Washington Journal of Law, Technology & Arts

Volume 1 | Issue 3 Article 1

8-2-2005

Will Wi-Fi Make Your Private Network Public? Wardriving, Criminal and Civil Liability, and the Security Risks of Wireless Networks

Anita Ramasastry
University of Washington School of Law

Jane Winn
University of Washington School of Law

Corporate & Commercial
Cite as: Anita Ramasastry, Jane K. Winn and Peter Winn, *Will Wi-Fi Make Your Private Network Public? Wardriving, Criminal and Civil Liability, and the Security Risks of Wireless Networks*, 1 Shidler J. L. Com. & Tech. 9 (Aug. 2, 2005), *at* <http://www.lctjournal.washington.edu/vol1/a009ramasastry.html>

WILL WI-FI MAKE YOUR PRIVATE NETWORK PUBLIC? WARDRIVING, CRIMINAL AND CIVIL LIABILITY, AND THE SECURITY RISKS OF WIRELESS NETWORKS

By Anita Ramasastry, Jane K. Winn and Peter Winn[1]

ABSTRACT

Wireless networking is growing in popularity because it is often cheaper and more convenient than other computer networking systems. Wireless networks, however, are also very hard to secure. Locating insecure wireless networks and advertising their locations is an activity known as "wardriving." Exploiting the vulnerability of a wireless network to hack into the computer system or to monitor the wireless transmissions can give rise to liability under federal felony and misdemeanor statutes, as well as federal civil liability and liability under state law private causes of action. When introducing wireless networking into business information systems, system administrators should use all possible care to secure the network, and IT policies and practices should be updated to make sure that wireless networking risks that cannot be eliminated through technology are managed prudently.

Table of Contents

INTRODUCTION

<1> Wireless networking is growing in popularity because it can be cheaper and more convenient than other systems for networking computers. But replacing old-fashioned wires with new wireless connections may undermine whatever security once protected a network. The security problems of wireless networks are so widespread that finding unprotected networks and publicizing their vulnerability has now become a sport among computer geeks and hackers known as "wardriving." [2]

<2> Some forms of wardriving may be perfectly legal. Some wireless networks, such as community networks, are deliberately left open and so welcome detection by members of the public. Other networks, even though not left open to the public, may be inadvertently left unsecured and subsequently discovered quite by accident. While the inadvertent accessing of an unsecured network does not constitute a crime, so-called war drivers do not "accidentally" access wireless networks. They actively seek them out, and they do not ask or obtain permission to publicize network locations or to access the networks.[3] Under these circumstances, wardriving has criminal implications.

<3> Wi-Fi (or wireless fidelity) is currently the most popular form of wireless networking technology and is based on a standard developed by the Institute of Electrical and Electronics Engineers (IEEE) known as 802.11b. Mobile computing devices such as laptop computers or personal digital assistants (PDAs) can gain access to a local area network using radio signals to share data in lieu of a fixed wire connection.

<4> In recent years, wireless local area networks (WLANs) connecting personal computers have grown in popularity because prices for wireless technology have fallen sharply. Wireless networking has become a cost effective alternative to more traditional wired networks. The true cost of using wireless technology may not be apparent, however, unless the costs of securing the network are considered. Unprotected wireless networks can be accessed at will by unauthorized users who may be interested in free Internet access or may have more nefarious objectives.

<5> The 802.11b standard includes a security protocol known as Wired Equivalent Privacy (WEP) that if used, makes it more difficult to gain unauthorized access to a network. Although WEP provides only limited security for a Wi-Fi network, if used in connection with other security measures such as passwords and firewalls, it can reduce the likelihood that casual passersby will

gain access to a network.

<6> The sudden popularity of wireless networks, combined with a popular misperception that no additional steps to secure those networks are necessary, has caused a marked increase in the number of insecure computer networks that can be accessed without authorization. This in turn has given rise to the sport of wardriving — detecting and reporting the existence of insecure wireless networks, ostensibly without actually accessing the network. Wardriving may also involve illegally accessing and monitoring the networks once so discovered. The sport of discovering connections to wireless computer networks can be done while driving in a car ("wardriving") or while strolling on foot with a PDA ("war strolling"). When a network is identified, the "hotspot" or "access point" (AP) can be marked with a coded symbol in chalk on a wall or sidewalk, or "war chalked". This will alert others to the presence of an open or insecure wireless network in a given location — which they might choose to access themselves. Other variations include "war stumbling" (accidental discovery of an open access point).

