases; connecting Palm Pilots to PCs, headsets to cell phones, printers to laptops; stretching to scanners; coiling around chair legs to connect PC networks. Enough!

It's time to banish the cable headache once and for all. Wireless technology is the remedy. Wireless devices are becoming commonplace: From network connections for our laptops and Palms to wireless earphones for our cell phones, wireless e-mail, and wireless Internet access at coffeehouses, we're walking in a wireless wonderland-and just in time.

What kinds of wireless devices make sense for lawyers? Many devices and applications are available for firms of all sizes and all practice types. Several key wireless technologies recently have morphed from de rigueur luxuries into must-haves.

Different methods for wireless connections-including wireless Ethernet (also known as "WiFi")

and its short-range cohort, Bluetooth technology-have appealing features that may serve you well. Most law firms with multiple PCs network them together to share data, programs, and peripherals such as printers and backup systems. Traditionally, this network has involved an interconnecting device, typically referred to as a "hub" or a "switch," and cables that connect the device to the PCs. Lawyers who work in firms that planned ahead and installed network cable outlets in their offices can sit and work, connected to their networks (and through them to the Internet), at any of these "cable points."

But what happens when a lawyer wants to sit in the library or the firm's kitchen area and work on his or her laptop or surf the Net? What if there aren't any cable points there? Then there is no practical way to access network documents, calendars, the Internet, or even e-mail from that point in the office. Today, that just isn't acceptable.

Switch gears and consider your home. In many families, several members have their own PCs. Add a speedy cable modem to access the Internet, and you end up with a logjam: Everyone in the household wants to access the Net at the same time. Spending hundreds, if not thousands, of dollars to run network cabling in an existing home is not an appealing option. In the interest of family harmony-if not just plain convenience-finding a way to share Internet connections and printers wirelessly becomes a necessity.

TECHNOLOGY WHOSE TIME HAS COME

Wireless networking technology isn't new. Until recently, however, none of the methods for connecting PCs without cables has been very workable, reliable, or affordable. The advent of a new generation of wireless network technology based on the ubiquitous Ethernet system brought

a new era for wireless connectivity. Many information technology experts predict that systems that use some version of WiFi may eventually outnumber those that rely on cords.

WiFi is the most popular wireless networking technology. A cableless derivative of the tried-and-true Ethernet network, it is now standard equipment in many laptops, as well as in some printers, personal digital assistants (PDAs), and liquid crystal display (LCD) projectors. The technology is successful because, well, it actually works.

The most common form is called "802.11b." This system sends and receives information via a device called a "wireless access point" at 11 megabits per second (mbps). Some systems are capable of "turbo" mode at double that speed. If you purchased a laptop with wireless capability in the last two years, it most likely follows the 802.11b transmission standard. Practical operating ranges extend to about 1,000 feet under perfect conditions, but ranges are actually more like 200 feet inside a building-more than enough to take a laptop outside onto the deck at home or into an office conference room.

'WiFi' technology is now standard equipment in many laptops, as well as in some printers, personal digital assistants, and even LCD projectors. It is successful because, well, it actually works.

A wireless access point is a small box that connects to your existing network. It enables the whole network (meaning all PCs on the network, including those without wireless capability) to communicate with the wireless-equipped devices. Some access points, often those designed for home use, also incorporate a "router" to allow shared access to a cable modem or DSL Internet connection, [plus standard network hub capabilities to interconnect cabled network components

as well.] They sometimes include Internet firewall capabilities as well.

Popular makers include Linksys, D-Link, U.S. Robotics, Netgear, Orinoco (Lucent Technologies), Cisco, 3COM, and Microsoft. Typically, a wireless access point with a cable/DSL router and network hub will cost between \$90 and \$200 for home units and as much as several thousand dollars for high-capacity, high-security units intended for large offices.

The next piece of the puzzle is the wireless "card"-the component either built into or added to a PC or printer so that it can communicate with the wireless access point. More and more laptops, and even several high-end PDAs , have built-in wireless capability that generally follows the 802.11b standard. A wireless PC card can be added to a laptop for between \$50 and \$150. For desktop PCs, the options are internal "peripheral component interconnect" (PCI) cards or external "universal signature bus" (USB) wireless adapters, which cost between \$50 and \$125.

It is also possible to wirelessly connect printers, scanners, and other equipment that has Ethernet capability, using a device called a "wireless bridge," offered for about \$100 by companies such as Linksys.

SECURITY: ALWAYS AN ISSUE WITH BITS AND BYTES FLOATING THROUGH THE AIR

Security is always an issue with a network-even more so when all those bits and bytes float through the air. The 802.11b standard uses a security system called "wired equivalent privacy" (WEP). Unfortunately, this system has been shown to be penetrable; nevertheless, it is still far better to use it than not.

