Using Public Wi-Fi Hotspots Can Land You in Hot Water by Risking Disclosure of Confidential Information

by Richard L. Ravin

The ability to access the Internet at hotels, airports, cafes, libraries and other public places with wireless devices is enormously convenient, but it comes at a price—a loss of privacy. It is indeed tempting to connect to the Internet via a hotspot to quickly check your email, send a document, or make an online transaction. However, as these Wi-Fi hotspots become ubiquitous, they also are becoming fertile ground for electronic eavesdroppers and spoofers to capture confidential information. Significantly, the interception of such unencrypted transmissions may be perfectly legal, even if such communications include user names, passwords, account numbers, credit card numbers, Social Security numbers, trade secrets and attorney-client privileged communications.

Interception of Wi-Fi Transmissions

Because unencrypted public hotspots use the public airwaves instead of wires for the transmission of communications, they are easily susceptible to being intercepted. Use of unencrypted Wi-Fi networks to send or receive confidential information could result in the unauthorized disclosure of attorney-client privileged communications, trade secrets, or other confidential information that could have serious malpractice and ethical ramifications for attorneys. Moreover, the mere use of such networks could call into question the status of such information as being confidential, privileged or trade secret.

Wi-Fi[1] hotspots are places where local area networks (LANs) are set up using high-frequency radio waves to transmit and receive signals traveling short distances of up to 300 feet (unobstructed, outside), which communicate with notebook computers, smartphones and other wireless devices, enabling users to access the Internet. Wi-Fi, which stands for wireless fidelity, uses a part of the radio frequency spectrum that is not licensed by the Federal Communications Commission.[2]

There are principally two types of activities that make users of public Wi-Fi networks vulnerable—interception (*i.e.*, eavesdropping or receiving) and spoofing. The federal Electronic Communications Privacy Act (ECPA), Title I, amended the Federal Wiretap Act (FWA) to make it unlawful for any person to intentionally intercept or endeavor to intercept any electronic communication.[3] The New Jersey Wiretapping and Electronic Surveillance Act (WESA) proscribes similar conduct.[4] However, both acts expressly exclude interception of radio communications that are "readily accessible to the general public."[5] ECPA provides that a radio communication is readily accessible to the general public if it is not:

> (A) scrambled or encrypted;
>
> (B) transmitted using modulation techniques whose essential parameters have been withheld from the public with the intention of preserving the privacy of such communication;
>
> (C) carried on a subcarrier or other signal subsidiary to a radio transmission;
>
> (D) transmitted over a communication system provided by a common carrier, unless the communication is a tone-only paging system communication; or
>
> (E) transmitted on frequencies allocated under part 25 [for satellites], subpart D, E, or F of part 74, or part 94 of the Rules of the Federal Communications Commission, unless, in the case of a communication transmitted on a frequency allocated under part 74 that is not exclusively allocated to broadcast auxiliary services, the communication is a two-way voice communication by radio.[6]

New Jersey's WESA uses the same definition of "readily accessible to the general public."[7]

Under this definition, intercepting an unencrypted transmission from a Wi-Fi network provided at hotels, airports, cafes, libraries, or other public places, would not be a violation under ECPA or WESA (unless the signal were transmitted using a subcarrier, or transmitted using modulation techniques whose essential parameters have been withheld from the public with the intention of preserving the privacy of such communication). Once the unencrypted radio signals are received by the eavesdropper's computer, its user could perceive any unencrypted or unscrambled information that is contained within the transmission, including confidential emails, attachments and other records. It is important to note that if the Wi-Fi network were provided by a common carrier, such as a telephone company, then the system would not be deemed readily accessible to the general public, and intentional eavesdropping or attempted eavesdropping of such signals would violate the ECPA and WESA.[8]

In 2001, the U.S. Supreme Court[9] implicitly recognized that ECPA prohibits the intentional interception of cell phone conversations.[10] Moreover, ECPA outlaws the manufacture, possession, sale, or sending through the mail of any "device" that is "primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications."[11] Unlike the monitoring of cell phone conversations, the devices used for receiving Wi-Fi communications are not "primarily useful for the surreptitious interception of...electronic communications,"[12] but are computers that are used for numerous other legitimate purposes.