<7> Most hackers or wardriving hobbyists use freeware tools such as NetStumbler,[4] or Kismet.[5] These software programs can be used for the wholly legitimate purpose of helping network administrators make their systems more secure. They work by detecting the "service set identifier" (SSID) number that wireless networks continuously broadcast to identify themselves to their authorized users. Unfortunately, unless steps are taken by the wireless network operator to restrict what and to whom the network broadcasts as part of this process of signaling to users, then unauthorized users can also discover the existence of the network. In that event, drive-by snoopers and casual passersby alike will not only be able to detect the network, but will be able to access network resources unless some system is in place to restrict network access, such as requiring a user ID and password to log on to the system.

<8> Information gathered in this manner can be correlated with geographical information provided by the Global Positioning System (GPS) and uploaded to maps posted on the Internet showing the location of access points (AP) for Wi-Fi networks.[6] Commercial services such as Wi-Finder provide maps of wireless networks that provide free or paid public Internet access.

CRIMINAL LIABILITY FOR WARDRIVING

<9> Wardriving may violate several different computer crime statutes. These include the Wiretap Act[7] which covers interceptions and disclosures of electronic communications, the

Electronic Communications Privacy Act (ECPA)[8] which addresses unauthorized access and disclosures of stored electronic communications such as e-mail, and the Computer Fraud and Abuse Act (CFAA)[9] which addresses unauthorized access and misuse of computers and computer networks, in general.

Federal Wiretap Act

<10> Interceptions of electronic communications in "real time" come under the federal Wiretap Act. That Act provides that any person who intentionally intercepts an electronic communication is guilty of a felony and subject to a fine of up to $250,000 and imprisonment for up to five years.[10] The Wiretap Act defines an "interception" as the "acquisition of the contents of any electronic communication through the use of any electronic, mechanical or other device."[11] So while some wardrivers may believe it is legal to peer into other people's networks, so long as they do not record any of the information, this is not correct. Any "acquisition" under the Wiretap Act is unlawful, even if it only involves listening to or monitoring a communication.[12] Although no federal prosecutions of wardriving under the Wiretap Act have yet occurred, Wiretap prosecutions occur with enough frequency to make such a prosecution a possibility, even if an unlikely one.[13]

<11> A war driver might argue that only "marking" the location of an insecure wireless network, but not accessing the network or any contents of the network, should not violate the law. For example, port scanning—that is, looking for open ports from an individual PC user's computer as it accesses the Internet is not necessarily illegal. Port scanning is akin to network discovery or reconnaissance, and such programs are found in the virtual tool chests of both hackers and cyber security professionals. However, a person conducting a port scan needs to proceed with great caution. While intuitively there would appear to be nothing wrong with conducting a port scan to obtain some "chirrups" indicating that a computer is located at that location and that a port is open—a relatively harmless activity with no potential for invasion of privacy—the language of the Pen Register Act appears to prohibit the unauthorized use of any "device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted."[14] This language is extremely broad and so might cover the standard information obtained from a typical port scan, such as the operating system and other programs the computer is running.[15]

Stored Electronic Communications Provisions of ECPA

<12> Access to electronic communications in storage comes under the Stored Electronic Communications provisions of the ECPA, which prohibits the unauthorized access to stored communications, such as electronic mail, and disclosure of the contents.[16] Using a wireless network connection to access stored email communications would appear to violate ECPA if a person hacked into the network provider's server.[17] A simple violation of the statute—that is, the mere unauthorized access or disclosure of stored electronic communications—is a misdemeanor.[18] If stored electronic communications are accessed without authorization for purposes of commercial advantage, malicious destruction or damage, or private commercial gain, the conduct becomes a more serious felony.[19]

