WI-FI LIABILITY: POTENTIAL LEGAL RISKS IN ACCESSING AND OPERATING WIRELESS INTERNET

Robert V. Hale II, Esq.†

I. BACKGROUND

Suppose you turn on your laptop while sitting at the kitchen table at home and respond "OK" to a prompt about accessing a nearby wireless Internet access point owned and operated by a neighbor. What potential liability may ensue from accessing someone else's wireless access point? How about intercepting wireless connection signals? What about setting up an open or unsecured wireless access point in your house or business? Attorneys can expect to grapple with these issues and other related questions as the popularity of wireless technology continues to increase.

Wireless local-area networks ("WLANs"), commonly known as "Wi-Fi" ("wireless fidelity") networks, connect users to the Internet through radio or infrared frequencies on the unlicensed 2.4 and 5 GHz radio bands.[1] Under Institute of Electrical and Electronics Engineers ("IEEE") standards, data transfer rates include 802.11b (11 Mbps), 802.11a (54 Mbps), and 802.11g (125 Mbps).[2] Wi-Fi networks come in several varieties, including WLANs deployed in private residences and businesses, as well as WLANs in public areas (typically known as "HotSpots"), such as airports, hotels and coffee shops. The rapid growth and adoption of Wi-Fi technology includes both the proliferation of wireless access availability, as well as the sale of Wi-

† © 2005 Robert V. Hale II. The author, an attorney in San Francisco, serves as an advisor to the Cyberspace Committee of the California Bar and as Chair of the IP Section of the San Francisco Bar Association Barristers Club. He has written articles and conducted presentations on numerous Internet Law issues, including unsolicited e-mail, privacy and online banking. He received his J.D. from the University of San Francisco School of Law and is an active member of the California Bar.

1. *See* CNET News.com Staff, *Wi-Fi: Unplugging Devices*, CNET NEWS.COM, Sept. 13, 2003, *at* http://news.com.com/Wi-Fi:+Unplugging+devices/2100-7351_3-5072011.html.

2. *See* IEEE, IEEE Wireless Standards Online, *available at* http://standards.ieee.org/wireless/ (last visited Jan. 31, 2005).

Fi equipped devices.[3] In addition to finding HotSpots in Starbucks, hotels and airports, Wi-Fi users often discover multiple, open WLANs in business districts and suburban neighborhoods. Most recently, the City of Philadelphia announced plans to provide free public Wi-Fi access.[4] Numerous websites offer meticulously documented maps of thousands of HotSpots in cities and localities across the United States and abroad.[5] Some Wi-Fi networking equipment manufacturers now produce routers and access points that support Voice over Internet Protocol ("VoIP") capabilities,[6] which permit users with VoIP enabled devices to make telephone calls over the Internet.

II. ACCESSING ANOTHER'S WIRELESS SIGNAL

A. The Computer Fraud and Abuse Act

The Computer Fraud and Abuse Act ("CFAA") makes punishable whoever "intentionally accesses a computer without authorization or exceeds authorized access and thereby obtains — . . . information from any protected computer if the conduct involves interstate or foreign communication."[7] Another section of the CFAA makes punishable whoever "intentionally accesses a protected computer without authorization, and, as a result of such conduct,

3.

> The WLAN IC market is expected to grow strongly over the forecast period of 2004–2008 from approximately 47 mln units shipped and $480 mln in revenue in 2003, to almost 390 mln units shipped and $2.1 bln in revenue in 2008. In the early years of the forecast, much of the shipment volume and revenue is composed of WLAN ICs utilized in Wi-Fi aggregation equipment (e.g., access points and wireless SOHO routers) and Wi-Fi clients (WLAN NICs used in various types of PCs.).

WLAN IC Market to Generate $2.1 Bln in 2008, ITFacts.biz, *at* http://www.itfacts.biz/index.php?id=P1826 (last visited Dec. 8, 2004).

4. *Philly: Let Wi-Fi Ring*, CBSNEWS.COM, Sept. 1, 2004, *available at* http://www.cbsnews.com/stories/2004/09/01/tech/main639967.shtml.

5. *See* WiFinder, Inc., *Find Public Access Wi-Fi Hotspots*, *available at* http://www.wifinder.com/ (last visited Dec. 8, 2004).

6. The FCC has described VoIP as follows:

> VoIP allows you to make telephone calls using a computer network, over a data network like the Internet. VoIP converts the voice signal from your telephone into a digital signal that travels over the internet then converts it back at the other end so you can speak to anyone with a regular phone number.

Federal Communications Comm'n Consumer and Governmental Affairs Bureau, *Frequently Asked Questions: What is VoIP/Internet Voice?*, *at* http://www.fcc.gov/voip/ (last visited Dec. 7, 2004).

