



Ross Ipsa Loquitur

A Wisconsin Law Journal Bi-Monthly Column

Wireless Security: Newest Oxymoron?

By

Ross L. Kodner

August 2004

It is not uncommon for the “average” lawyer today to have a wireless-equipped laptop, as well as a home wireless network. More law offices have setup wireless “zones” in conference rooms, libraries and break rooms. At home, families often have more than one computer, all competing for internet access via wireless networking, or WiFi. With second-generation 802.11g wireless that connects at faster speeds, the usefulness of what can be accomplished untethered, has soared.

Lawyers use WiFi connections in coffeehouses and bookstores. Lawyers use WiFi connections in densely populated high-rise buildings: home and office. Lawyers use home WiFi connections, within shouting distance of neighbors who are also WiFi'd. All good? Certainly if your mantra is: “practice anytime, any place.” For some “wireless = more billables.” Quality of life issues are a different matter as more of have found that an “always on, always connected” approach to law practice and life has a serious downside. Good for business, rough in the “pretending to have a life” category. But wireless is here, it is an inseparable part of the fabric of modern computing for ourselves, our clients and our families; it is not going away.

This article is not a technical primer on wireless law practice. The purpose here is different. Bits and bytes of confidential client information and private firm data are beamed about in the ether. The possibility for malicious interception at worst, and nuisance-level mischief at best, are real threats.

Lawyers may connecting through “secure” Internet-based remote access systems. They may not be as secure as they think. Picture this: lawyer working in the evening at home on a laptop. She's on the couch with her family, connected to her office network, entering time slips and editing client documents. She logged in through a secure VPN her office provided. But the 60' feet between her laptop and Internet connection are “open” - she's wirelessly connected.

Ross Ipsa Loquitur

A Wisconsin Law Journal Bi-Monthly Column

Page 2

Anyone downloading free Netstumbler (netstumbler.com), an application that “sniffs” for nearby WiFi wireless signals, can find her connection. Odds are high that the lawyer’s laptop has no software firewall protecting it and that her wireless network has few if any security functions active. Even with wireless security “on” - a “WEP” or “WPA” key, software called Aircrack (from <http://aircrack.shmoo.com>) has a good shot at “unlocking” that “security.” Intercepting the wireless signal to “piggyback” for free Internet access may be the aim of this breed of hacker, known as “wardrivers.” However, a “wardriver” of sufficient sophistication, finding an unprotected laptop can exploit it. Invisibly, the wardriver becomes the “lawyer” and “see” what she sees: the contents of her laptop hard drive. But as frightening as that seems, it’s actually worse.

If she has a secure connection to her office network, so does her new invisible wardriving buddy. He’s now on the law firm or corporate network, with the access rights she has. Anything he does will look like she did it - because “he” is “her” for the purpose of this intrusion. Confidential client information is compromised. Firm data is exposed. Neither the lawyer nor her firm would know it happened. Exposure to malpractice claims based on disclosure, and certainly ethical violations is very real. You should be terrified - that would be well-founded.

Other wireless exploitation: Perhaps you sync your Smartphone’s PDA functions with your office network or laptop. You may tote “portabilized” client work product, your confidential rolodex, client lists, etc. And if your Smartphone or cell phone has Bluetooth wireless capability, any other Bluetooth phone or laptop within 30 feet can access that information - totally clandestinely - no trace, no footprints, no warnings. It’s called “Bluesnarfing” (see “Nokia admits multiple Bluetooth security holes,” ZD Net UK, February 9, 2004 at <http://news.zdnet.co.uk/communications/wireless/0,39020348,39145886,00.htm>).

The law practice risk and danger of Bluetooth security cannot be overestimated. A scenario: you’re taking a deposition. Both you and opposing counsel (or her expert) have Bluetooth phones. You have your to-do list synch’d to your Smartphone phone. In the list is an entry stating: “Push for settlement based on client’s million dollar exposure because of the damaging e-mail that will be discovered.” What if opposing counsel or their expert were to “bluesnarf” that entry?