Computer Fraud and Abuse Act

<13> The CFAA prohibits various forms of unauthorized access of "protected computers." In 1996, the definition of "protected computer" was considerably expanded so now any unauthorized interference with a computer with access to the Internet may be a federal crime.[20] The CFAA prohibits unauthorized access or exceeding authorized access to obtain information from a protected computer,[21] accessing a protected computer with intent to defraud or obtain anything of value,[22] or intentionally, recklessly or negligently harming a protected computer.[23]

<14> War drivers may access an insecure network, in order to take advantage of free access to the Internet and computer services. Proponents of wardriving or war chalking may argue that there is nothing wrong with surreptitiously accessing someone else's network as long as the network owner has not incurred any financial loss. In essence, they claim there is no "theft." They may point to the fact that a network owner may pay a fixed amount for Internet access without regard to traffic volume, and that under the CFAA, a felony prosecution for unauthorized access to most private computer networks usually requires a showing that the value of the use of the network exceeded $5,000[24] . While prosecutions based on a conversion theory have not always been successful,[25] the definition of "loss" under the CFAA has been considerably broadened as of late. Thus, relying on these cases to justify the continued unauthorized access to insecure wireless networks involves considerable risk.

<15> It is possible for a network owner to exceed bandwidth quota, causing the owner to incur additional expenses or receive slower service as a result of wardriving. Perhaps because of these types of problems, some states prohibit the unauthorized access of someone else's computer network or wireless communication services as a means of avoiding payment for those services. State law varies considerably in this area. Some states have laws that recognize "theft of computer services" as a crime. Some relate specifically to computer networks while others prohibit theft of telecommunications services. Virginia, for example, prohibits anyone from willfully using a computer or computer network with intent to obtain computer services without authority.[26] The term "phreaking," which relates to the unauthorized access of telephone services including cellular services, has been criminalized as theft of services.

<16> Still other state laws include more general prohibitions relating to broader classes of property and services. For example, many states have computer trespass laws. Under Washington's computer trespass statute, for example, a wardriver commits a gross misdemeanor if "the person, without authorization, intentionally gains access to a computer system or electronic database of another." [27] A wardriver is violating this statute anytime he intentionally accesses a WLAN without authorization.

<17> The majority of these statutes have a knowledge requirement. A person has to access the services with the knowledge that the services are available only for compensation (as opposed to being free) and access the services as a means of avoiding payment. In some circumstances, the access of a computer system or program may be prohibited when the user has "reckless disregard" that their use may be unauthorized. Furthermore, even within a state that does not specifically outlaw "phreaking," it does not follow that wardriving or war chalking does not involve violations of federal and state electronic surveillance laws discussed above, which protect non-financial privacy interests of individuals.

Is It a Crime to Access a Wireless Network Accidentally?

<18> With old-fashioned wired computer networks, it is usually impossible to access someone else's network unintentionally. In contrast, wireless networks may actually seem to beckon to potential users by broadcasting their SSIDs over the airwaves, so merely noticing the existence of an insecure wireless network might seem no more illegal than receiving a radio broadcast with a radio receiver. No special equipment is necessary to detect

the SSID number that a wireless network broadcasts to identify itself to its authorized users. When Windows XP is set to run wirelessly, it automatically searches for any SSIDs that are being broadcast within range of the wireless card in the machine. Even intentionally searching for wireless networks may not violate any laws, for example, when a network administrator within a company tries to determine whether rogue employees have set up wireless networks within company facilities without authorization.

<19> Since there are many organizations that make their Wi-Fi networks available for public use, the mere act of searching for a Wi-Fi connection would probably not be considered criminal, since the "searcher" would argue he or she was merely looking for "open" wireless networks—whose owners had consented to the public use of their network. Someone connecting, or attempting to connect, to a wireless network, in the mistaken belief that the network owner consents to public access would not be committing a crime as the requisite intent would be lacking. However, using tools to crack the WEP keys in order to intercept encrypted transmissions by others on an "open" network, or using an "open" network connection to attempt to access data stored on computers that are on that network, likely would be a crime. In between these two extreme cases are many situations that are difficult to characterize as either lawful or criminal because it is unclear how the fact that a user has encountered an open wireless network should be construed.