7. 18 U.S.C. § 1030(a)(2)(C) (2001).

recklessly causes damage."[8] The Act also provides for a private right of action for individuals damaged by computer fraud.[9] In each case, the statute defines "protected computer" broadly to cover essentially any computer connected to the Internet.[10] To date, the Justice Department has reported at least one CFAA prosecution involving Wi-Fi. In *United States v. Salcedo*, the defendants hacked into the computer system of a retail store through an unsecured Wi-Fi network to steal credit card information while sitting in a car in the parking lot of the store.[11]

In the context of accessing a neighbor's WLAN, liability with respect to both of the previously listed sections depends first on establishing intentional access without authorization. "Access" refers to the intent to access, not the intent to damage the protected computer.[12] The user interface on Wi-Fi equipped devices typically lists detectable access points automatically by a name the Wireless Access Point ("WAP") owner designates. In a residential area, the WAP name may refer to a neighbor's last name, such as in "Jones Family Access Point." The act of choosing an access point in this context could provide evidence of intentional access.

The CFAA does not define "without authorization" or what it means to exceed authorization.[13] Under CFAA case law, establishing unauthorized access or lack of authorization has involved reference to

8. *Id*. § 1030(a)(5)(A)(iii).

9. *Id*. § 1030(g).

10. *Id*. § 1030(e)(2)(B). The statute defines the term "protected computer" to mean a computer "which is used in interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States."

11. *See* Bill of Indictment at 1–2, United States v. Salcedo, (W.D.N.C. Nov. 19, 2003) (No. 5.03cr53-MCK); Criminal Docket for Case #: 03-CR-53-ALL, *available at* http://pacer.ncwd.uscourts.gov/dc/cgi-bin/pacer250.pl?puid=01094528557 (last visited Feb. 21, 2005); *see also* Press Release, U.S. Department of Justice, Western District of North Carolina, Hacker Sentenced to Prison for Breaking into Lowe's Companies' Computers with Intent to Steal Credit Card Information (Dec. 15, 2004), *at* http://www.cybercrime.gov/salcedoSent.htm. Note that the defendants discovered the unsecured wireless network while driving around charting wireless networks on their laptop (a geek sport known as "wardriving"). Salcedo and others later returned to the network to perpetrate the crime. The federal court sentenced Salcedo to nine years in prison.

12. *See* United States v. Sablan, 92 F.3d 865, 867–68 (9th Cir. 1996).

13. Some commentary regarding "authorization" under the CFAA has invoked the common law tort of trespass to chattels to illustrate what the statute leaves largely undefined in this respect (a separate discussion of trespass to chattels follows a later section of this paper). *See* S. REP. NO. 104-357, at 11 (1996). In discussing unauthorized access under the CFAA, the Senate Report provides: "[O]utside hackers who break into a computer could be punished for any intentional, reckless, or other damage they cause by their *trespass*." *Id*. (emphasis added).

the means of access[14] or its purpose.[15] Courts have also found unauthorized access through a "Terms of Service" violation, even where the defendant did not receive notice of the terms.[16] In *America Online v. LCGM*, involving defendant's mass spamming of AOL customers, the court wrote that "Defendants' actions violated AOL's Terms of Service [agreement], and as such was unauthorized."[17] At least one other court has held that a plaintiff can establish a lack of authorization through the use of an "explicit statement on the website restricting access."[18] In *EF Cultural Travel v. Zefer*, involving a defendant who used a scraper tool to extract data from a competitor's website in order to underbid projects, the court also recognized that a lack of authorization could exist implicitly, rather than explicitly in the form of a statement.[19] For example, the court noted that "password protection itself normally limits authorization by implication (and technology), even without express terms."[20] Of particular relevance to the Wi-Fi context, the court found an implicit lack of authorization, rejecting the view that there exists a "presumption" of open access to the Internet.[21]

This panoply of case law provides fairly broad (and potentially confusing) latitude to courts in determining whether unauthorized access has occurred in the case where defendant piggy-backs off of another's WLAN. Under *Zefer*, lack of authorization can depend on whether or not the WAP owner has implemented some procedure for gaining access to the wireless network.[22] In this respect, absence of

14. *See* Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238, 253 (S.D.N.Y. 2000) (discussing access to public website using improper means of automating "robot"); *see also* Four Seasons Hotels and Resorts B.V. v. Consorcio Barr, S.A., 267 F. Supp. 2d 1268, 1322 (S.D. Fla. 2003) (discussing access to protected business network through improper means of "spoofing," or forging, IP addresses to make unauthorized computer appear authorized).

15. *See Register.com, Inc.*, 126 F. Supp. 2d at 253 (establishing unauthorized access based on the use of data for mass marketing in competition with plaintiff).