When an employee uses a public Wi-Fi hotspot to transmit company trade secrets or confidential business information without access controls or encryption, he or she risks disclosing such secrets during the transmission, and jeopardizes the status of such information as secret or confidential.

With respect to operating a Wi-Fi network at home or the office, using encryption not only provides a measure of security, it also may make the intentional interception of such communications unlawful. Implementing encryption would give the user of that network a reasonable expectation of privacy, which could require a warrant under the Fourth Amendment before such communications could be intercepted by law enforcement personnel.[13]

Spoofing Wi-Fi Network Users

Another concern for Wi-Fi users is when sham wireless networks are set up to fool or spoof a user into thinking that he or she has logged onto a legitimate public network operated by a nearby establishment. Experts warn, and common sense dictates, that spoofers may be present at public facilities, actively luring unwitting users of Wi-Fi networks into connecting to their counterfeit network, as a way to capture private information.

While sitting at a library, cafe or hotel, for instance, one or more available wireless network connections may appear on your computer screen and seem to be legitimate because the names match or describe your location, perhaps even using the trademark, or a variation thereof, of the facility you think is offering the service (*e.g.*, Rick's Cafe). When the name of the counterfeit Wi-Fi network mimics the name of real network, it is called an evil twin network. In fact, all of the networks at a given location could be fake. Once you log on, the spoofer can monitor all your communications. Spoofing a wireless network can be done with a notebook computer, software that is readily available, and a small USB device to act as the access point. When unsuspecting victims connect with the spoofed access point to make supposedly secure transactions, the spoofer could capture passwords, bank account information and other valuable personal information. Under this scenario, it is unclear whether such conduct would be in violation of the FWA, 18 U.S.C. Section 2511, for the reasons discussed above. However, if the conduct of the spoofer involved unauthorized *access* to the victim's computer, a spoofer could be in violation of Title II of ECPA, which created the federal Stored Wire and Electronic Communications Act (SWEC). Section 2701 of SWEC prohibits intentionally accessing stored communications without authorization.[14]

The conduct of spoofers is distinguished from that of electronic eavesdroppers who receive radio signals without accessing the sender's computer, and thus, do not run afoul of the SWEC.

If a spoofer has accessed the victim's computer without authority, the spoofer may be subject to civil liability for economic damages under the Computer Fraud and Abuse Act (CFAA), providing the loss requirement is satisfied.[15] Under the civil action portion of the CFAA, the loss to the victim's computer'[16] must be $5,000 or more within one year. The term "loss" is broadly defined by statute to mean "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." Of course, such a recovery presupposes the spoofer can be found or identified.

It is noted that with respect to the interception of transitory electronic communications (*e.g.*, emails in route from the sending email server to the destination email server via the Internet), ECPA, Title I,[17] provides that depending on the defendant's conduct, a plaintiff has the right to recover either actual damages plus any profits of the defendant, or statutory damages that are the greater of $100 per day or $10,000.[18] As discussed above, however, the part of an email's journey that travels via an unencrypted public Wi-Fi network would not be protected under ECPA because that part of the transmission would be "readily accessible to the general public."[19]

One of the problems with being spoofed or being the victim of eavesdropping is that when the Wi-Fi user communicates with another computer system, such as his or her employer's network, a spoofer or eavesdropper can capture user names and passwords, and thereby compromise the security of the employer's network. While the snoop may not have been in violation of law when the data was intercepted from the airwaves, clearly if he or she were to later log in to the company's network using the user names and passwords obtained while lawfully eavesdropping, he or she would arguably be committing an unauthorized access of the company's computers, in violation of Section 2701 of SWEC. Further, such conduct could also be contrary to the CFAA.