<20> One view would be to place the burden on the network operator to secure their network. This view would require network operators to take full advantage of the tools that come with the wireless hardware to limit access. Under this view, a user who encounters an open network would be entitled to assume that the network is intended by the owner to be open rather than that the owner accidentally left the door to the system open without intending for the system to be available to the public. While it may make sense to place the burden of encrypting wireless networks on the owners of commercial wireless networks, it may not make sense to place the same burden on homeowners with wireless connections to the Internet from home computers.

<21> The analogy with the bricks and mortar world might be to someone who "cased" homes in a neighborhood to find homes with their front doors open. If someone opened a door of a private home without knowing the owner or having any purpose for the activity, he or she might be prosecuted for trespass. However, a different intuition results as to someone who walked into a public shop after the storeowner accidentally left the door

open even if the store was officially closed.

<22> On the other hand, an innocent accidental interception of a wireless computer network can quickly become a criminal violation when someone, who realizes they have intercepted another person's network, continues to do so at the other's expense. Although there have been no published decisions involving wireless networks, this factual situation is closely analogous to a line of cases involving the interception of calls on cordless telephones that date from the mid-1990s. At that time, many individuals who purchased police scanners discovered that the scanners could also be used to intercept and monitor the telephone conversations of their neighbors' cordless telephones. These individuals would have had no liability if they had stopped when they realized they had accidentally intercepted their neighbors' telephone calls. When they continued to eavesdrop on their neighbors' telephone conversations they were held by courts to have violated the Wiretap Act.[28] The interception of cordless telephone conversations appears closely analogous to the interception of insecure wireless computer networks. In neither case, does the fact that it is easy to conduct the interception provide a defense to liability under the Wiretap Act.

CIVIL LIABILITY FOR WARDRIVING

<23> The Wiretap Act, the ECPA and the CFAA each establish private causes of action. The Wiretap Act[29] and the ECPA[30] each provide for injunctions, actual or statutory damages (whichever is greater), and reasonable attorney's fees.[31] There has been significant private litigation involving claims of Wiretap Act violations. Cases involving the interception of cordless or mobile telephone conversations are closely analogous to the interception of electronic communications in the context of an insecure wireless computer network.[32] The CFAA also provides for a private cause of action, but allows only compensatory damages and injunctive relief. In most cases parties must show damages in excess of $5000, and then only economic damages are recoverable.[33] Nevertheless, recent years have seen an explosion in private litigation alleging violations of the CFAA, particularly in the context of commercial litigation between businesses. This expansion in litigation appears to be due in part to the broad interpretation courts have given to the term "access,"[34] and the even broader interpretation of the concept of "authorization." In one set of cases, violations of the CFAA have been found when employees who have authority to access their employer's computers misuse that authority to obtain confidential business information for one of their employer's

competitors.[35] Another set of cases involves situations in which two parties are governed by a contract that implicitly or explicitly governs one party's access to the other party's computer. When one party uses the computer in a manner that arguably breaches the contract, courts have allowed the offended party to allege that the breach of the contract by the other party—ordinarily creating only civil liability—constitutes a violation of the CFAA.[36]

<24> If information stored on a computer qualifies as a trade secret, unauthorized access of that computer resulting in the misappropriation of that information may be a violation of the federal Economic Espionage Act[37] or a state law criminalizing theft of trade secrets. In addition, misappropriation of a trade secret may also give rise to civil liability. In either case, however, the party suffering the loss of a trade secret has to be able to show that the misappropriation was done by someone with knowledge of the information's status as a trade secret. This limitation on recovery may make it impossible for the trade secret owner to recover from a hacker in some cases where trade secret protection has been lost due to the network operator's failure to secure the network.

