By Janice C. Sipior and Burke T. Ward

UNINTENDED INVITATION: ORGANIZATIONAL WI-FI USE BY EXTERNAL ROAMING USERS

Unauthorized users risk civil and criminal liability; Wi-Fi network providers risk system intrusion and disruption.

Paul Timmins and Adam Botbyl stumbled onto an unsecured wireless fidelity (Wi-Fi) network while looking for wireless access points in 2003. Timmins wanted to check his email on his laptop. He later claimed that when he tried to surf the Web, he was routed to a corporate portal of Lowe's, the second-largest home improvement retailer in the U.S. Botbyl then returned with Brian Salcedo to access Lowe's corporate data center, as well as local networks at stores in six states. These roaming users allegedly accessed consumer credit information. The following year, Timmins

Illustration by Richard Downs

pled guilty to a misdemeanor for checking his email through Lowe's network, the first criminal conviction for wardriving in the U.S. He was sentenced to two years probation. Botbyl pled guilty to one count of conspiracy and was sentenced to 26 months in federal prison followed by two years on parole. Salcedo pled guilty to conspiracy, transmitting computer code to cause damage to a computer, unauthorized computer access, and computer fraud and was sentenced to nine years in federal prison.

"Wireless technology," according to [2] "has opened the largest computer network security hole since the advent of modems." The use of Wi-Fi networks is increasing worldwide, projected to reach 707 million users by 2008, according to Pyramid Research. In 2004, approximately 5% of Americans had wireless local area networks (WLANs) in their homes [7]. Here, we compare the perspectives of roaming users and organizational providers who may incur financial costs, be subject to security risks, and potentially be held legally liable for user activity. We characterize types of roaming users in order to analyze the applicability of existing laws enacted before the advent of wireless technology. While protection is provided to organizations for malicious or destructive wireless hackers (whackers), laws are generally favorable to roaming users. In response, we call for a national (U.S.) public policy and ultimately a global solution to the risk of wireless intrusion.

Roaming Users' Perspective	Organizations' Perspective
Convenient Internet access	Operational benefits
Wi-Fi deliberately unsecured for sharing	Economic costs
Enhanced information exchange	Trespass
Enhanced products and services	Violation of ISP user agreement
Raise organizational awareness about security	Violation of legally required security
Add value to society	Security risks
	Security challenges of roaming employees

Table 1. Roaming-user vs. organizational perspective.

Roaming users' views (see Table 1) provide insight into the motivation for, and defense of, roaming use:

Convenient Internet access. Mobile users connect through a wireless access point broadcasting predefined radio-wave frequencies to approximately 300 feet; signal-boosting can increase the distance to nearly 75 miles;

Deliberate sharing. Wireless-capable computers connect to the first available signal. Roaming users are unlikely to view themselves as trespassing or stealing bandwidth; rather, they likely view the signal as having fortuitously entered their airspace;

Enhance information exchange. The core benefits of convenience, timeliness, flexibility, and frequency expand public discourse, resulting in the characterization of the Internet as "one of the core and noblest of American ideals: the free and open marketplace of ideas" [4];

Enhance products and services. Mobile commerce changes products and services; among its consumer concerns is limited availability of wireless connections, according to the U.S. Federal Trade Commission;

Raise organizational security awareness. The activity of wardriving, or driving in an automobile to seek out open wireless access points, and warchalking, or marking the physical location of wireless access points, force organizations to confront security shortfalls; and

Add value to society. Robert Metcalfe, inventor of Ethernet network technology, says, "Connected computers are better. Having the only telephone in the world would be of zero value, but this value increases for each new telephone it can call."

Providers of wireless access are responsible for proper management of this resource. Organizations may see operational benefits (see Table 1) but also have concerns:

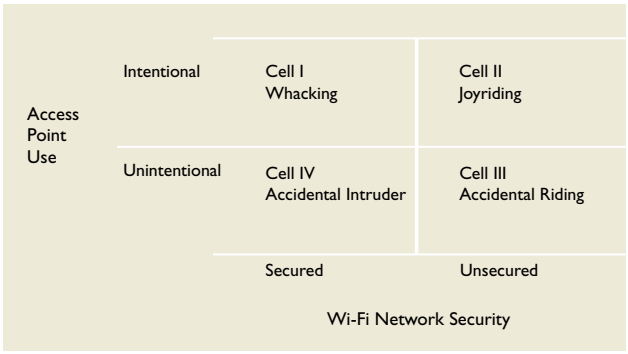
Operational benefits. A majority of corporate respondents to a 2005 survey reported using basic applications, including wireless email, Web browsing, and intranet, as indicated by 89%, 86%, and 81% of them, respectively [10]. Corporations also realize reductions in transaction costs and time and geographic limitations afforded by wireless connectivity for key applications (such as mobile supply-chain management and enterprise resource planning applications), as reported by 49% of respondents [10]. Further expanding wireless connectivity could bring about a new ubiquitous economic environment;