Wardrivers and Peering Neighbors

While the scenarios discussed above involved Wi-Fi networks intended for use by the public, there are numerous—probably hundreds of thousands—of non-encrypted Wi-Fi networks across the country, operated by private citizens out of their homes and business, but nonetheless available to the public. The laws discussed above do not expressly outlaw accessing of such networks by third parties.

A worrisome problem for unencrypted Wi-Fi networks open to the public is a practice known as wardriving,[20] whereby one drives around in a car with a laptop computer to detect unencrypted Wi-Fi networks. While Internet access is the primary reason why people access Wi-Fi networks in public places, the target of wardrivers, or even unscrupulous neighbors of homes and businesses operating Wi-Fi networks, could be the data residing on unprotected computers attached to the network. Wi-Fi networks in public places, the target of wardrivers, or even unscrupulous neighbors of homes and businesses operating Wi-Fi networks, could be the data residing on unprotected computers attached to the network.

These *open* Wi-Fi networks also could be used by the wardriver or neighbor to send and receive unlawful material such as child pornography, or to conduct other criminal activity. Not only can data be downloaded, uploaded, altered or destroyed, but programs, and even extra computers, can be added to the unsecure network without the knowledge of the Wi-Fi operator. This risk is highest in densely populated neighborhoods and office building complexes. It is noted that the Internet service provider has an interest in minimizing unauthorized access to the Wi-Fi networks, since these users take up bandwidth without paying any fees.

Securing Wi-Fi Networks

Wireless networks lack the inherent security feature of wired networks, which require a physical connection to the network in order to log-on and are usually located within a secure facility, such as a locked building, office or room. Wi-Fi networks do not give the user the ability to unilaterally implement encryption—that must be done by the operator of the network. Choosing the right protection method is important when operating a Wi-Fi network to obtain a proper level of security for the network and the data being exchanged over the network.

Wi-Fi-protected access (WPA) encryption is the preferred method for securing a Wi-Fi network, although the most common form of security is wired equivalent privacy (WEP). Note that the "E" does not stand for encryption. Many within the information technology industry view WEP as less-than-optimal security, because a WEP key can be deciphered without much effort, depending on the bit size, and by utilizing generally available programs. These decoding programs monitor the keys generated by the wireless network that accompany each transmitted packet of information in an attempt to deduce the central key that will allow access to the network. WEP keys are either 5, 13, 16, or 29 characters long, depending on the encryption bit size of 64, 128, 152, or 256, respectively. The longer the key, the more powerful the encryption, and the longer it takes to crack.

Changing the key periodically helps prevent cracking by requiring the would-be hacker to start over. It is generally thought that merely by implementing WEP, at any level, many hackers would be deterred and move on to a non-secure network.

Michel Cukier, assistant professor of mechanical engineering and affiliate of the Clark School's Center for Risk and Reliability and Institute for Systems Research at the University of Maryland, recommends limiting the signal coverage so the signal for the network will not reach outside your home or office, turning off service set identifier (SSID) so your network won't be identified by unwanted users, employing WEP, or even better, WPA, so confidential information is not shared with unwanted readers, frequently changing your network key, or setting your wireless access point so it only accepts known media access control (MAC) addresses, which means that only known computers will have access to the network since a MAC address is essentially a serial number unique to each manufactured, network adaptor.[21]

Alternatives: Using Mobile Broadband and Encrypting Individual Communications

As an alternative to using unencrypted public Wi-Fi networks, many wireless telephone carriers provide broadband access, which is also known as mobile broadband. This system allows users with wireless broadband network adapter cards (either internal or PCMCIA) to access the Internet via cell phone networks. The speeds of access vary depending on the location and whether the particular cell tower being accessed is set up for broadband or slower connection speeds. Because such signals are "transmitted over a communication system provided by a common carrier," interception or attempted interception of such transmissions would be in violation of ECPA.[22] Additionally, assuming the common carrier employs encryption," then use of the encryption itself would be a separate basis for making access of such communications unlawful. More importantly, such communications would be secure and protected from disclosure or interception.