Also, every wireless network has a "service set identifier" (SSID)-that is essentially a code exchanged between the wireless access point and the PCs trying to connect with it. It is critical to set the SSID on a new wireless access point (and on the PCs connecting to it) to something other than the default setting. At a minimum, this can prevent unauthorized users from "leveraging" you wireless network connections. ["leveraging" = stealing!]

The newer 802.11g systems have far more sophisticated security capabilities. While some clever hacker may someday demonstrate that the security of the "g" system can be broken, it hasn't happened yet (at least that we know of). This-along with connection speeds nearly five times faster than systems using the 802.11b standard-is a compelling reason to invest in a "g" system.

More and more manufacturers of electronic devices are embedding WiFi capability into an ever-widening array of products. Wireless access points in public locations are multiplying rapidly. Hotels are investing in 802.11b technology to create wireless zones in their properties, a less costly option than running cables to every guest room to provide guests with high-speed Internet access. Many Starbucks locations around the country offer a version of 802.11b access, with online charges offered daily or by monthly subscription.

Services like Boingo (www.boingo.com) offer a flavor of 802.11b at hundreds of access locations nationwide. Laptop-maker Toshiba has teamed up with Circle K convenience stores to offer wireless zones. Expect to see more 802.11b access points nationwide (even some McDonalds locations offer wireless access - Big Macs and WiFi - weird but true).

SHORT-RANGE CONNECTIONS: THE BLUETOOTH APPROACH

WiFi is not the only wireless system for connecting electronic gizmos. A standard called Bluetooth—a short-range transmission system intended for connecting personal devices into what some have referred to as a personal area network (PAN)—has been in the offing for years and is now coming to fruition.

Bluetooth devices have a transmission range of about 30 feet. Capabilities include cordless communication between an earphone/headset and a cell phone. The technology can also enable a cell phone and a PDA to "talk" to each other when they're in range and automatically synchronize their contact lists. A Bluetooth-enabled PDA can print to a Bluetooth-equipped laser printer. Future possibilities might include synchronizing a PDA's street map software to a Bluetooth-equipped car's in-dash navigation system. In fact, the 2004 Acura TL is the first auto available with Bluetooth capabilities - linking certain Bluetooth-enabled cellphones to the car's hands-free system. Expect more Bluetooth options to come.

Another tool for short-range wireless connection is infrared (IR) technology (the system that makes remote controls work), which has been available in PCs for some time. Most PDAs have an infrared system that can be used to beam information between two handheld devices or to connect a PDA and a PC, without cables, to synchronize information. Some printers also have IR capability, allowing an IR-equipped laptop or PDA to print without a bulky parallel cable or USB connection.

IR technology is convenient, but it is also very short range and requires a direct line of sight between connected devices. Bluetooth and WiFi are radio frequency transmission systems that require no direct line of sight.

THE WIRELESS NET: CUTTING THE LONGEST CORDS

Wireless technology is going a step further into the realm of portable Internet and e-mail access. Web access and paging systems that work like cell phones have been available for some time, but only recently at speeds fast enough to make the effort worthwhile.

Using the platform of 2.5G and 3G cell transmission systems, companies like Verizon are offering relatively high-speed wireless Internet access in a growing number of metro areas around the country. This access uses a PC card with an antenna-and really does work. However, it requires a monthly fee, and coverage areas are limited. Expect this approach, with its costly infrastructure, to lose out to much more economical WiFi access points in many public locations. In the meantime, if you often need Internet access when you're away from your PC, these systems are worth exploring.

Devices that look like traditional alphanumeric pagers or PDAs have become popular for paging and sending e-mail wirelessly. Devices made by RIM Technologies feature a thumb board on which users enter text, meaning you type with your thumbs. (Although it sounds silly, it's possible to become quite speedy.) Likewise, the well-known BlackBerry device, manufactured by Research in Motion, Ltd., can send and receive Internet e-mail and provide PDA-like functions using a software system like the one in the manufacturer's e-pager devices. Costs range from \$300 to \$600, with monthly service fees from \$20 to \$60.

A comparable product called the G100 from Good Technology is a notable BlackBerry competitor, with service offered by Cingular Wireless. Law firms that use Microsoft Outlook and

Exchange Server software may find this product's cradle-free, real-time synchronization attractive.

From WiFi and Bluetooth wireless Net and Blackberry e-mail, wireless technology is growing explosively. The lure of a cordless world is one that few can resist, and one that all well-connected lawyers should explore.