Economic cost. Organizations bear the financial cost of providing wireless service. The Wi-Fi hotspot services market is projected by consulting firm Frost & Sullivan (www.frost.com) to reach $1.4 billion in revenue by 2009 [3]. Organizations also bear the costs associated with unauthorized roaming-user activities (such as theft of service and trespass). Additionally, customer confidence, as reflected in an organization's ability to protect the

privacy of its customers' information, can be lost;

Trespass. Roaming users may arrive uninvited to avail themselves of free Internet connectivity. Additional use of bandwidth could slow performance of key applications that rely on WLANs. Diagnosing inferior performance and identifying unauthorized users burden support departments. Legal protections against trespassing are covered in the analysis of the common law tort called "trespass to chattels," or personal property;

Violation of the Internet service provider user agreement. More roaming users could increase Internet use beyond planned levels, and ISPs may lack the infrastructure to support unplanned use. Moreover, sharing may discourage otherwise potential new subscribers. In response, ISPs may disallow sharing and even "signal leakage," or signals broadcast beyond an organization's facility, within the terms of the use agreement. However, roaming users cannot read the agreement and are therefore unable to determine whether connection sharing is allowed;



Types of roaming use.

Violation of legally required security. Security cannot be guaranteed should uninvited roaming users arrive. This risk is especially critical in industry sectors regulated by security provisions in laws (such as the Health Insurance Portability and Accountability Act of 1996 and the Sarbanes-Oxley Act of 2002). For example, section 404 of Sarbanes-Oxley requires publicly held companies to annually evaluate financial reporting controls and procedures. An unsecured WLAN used by unknown roaming users or employees working from home would violate security requirements;

Security risks. Wireless networks are subject to security challenges (such as eavesdropping, traffic analysis, masquerading, replay, message modification, and jamming), according to a report by the U.S. Government Accountability Office (GAO). Unauthorized roaming users can obtain proprietary data, passwords, and other organizational information. Organizations may be liable for exploitive activities (such as document perusal, port scanning, and spamming); and

Security challenges of roaming employees. Employee use of public wireless networks can expose organizational communications to "man-in-the-middle" attacks; for example, a whacker using a wireless tool can capture an entire wireless session, including user log-in, if the user is not using a secure sockets layer connection [8]. Employees working from wireless home networks may not have enabled their security features; it's been estimated that about 80% of U.S. residential wireless networks are unsecured [5]. However, even with security enabled, "WiFi is vulnerable to hacking," according to [1].

Types of Roaming Wi-Fi Users

We characterize unauthorized roaming use along two dimensions—intentional or unintentional access and secured or unsecured Wi-Fi networks—when determining whether such use is legal. The four combinations result in Cells I–IV (see the Figure here):

Cell 1 (Whacking). Intentional access of secured wireless networks. Whackers may engage in destructive, malicious, theft, espionage, or entertainment activities. Organizations and ISPs could be liable for unwittingly partaking in illegal activities (such as spamming, sharing copyrighted files, accessing pornography, port scanning for vulnerable services on an Internet host, stealing, modifying, deleting, or viewing data, and otherwise causing harm;

Cell 2 (Joyriding). Intentional access of unsecured wireless networks. Joyriders are roaming users who intentionally access an unsecured wireless network without express prior consent. Indeed, a survey of 228,537 access points worldwide by participants in the 2004 "WorldWide WarDrive" (www.worldwidewardrive.org) revealed that only 38.3% had enabled wired equivalent privacy (WEP), a native security mechanism in the 802.11 WLAN standard. The GAO reported that a test of six federal agencies detected signal leakage at all six and that 13 of 24 major federal agencies do not require Wi-Fi networks to be secured;

Cell 3 (Accidental riding). Unintentional access of unsecured wireless networks. When unintentionally connecting to an unsecured Wi-Fi network, accidental riders may not realize the connection was made or believe it was made through their own networks; for example, the Microsoft Windows XP operating system contains a "zero configuration" feature to facilitate connecting to Wi-Fi networks, but this feature can also cause a user to connect unintentionally. Such use does not constitute "intentional" access required by most statutes; and

Cell 4 (Accidental intruder). Unintentional access of secured wireless networks. Accidental intruders "accidentally" or unintentionally gain access to a secured network. Such access is unlikely because a secured network would likely prompt for a username and password for user authentication, alerting the user to the presence of security. Such access could result from a security flaw.