16. *See* Am. Online, Inc. v. LCGM, Inc., 46 F. Supp. 2d 444, 450 (E.D. Va. 1998). AOL's terms of service provision against unsolicited e-mail applied to AOL members and non-members. *See also* Am. Online, Inc. v. Nat'l Health Care Disc., Inc., 121 F. Supp. 2d 1255, 1273 (N.D. Iowa 2000).

17. *Am. Online, Inc.*, 46 F. Supp. 2d at 450.

18. *See* EF Cultural Travel BV v. Zefer Corp., 318 F.3d 58, 62 (1st Cir. 2003).

19. *Id*. at 63.

20. *Id*.

21. *See id*.; *see also* Jon Stanley, *Whose "Hands" are "Unclean?" — SCO, IBM's 'Agents', and the CFAA*, GROKLAW, Dec. 17, 2004, *at* http://www.groklaw.net/article.php?story=20041217091956894&query=Whose+%93Hands%94+are+%93Unclean%3F%94+.

22. *See Zefer*, 318 F.3d at 63, where the court recognized password protection as a limit on authorization: "We agree with the district court that lack of authorization may be implicit,

password protection, or a similar failure to take reasonable safeguards against unauthorized use, such as encryption, may rebut the view that any outside access to a private WLAN constitutes unauthorized access. Still, under the presumption in *Zefer* that the end user's default status in cyberspace remains "unauthorized" until governed by either explicit or implicit agreements that grant access, the end user's initial act of choosing an access point without permission, as described above, could constitute unauthorized access in itself. This aspect of the analysis becomes further complicated by the fact that, for a variety of reasons, a certain percentage of HotSpot operators and home-based Wi-Fi operators do not deploy any network security.[23] Of 88,122 WAPs scanned in 2003, 67% had not enabled security measures.[24] A more recent survey estimates that some 80% of U.S. residential WLANs will classify as "unsecured' by 2007.[25] Commentators speculate that operators fail to implement security mainly due to a lack of expertise.[26] While automation and simplification by manufacturers of the basic steps required to get a WAP up and running has contributed to widespread adoption of Wi-Fi technology, security implementation remains a painstaking and complicated process for the average user.[27] Further complexity has arisen from the growing popularity of signal-boosting technology that allows WAP users to expand the range of Wi-Fi signals, which can in some cases provide access nearly 75 miles away to a WAP with a normal range of 300 feet.[28] Such factors invite inquiry about whether open or unsecured WLANs serve as invitations to an implicit agreement regarding Internet access, acceptance of which amounts to authorization.[29]

rather than explicit. After all, password protection itself normally limits authorization by implication (and technology), even without express terms." *Id*.

23. Matt Hines, *Worried about Wi-Fi Security?*, CNET NEWS.COM, Jan. 9, 2005, *at* http://news.com.com/Worried+about+Wi-Fi+security/2100-7347_3-5540969.html?tag=nefd.lede.

24. *See Statistics for WorldWide WarDrive III*, Worldwide Wardrive, *at* http://www.worldwidewardrive.org/wwwdstats.html (last visited Dec. 17, 2004).

25. *See* Hines, *supra* note 23.

26. *See id*.

27. *See* Patrick S. Ryan, *War, Peace, or Stalemate: Wargames, Wardialing, Wardriving, and the Emerging Market for Hacker Ethics*, 9 VA. J.L. & TECH. 7, ¶ 108 (2004), *at* http://www.vjolt.net/vol9/issue3/v9i3_a07-Ryan.pdf.; *see also* Jeremy Paul Sirota, *Analog to Digital: Harnessing Peer Computing*, 55 HASTINGS L.J. 759, 778 (2004).

28. *See* Hines, *supra* note 23.

29. *See* Benjamin D. Kern, *Whacking, Joyriding and War-Driving: Roaming Use of Wi-Fi and the Law*, 21 SANTA CLARA COMPUTER & HIGH TECH. L.J. 101, 128 (2004) (discussing in more detail different approaches for finding intentional unauthorized access under the CFAA).

With regard to finding unauthorized access through a "Terms of Service" violation, the AOL cases cited above provide precedent for enforcing such terms on third parties with no privity of contract and no notice of the terms.[30] Internet Service Provider ("ISP") "Terms of Service" typically prohibit many different types of activities, including Internet access by those outside the subscriber's household or business.[31] Although the term applies directly to the customer paying for the service, and not a third-party end user (or "Wi-Fi interloper"), under the rationale of the AOL case cited above, violation of such terms by non-members can amount to unauthorized access for the purposes of the CFAA.[32] In *Register.com v. Verio, Inc.,* which, under the CFAA, enjoined defendant from accessing noncopyrightable information on plaintiff's website, the court established unauthorized access through Verio's violation of Register.com's terms of use.[33] The court found that, although Verio did not actually read and accept the terms of use, it manifested assent to such terms when it submitted a request to the website for information.[34] The line of reasoning in *Zefer* further supports this view to the extent that the end user remains "unauthorized" by default, absent some explicit or implicit agreement.