<25> Trespass to chattels requires specific intent to interfere with the property rights of another.[38] Anyone threatened with liability for such accidental access might be able to raise a defense based on implied authorization to access evidenced by the network owner's failure to take reasonable steps to restrict access, or even on an updated notion of "attractive nuisance" that lures a trespasser onto the owner's property. In tort law, an attractive nuisance is a potentially harmful object, so inviting, interesting or intruding to children that it lures them on to private property to investigate the attraction. When a landowner knows, or should know, that children are attracted to his land, he has a heightened responsibility to protect these children. The law thus imposes a heightened duty on the landowner. By analogy, one could argue that if a network owner does not want passersby to access their network, the owner has a heightened duty to secure the network from outside access.

CAN WIRELESS NETWORKS BE SECURED?

<26> Just as burglary and trespass laws cannot prevent a house from being robbed, computer crime laws cannot ensure the security of a wireless computer network. With a house, one should buy effective locks and make sure the family uses them; with a wireless computer network, one should take full advantage of technologies available now to reduce the

vulnerability of wireless networks.

<27> Although strong security is not a hallmark of Wi-Fi technology, it is possible for a network operator to reduce dramatically the vulnerability of a wireless network. In the interest of "keeping honest people honest," a network operator should take full advantage of whatever WEP (Wired Equivalent Privacy) features are available. WEP permits communications between the network access point and a mobile device to be encrypted. The weakness of WEP has been well-documented[39] and can easily be exploited by determined hackers, but it can serve to deflect the interest of more casual snoopers toward other nearby networks that are not using WEP.

<28> Devices authorized to access a wireless network are assigned Media Access Control (MAC) addresses. Some wireless networking systems support authentication of MAC addresses, which will prevent casual unauthorized users from logging on to the network. Determined hackers, however, can generally find a way to "spoof" a MAC address, and so fool the network into thinking they are authorized users.

<29> Wireless routers come with default SSIDs and AP passwords set at the factory. These factory defaults should be changed to make it more difficult for a hacker to gain control over network resources. If possible, the default "broadcast SSID" should be disabled to avoid beckoning to casual hackers. A SSID should not be changed from the default setting to some descriptive term such as the name of the company operating the network or "Accounts Payable" which only makes a hacker's job easier. The location of wireless APs should be carefully considered to reduce the likelihood that signals can be intercepted outside the building where they are located. Another simple precaution that can reduce the risk of casual or inadvertent access is to turn off the file-sharing option for computers connected to a wireless network. Computers configured in this manner will not be identified on the network.

<30> Raising the overall level of network security through implementation of a "virtual private network" (VPN) may be necessary to achieve a significant reduction in the insecurity of wireless networks. VPNs use encryption, authentication and firewall technologies to create secure "tunnels" within public networks such as the Internet that permit secure communications to be exchanged between different points on a network. (Secure sockets layer (SSL) technology which is already widely used in Internet commerce is a simple form of VPN technology.)

<31> Work is underway at the IEEE, the organization that

developed the current 802.11b standards, to develop new standards incorporating stronger security protocols. This new standard has not yet been finalized, so it may be several years before Wi-Fi products with stronger security built in become generally available.

CONCLUSION

<32> Because wardriving is not difficult to do, many once thought it was legal. While this perception is no longer widely shared,[40] it still appears to be a widespread practice, perhaps because practitioners believe the likelihood of being prosecuted is not large. Operators of wireless networks should not assume that because individuals engaged in wardriving may be civilly and criminally liable that their networks are protected. The technologies for securing wireless networks have not yet reached the same level of effectiveness as those used to secure wired networks; many wireless network operators even fail to take advantage of the security technologies that are available. As a result of the weakness of currently available legal and technological protections, operating wireless computer networks involve significant risks—risks that may well outweigh the benefits of the convenience the technology offers for business information systems. If, after carefully assessing the risks and the benefits, it appears that the risks of using the technology outweigh the benefits, it may be best to defer adoption of the wireless technology until more effective technologies are developed to secure the network.