Wardriving and warchalking. Wardrivers are not a type of roaming user, based on the narrow definition (limited to access-point identification) provided by the wardriving community [6]. U.S. Federal Bureau of Investigation agent Bill Shore unofficially warned in 2002 that identification of access points may not be illegal, but actual access may be a criminal violation of the Federal Computer Fraud and Abuse Statute, Theft of Trade Secrets, and other federal statutes. Wardriving may lead to warchalking, which may indeed constitute an invasion of the provider's privacy. Chalking the location of an open access point, without authorization, has been compared to placing a sign in front of a home that says "This door is unlocked; there is no security" [9].

	Wardriving	Cells			
		I	II	III	IV
Federal Law					
Computer Fraud and Abuse Act	NA	Yes	Possible	Unlikely	Unlikely
Electronic Communications Privacy Act	NA	Yes	No	No	No
State Laws					
Prohibition of Access to Networks	NA	Uncertain	Uncertain	Uncertain	Uncertain
Theft of Services	NA	Yes	No	No	No
Prohibition of Interruption or Degradation of Services	NA	Possible	Possible	Possible	Possible
Prohibition of Interception of Communications	NA	Possible	No	No	Unlikely
Prohibition of Facilitation of Access to Networks	Yes	Uncertain	Uncertain	Uncertain	Uncertain
Common Law					
Trespass to Chattels	NA	Possible	Possible	Unlikely	Unlikely

Table 2. Applicability of U.S. law to wardriving and roaming use.

Is It Legal?

The legal protection of an organization's Wi-Fi network from unauthorized roaming use is unclear. Legal acceptability depends on whether roaming use is an intentional intrusion by the user and unauthorized by the provider. However, what constitutes intentional and unauthorized Wi-Fi access is not explicitly defined by most legal jurisdictions.

We focus primarily on protections from joyriders and accidental users—Cells II–IV in the figure. Existing laws apply to whackers—Cell I—in the same way they apply to a hacker who intentionally gains unauthorized access to a network, whether wired or wireless, making whacking illegal. The results of our analysis are outlined in Table 2.

Federal law. Applicable federal laws include the Computer Fraud and Abuse Act (CFAA) of 1986 and the Electronic Communications Privacy Act (ECPA) of 1986, both enacted before wireless technology came into widespread use.

The CFAA, which prohibits intentional, unauthorized access to a computer, appears to apply to Cell I (whackers) and Cell II (joyriders who engage in a high volume of downloading); Cells III and IV are not included because such users lack intent. The CFAA requires the standard of "wrongful intent" by the user, among other legal criteria. For subsection 1030(a)(5)(A)(i) to be applicable, a user must "intend" to cause damage; it would seem this section applies only to whackers (Cell I), whose activities are damaging. However, joyriders (Cell II) may also fall within this realm if excessive file downloading resulted in, say, damage exceeding the required minimum of $5,000 over the course of a year. The cost of excessive use includes bandwidth and processing power, coupled with costs related to slowed performance for other users (such as customers).

The ECPA, which prohibits intentional unauthorized interception of encrypted communications, may apply to whackers (Cell I). Whackers who intentionally access secure Wi-Fi networks and encrypted content may be subject to federal penalties. The ECPA does not apply to Cell II (joyriders) and Cell III (accidental riders) using unsecured Wi-Fi connections with no encryption capabilities enabled. Similarly, the ECPA does not apply to Cell IV because accidental intruders lack the legal intent criterion.

Meanwhile, various state criminal statutes supplement federal law, prohibiting access to networks, theft of service, interruption or degradation of service, interception of communications, and facilitation of access to networks (see Table 2). As with the CFAA, intent is often a key element in legally determining whether a criminal violation was committed by a roaming user.

In state common law, uninvited roaming users could be trespassing. According to the common law Restatement (Second) of Torts, ß 217, "[a] trespass to chattel, [or personal property], may be committed by intentionally:

(a) dispossessing another of the chattel; or
(b) using or intermeddling with a chattel in the pos-

session of another."

Trespass to chattels has not been applied to roaming use but could be applied to all types of roaming users in a future criminal prosecution.