Finally, if open Wi-Fi networks are used to transmit confidential information, then users are advised to send and receive only emails and documents which have themselves been encrypted by the sender, so that even if the communications are intercepted, the information contained within such communications will remain secure. ⚖

Endnotes

1. Wi-Fi is also the registered trademark of Wi-Fi Alliance Corporation, which is a trade organization that sets Wi-Fi standards.
2. Kevin Werbach, Radio Revolution: The Coming Age of Unlicensed Wireless (2003) at 22, 25-28, http://www.werbach.com/docs/RadioRevolution.pdf, accessed on March 6, 2008. The Institute for Electrical and Electronic Engineers (IEEE) standard 802.11a (Wireless-a) uses the 5 GHz band of the public radio frequency spectrum, and standards IEEE802.llb/g (Wireless b/g) use the 2.4 GHz band.
3. 18 U.S.C. §2511.
4. N.J.S.A. 2A:156A-3.
5. 18 U.S.C. §2511(2)(g)(i).
6. 18 U.S.C. §2510(16).
7. N.J.S.A. 2A:156A-2.r.
8. 18 U.S.C. §2510(16)(D); N.J.S.A. 2A:156A-2.r(4).
9. *Bartnicki v. Vopper*, 532 U.S. 514 at 521, fn 4 (2001), *citing* 18 U.S.C. §2511(1)(a).
10. 18 U.S.C. §2511(1).
11. 18 U.S.C. §2512(1)(b).
12. *Id.*
13. *See United States v. Slanina*, 283 F.3d 670, 676-77 (5th Cir. 2002)(employee had a reasonable expectation of privacy in his computer and files where the computer was maintained in a closed, locked office, the employee had installed passwords to limit access, and the employer "did not disseminate any policy that prevented the storage of personal information on city computers and also did not inform its employees that computer usage and Internet access would be monitored"), vacated on other grounds, 537 U.S. 802 (2002); *see Lown v. State*, 172 S.W.3d 753, 761 (Tex. App. 2005); *State v. Moller*, WL 628634 at *6 (Ohio App. 2002), not reported in N.E.2d.
14. 18 U.S.C. §2701 *et seq.*
15. 18 U.S.C. §1030(a)(4), (a)(5)(B)(i) and (g).
16. The affected computer must be a "protected computer," defined by 18 U.S.C. §1030(e)(2), to include one which is used in interstate or foreign commerce or communication (*e.g.*, one connected to the Internet).
17. 18 U.S.C. §2511(1)(a).
18. 18 U.S.C. §2520(c)(2)(A) and (B).
19. 18 U.S.C. §2510(16).
20. wikipedia.org/wiki/Wardriving.
21. Benjamin Fryson, Study: Passwords Alone Not Enough to Keep Wireless Networks Secure, Aug. 23, 2007, www.associatedcontent.com/article/355815/study_passwords_alone_not_enough_to.htm, accessed on Sept. 15, 2007. See also, University of Maryland Study: Password Protecting Your Wireless Network Is Not Enough prnewswire.com/cgi-bin/stories.pl?ACCT=104&STORY=/www/story/08-22-2007/0004649513&EDATE, accessed on Sept. 15, 2007.
22. 18 U.S.C. §2510(16)(D).
23. *See, e.g.*, b2b.vzw.com/govt/security.html, accessed on March 7, 2008: "Verizon Wireless employs Code Division Multiple Access (CDMA) technology that scrambles voice and data information, encrypts signaling messages, and authenticates devices to the Verizon Wireless network to hinder unauthorized users from capturing and deciphering wireless messages."

Richard L. Ravin *is a member of Hartman & Winnicki, P.C., and heads the firm's Internet, intellectual property law, and debtor-creditor rights practice areas, with offices in Paramus and New York City. He is immediate past chair of the New York State Bar Association's Intellectual Property Section, and past (founding) co-chair of the section's Internet and Technology Law Committee. The author gratefully acknowledges the contributions of Shifra Apter, an associate with the firm, and Quentin W. Wiest, a law clerk for the firm, when this article was originally written.*

(Originally published in April 2008.)