PRACTICE POINTERS

- Clients should be encouraged to consider managing the additional security risks associated with current wireless technology among the costs of switching from wired to wireless networking. Potential security problems should be taken into account when comparing prices and contract terms offered for wireless networking equipment and services. When the cost of maintaining acceptable levels of computer security is factored into price calculations, wireless networking may not be less expensive than more conventional alternatives.
- A major change in IT architecture such as a switch from wired to wireless networking should trigger a review of IT policies within an organization, including security, disaster recovery and record management

policies. Clients should already have in place IT policies that provide a framework for managing the risk of wireless networking. Employees should know that they are not permitted to create "rogue networks" without the knowledge of IT managers, for example, by adding their own personal wireless networks onto laptop computers issued by the employer. Such unauthorized wireless networks might make life easier for the individuals setting them up, but may undermine the security of an entire organization's IT system.

- If the addition of wireless networking to an existing IT system diminishes its overall level of security, then a client may find it has breached obligations it has to its own customers or trading partners. For example, it may not be violating its commitments to protect the privacy of personal information contained in a posted data privacy policy, or its obligations under confidentiality agreements. It may also be undermining the trade secret status of important internal information.

<< Top

FOOTNOTES

1. Anita Ramasastry is an Associate Professor of Law and Co-Director of the Shidler Center for Law, Commerce & Technology, University of Washington School of Law. Jane K. Winn is a Professor of Law and Co-Director of the Shidler Center for Law, Commerce & Technology, University of Washington School of Law. Peter Winn is Assistant U.S. Attorney, U.S. Department of Justice; Part Time Instructor, University of Washington School of Law. The views expressed in this article are the personal views of the author alone and should not considered in any way to represent the views of the United States Department of Justice.

2. The term "wardriving" is derived from "war dialing"--the practice of programming a computer to dial a sequential series of telephone numbers until it detects another computer and then attempts to gain access to any computers so discovered. War dialing was a computer security problem that emerged in the 1980s with the widespread use of telephone modems, and was made famous by the 1983 film War Games.

3. For example, hackers can use freeware such as AirSnort, available from www.airsnort.shmoo.com, or WEPcrack, available from www.sourceforge.net/projects/wepcrack, to monitor communications until the encryption key being used can be guessed.

4. *See* www.netstumbler.com (accessed July 27, 2005).

5. *See* www.kismetwireless.net (accessed July 27, 2005).

6. These maps can be accessed at Web sites such as www.wigle.net (Wireless Geographic Logging Engine) (accessed July 27 2005).

7. 18 U.S.C. §§ 2510-2522 (2005).

8. 18 U.S.C. §§ 2701-2712 (2005).

9. 18 U.S.C. § 1030 (2005).

10. 18 U.S.C. §§ 2511(1)(a), (4)(a) (2005).

11. 18 U.S.C. § 2510(4) (2005).

12. *See* Watkins v. L.M. Berry & Co., 704 F.2d 577, 584 (11th Cir. 1983) ("A violation of section 2511(1)(b) is the interception itself, not the interception of particular material. It is not necessary to recovery of damages that the violator hear anything in particular; she need do no more than listen.").

13. *See, e.g.*, U.S. v. Townsend, 987 F.2d 927 (2nd Cir. 1993); U.S. v. Lentz, 624 F.2d 1280 (5th Cir. 1980); U.S. v. Duncan, 598 F.2d 839 (4th Cir. 1979); U.S. v. Harman, No. 3-96-CR-272-D (N.D. Tex. 1996).

14. 18 U.S.C. § 3127(3) (2005).

15. One can access http://news.netcraft.com/ (last viewed April 22, 2005) to conduct a port scan of any Web site and obtain this type of identifying information.

16. 18 U.S.C. §§ 2701-2711 (2005).

17. U.S.C. § 2701(a) (2005); By definition, ECPA only applies to situations where a person accesses a facility without or in excess of authorization and then obtains, alters, or prevents access to an electronic communication "while it is in electronic storage in such system…." *See, e.g.*, Theofel v. Farley-Jones,

359 F.3d 1066 (9th Cir. 2004) (unauthorized access to stored email communications held to violate ECPA). *But see* Fraser v. Nationwide Ins. Co., 352 F.3d 108 (3rd Cir. 2003) (access to opened emails held not to constitute an offense under ECPA).

18. 18 U.S.C. § 2701(b)(2) (2005).