Recommendations for Roaming Use

Table 3 outlines our own recommendations for roaming use. "Security is the paramount concern in evaluating any...wireless offering" [11]. Security measures include encryption software, firewalls, authenticating user devices, and virtual private networks for password protection. However, the three main security protocols—WEP, Wi-Fi Protected Access and Extensible Authentication Protocol, and Cisco Systems' proprietary implementation Lightweight EAP, or LEA—have all been hacked [1]. Periodic monitoring of security measures detect unauthorized devices, inappropriate communications, and signal leakage to help assure compliance with ISP user agreements and security provisions in the law. Training and support for employee use from home and while in transit is fundamental to securing home networks and portable access devices. Acceptable use of publicly accessible Wi-Fi should state what information may be communicated. An enterprisewide wireless plan should provide standardization, allowing improved implementation, management, and support.

Organizations
Implement enterprisewide Wi-Fi plan
• Install a firewall
• Install encryption software
• Authenticate approved user devices
• Implement a virtual private network
• Monitor security periodically
• Comply with ISP user agreement
• Comply with security provisions in laws
• Train roaming employees:
o Secure access of organizational systems and data
o Secure portable access devices
o Define use of publicly accessible Wi-Fi
Roaming Users
• Access only publicly accessible Wi-Fi
Public Policy
• Encourage ubiquity in publicly accessible Wi-Fi
• Do not hold users responsible to ascertain public accessibility status of Wi-Fi
• Hold organizations responsible for securing proprietary Wi-Fi

Table 3. Recommendations for roaming use.

It may seem to roaming users that the burden of responsibility should be on the broadcaster, since wireless devices may access the first signal detected. Such access is unintended but could become intentional, with unclear legal consequences to the user.

Ubiquity in publicly accessible wireless networks must be encouraged to increase value to society. Roaming users should not be responsible for determining whether a connection is achieved through a public or private network. Wi-Fi network providers should be responsible for reasonably managing their resources and protecting against unauthorized use.

Conclusion

We would all be better off with open Wi-Fi access, facilitating greater mobility, information access, and efficiency. This position is unobjectionable as long as public use is intended. Unauthorized use can subject roaming users to civil and criminal liability. Organizations are exposed to potential system disruption and degradation, increased costs, security risk, and liability to third parties. National legislation, and ultimately a global solution, must therefore balance the competing interests of roaming users vs. the proprietary rights of organizational Wi-Fi network providers. C

References

1. Berghel, H. and Uecker, J. WiFi attack vectors. *Commun. ACM 48,* 8 (Aug. 2005), 21–28.
2. Berghel, H. Wireless infidelity I: War driving. *Commun. ACM 47,* 9 (Sept. 2004), 21–26.
3. Frost & Sullivan. *Free Hotspots Restrict Revenues for Wi-Fi service Providers.* Presss Release, July 30, 2003; www.frost.com/prod/servlet/press-release.pag?docid=5115637&ctxixpLink=FcmCtx6 &ctxixpLabel=FcmCtx7.
4. Goldsborough, R. Leveraging the Internet's marketplace of ideas. *Tech Directions 64,* 5 (Dec. 2004), 9.
5. Hines, M. Worried about Wi-Fi security? CNET News.com (Jan. 19, 2005); news.com.com/Worried+about+Wi-Fi+security/2100-7347_3-5540969.html.
6. Hurley, C., Puchol, M. (Ed.), Rogers, R., and Thornton, F. *WarDriving: Drive, Detect, Defend, A Guide to Wireless Security.* Syngress Publishing, Inc., Rockland, MA, 2004.
7. Kapica, J. Consumers still hazy on Wi-Fi facts: Study. Globeandmail.com, a division of CTVglobalmedia Publishing, Inc., Toronto (Feb. 25, 2004); www.globetechnology.com/servlet/story/RTGAM.20040225.gtWi-ifeb25/ BNStory /Technology.
8. Mullins, M. Be aware of wireless threats. *TechRepublic,* a CNET Networks site (Oct. 21, 2005); insight.zdnet.co.uk/communications/wireless/0,39020430,39232729,00.htm.
9. Ryan, P. War, peace, or stalemate: Wargames, wordily, wardriving, and the emerging market for hacker ethics. *Virginia Journal of Law & Technology 9,* 7 (Summer 2004), 1–57.
10. Webb, R. The untethered business. *Communication News 42,* 3 (Mar. 2005), 50.
11. Zenel, B. and Toy, A. Enterprise-grade wireless. *Queue 3,* 4 (May 2005), 30–37.

Janice C. Sipior (janice.sipior@villanova.edu) is an associate professor in the School of Business at Villanova University, Villanova, PA. **Burke T. Ward** (burke.ward@villanova.edu) is a professor in the School of Business at Villanova University, Villanova, PA.