What can you do to protect yourself from wireless intrusion? No security approach is perfect, but precautions must be taken. Here are a few:

For Wireless “WiFi” Connections:

* Wireless laptops absolutely must have software firewalls (such as Symantec Corporation’s Norton Internet Security or Zonelab’s ZoneAlarm Pro). Windows XP users note: the built-in “Internet Connection Firewall” does not fall into the “better than nothing category.” Why?

Ross Ipsa Loquitur

A Wisconsin Law Journal Bi-Monthly Column

Page 3

Consider the oxymoronic state of the phrase: "Microsoft Security" - it doesn't cut the security mustard.

* Activate security functions of the wireless access point (WAP) through which you connect. Most WAPs ship with ALL security functions turned off. Consumers and IT professionals should demand the opposite condition - security all turned ON and it being up to us to scale it back. Turning on security means:

- 1) Changing the SSID - change the unique identifier name of the WAP from the factory default to anything else.
- 2) Set your WAP's "Administrative Password" - Changing the administrative password can bar intruders from accessing the setup functions of the WAP and turning off your security.
- 3) Use Wireless Encryption - The "old" approach, called "128 bit WEP" (Wireless Equivalency Privacy) is "better than nothing," although has been proven "breakable." The newer "WPA" encryption is preferred, if your WAP device supports it. You assign a "network key" that must be provided by anyone trying to wirelessly connect to your WAP - the more characters the better the protection (the harder it becomes for a WEP key-breaker like Airsnort to figure out the key).
- 4) Limit Access by MAC Address - Inconvenient if you have wireless guests who share your Internet connection from office conference room. This is a table stored in the WAP that holds the unique network adapter addresses specific to your authorized wireless users. No one else should be able to connect.
- 5) Consider Stopping SSID Broadcasting - WAPs normally digitally shout to potential wireless users "My name is "SMITH WIRELESS NETWORK! Connect here!" Turning off SSID broadcasting makes it harder for intruders to find your wireless connection (but doesn't affect permitted users who know what SSID to look for).
- 6) Say No to Wireless Signal Boosters - Resist the crop of wireless "signal boosters." If you need to wirelessly connect from a longer distance, security "best practices" says you should establishing a closer WAP. Signal boosters create a wider "Circle of Wireless Destruction." Intruders can connect from relatively far away - even another floor in an office building, or down the block at home.
- 7) Self-Hack or Know a "Good Hacker" - Download a copy of Netstumbler and check to

Ross Ipsa Loquitur

A Wisconsin Law Journal Bi-Monthly Column
Page 4

see if you can “see” your own wireless connection (from a system which has wireless capability but is NOT setup to access your now-secured WiFi connection). If you “see” it, others can too; more “tweaking” is required. If this sounds cryptic, employ a security expert to audit the wireless firm and home connections.

- 8) WiFi connections in Public Hotspots - go to No. 1 and be firewalled and consider not accessing any secure office or client systems you would not want to be exploited by the latté drinker at the next table.

For Bluetooth Owners: Beware Bluetooth - learn to turn off your Bluetooth functions on any equipped laptop or phone. force yourself to develop a habit of doing so in any public place. Bluetooth security is just coming to the forefront, but it's not mainstreamed (e.g. <http://www.thewirelessdirectory.com/Bluetooth-Software/Bluetooth-Security.htm>). Bluetooth-equipped cell purveyors are just waking up to the issue (see, “Nokia releases 'invisible' Bluetooth security fix,” ZD Net UK, July 22, 2004 at <http://news.zdnet.co.uk/internet/security/0,39020375,39161309,00.htm>).

The bottom line: wireless law practice is here to stay, Wireless security risks abound, but are manageable. Securely accessing confidential client and firm information doesn't happen “magically.” Rather, only enlightened awareness, proactivity and prioritization of data security will protect lawyers and their clients. Wireless security, as with most law practice electronic security issues, may be three parts technology, but it is most certainly at least one part attitude.

Ross Kodner is a “recovering lawyer” who saw the light and founded Milwaukee, Wisconsin's MicroLaw, Inc. a legal technology consultancy and CLE education company. He consults with and teaches lawyers worldwide about technology. He can be reached at rkodner@microlaw.com, via www.microlaw.com and at 414-540-9433.