19. 18 U.S.C. § 2701(b)(1) (2005).

20. 18 U.S.C. § 1030(e)(2) (2005).

21. 18 U.S.C. § 1030(a)(2) (2005). A wardriver is unlikely to violate the "obtaining information" subsection of the CFAA found in Section 1030(a)(2). Typically, the information obtained will not be of the sort specifically listed under parts (A) and (B) of Section 1030(a)(2), i.e., U.S. government information or financial records of a financial institution, card issuer, or consumer reporting agency. That leaves Section 1030(a)(2)(c), which a wardriver violates only if his "conduct involved an interstate or foreign communication…" Most wardriving will involve wholly intrastate conduct and thus will not violate this subsection.

22. 18 U.S.C. § 1030(a)(4) (2005).

23. 18 U.S.C. § 1030(a)(5) (2005).

24. 18 U.S.C. § 1030(a)(4) (2005).

25. U.S. v. Collins, 56 F.3d 1416 (D.C. Cir. 1995) (dismissing criminal charges against government employee for conversion based on use of federal computer system for personal matters). *See also*, State v. McGraw, 480 N.E.2d 552 (Ind. 1985) (dismissing charges under state theft law for unauthorized personal use of city computer).

26. Va. Code Ann. § 18.2-152.6 (Michie 2004).

27. Wash. Rev. Code § 9A52. 110, 120 (2005). *See also* State v. Riley, 121 Wn.2d 22 (1993) (defendant violated statute by directing his computer to dial telephone company's access number repeatedly and enter random digits in order to discover customer access codes).

28. *See, e.g.*, U.S. v. Harman, No. 3-96-CR-272-D (N.D. Tex. 1996); Goodspeed v. Harman, 39 F. Supp. 2d 787 (N.D. Tex. 1999); Peavy v. WFAA-TV, Inc., 221 F.3d 158 (5th Cir. 2000); Boehner v.

McDermott, 191 F.3d 463 (D.C. Cir. 1999); Bartnicki v. Vopper, 200 F.3d 109 (3d Cir. 1999), *aff'd*, 532 U.S. 514 (2001).

29. 18 U.S.C. § 2520(a) (2005).

30. 18 U.S.C. § 2707(a) (2005).

31. 18 U.S.C. §§ 2520(b), 2707(b) (2005).

32. Goodspeed v. Harman, 39 F.Supp.2d 787 (N.D.Tex. 1999); Peavy v. WFAA-TV, Inc., 221 F.3d 158 (5th Cir. 2000); Boehner v. McDermott, 191 F.3d 463 (D.C. Cir. 1999); Bartnicki v. Vopper, 200 F.3d 109 (3d Cir. 1999) *rev'd on other grounds*, 532 U.S. 514 (2001).

33. 18 U.S.C. § 1030(g) (2005).

34. American Online v. National Health Care Discount, Inc., 121 F.Supp.2d 1255, 1272 (N.D. Iowa, 2000).

35. Shurgard Storage Centers v. Safeguard Self Storage, 119 F.Supp.2d 1121 (W.D. Wash. 2000).

36. *See, e.g.*, EF Cultural Travel v. Explorica, 274 F.3d 577 (1st Cir. 2001); American Online v. LCGM, Inc., 46 F.Supp.2d 444 (E.D. Va. 1998); Register.com v. Verio, 126 F.Supp.2d 238 (S.D.N.Y. 2000). *See generally*, Orin Kerr, *Cybercrime's Scope, Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. Rev. 1596 (2003).

37. 18 U.S.C. §§ 1831, 1832 (2005).

38. Restatement (Second) of Torts § 217 (1965).

39. *See, e.g.*, Nikita Borisov et. al., *Security of the WEP Algorithm* (last visited July 27, 2005), *at* http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html.

40. *See, e.g.*, Wardriving encyclopedia entry on Wikipedia.org, *at* http://en.wikipedia.org/wiki/Wardriving (accessed July 27, 2005). ("In the USA, accessing the files on an open network is illegal under both Federal and State laws, as is using the Internet connection of an open wireless network.").

<< Top