Section 1030(a)(2) raises the issue of whether the unauthorized access involves obtaining information. Although Congress intended the CFAA to apply to theft-related acts,[35] some courts have interpreted information obtained as "the showing of some additional end—to which the unauthorized access is a means."[36] In this regard, access to any WLAN involves some exchange of information that typically passes between computers (IP address, data packets, etc.) as a means of gaining access to the Internet. Since the statute does not

30. *See* Am. Online, Inc. v. LCGM, Inc., 46 F. Supp. 2d 444, 451 (E.D. Va. 1998).

31. *See SBC Yahoo! Terms of Service*, SBC Yahoo!, *available at* http://sbc.yahoo.com/terms/ (last visited Dec. 8, 2004).

32. *See* Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238, 255 (S.D.N.Y. 2000).

33. *Id*. at 251–53.

34. *Id*. at 248. For a detailed analysis of the Verio case and the issue of establishing unauthorized access under the CFAA via contract, see Christine D. Galbraith, *Access Denied: Improper Use of the Computer Fraud and Abuse Act to Control Information on Publicly Accessible Internet Websites*, 63 MD. L. REV. 320 (2004). Professor Galbraith cites several court decisions and other factors that have facilitated the enforcement of standardized form agreements on the Internet irrespective of whether a party assented to the terms (i.e., "shrink-wrap" software licensing agreements and passage of the Uniform Computer Information Transaction Act in some states). *See id*. at 338–45.

35. *See* United States v. Czubinski, 106 F.3d 1069, 1078 (1st Cir. 1997).

36. *Id*.

specify exactly what information the end user must obtain, the end user who accesses a neighbor's WLAN has potentially committed a misdemeanor violation of section 1030(a)(2), which could then rise to the level of a felony if the acts involved commercial advantage or private financial gain.[37] Criminalization of Wi-Fi interloping under section 1030(a)(2), wherein someone merely uses another's WLAN to check e-mail or to perform other common, relatively unobtrusive acts, seems unlikely. In such a scenario, the end user does not access the Internet to obtain information from the WAP operator, but rather to simply access the Internet.

The next issue, raised by section 1030(a)(5)(A)(ii), concerns whether the unauthorized access "recklessly causes damage."[38] The statute defines "damage" as "any impairment to the integrity or availability of data, a program, a system, or information."[39] Courts have held that prohibited conduct under the CFAA that causes slowdowns and diminished capacity of computers, thereby impairing the availability of the system, also constitutes "damage" under the statute.[40] In this regard, those using a neighbor's WLAN to download large media files or large amounts of content could very easily slow down or diminish Internet access availability on the neighbor's computer. Given that most Internet users, especially those savvy enough to have wireless access, know through experience that content-rich files have a tendency to exhaust broadband capacity, prosecutors could probably meet the statute's *mens rea* requirement of recklessness by providing evidence of the defendant's regular access of large media files. In this sense, the actions of a defendant who systematically downloaded large amounts of data, including music, movies and video games, would reach beyond mere negligence to the higher threshold of recklessness. For civil relief, the CFAA requires proof of "loss to [one] or more persons during any [one]-year period . . . aggregating at least $5,000 in value."[41] Although $5,000 may appear difficult to meet for cases involving the occasional interloper, systematic downloading in numerous instances over a period of months could easily aggregate damage figures beyond this threshold. Also, in class actions, courts have permitted aggregation of the statutory amount among various members of the

37. 18 U.S.C. § 1030 (c)(2)(B)(i) (2001).

38. *Id*. § 1030(a)(5)(A)(ii).

39. *Id*. § 1030(e)(8).

40. *See* Am. Online, Inc. v. Nat'l Health Care Disc., Inc., 121 F. Supp. 2d 1255, 1274 (N.D. Iowa 2000).

41. 18 U.S.C. § 1030(a)(5)(B)(i), (g) (2001).

plaintiff's class.[42]

Although prosecutors have tended to use the CFAA solely to punish theft-related acts involving computers, the proliferating use of Wi-Fi could change this, or provoke related activity at the state level[43] or under federal wiretap laws, such as the Electronic Communications Privacy Act.[44]

B. Intercepting a Wireless Signal

The Electronic Communications Privacy Act ("ECPA"), also known as the "Wire Tap Law," holds that "[it shall not be unlawful] for other users of the same frequency to intercept any radio communication made through a system that utilizes frequencies monitored by individuals engaged in the provision or the use of such system, if such communication is not scrambled or encrypted."[45] Prosecutors have used the law to target certain acts of wireless interceptions and signal theft.[46] The ECPA also imposes federal penalties, both criminal and civil, on anyone who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication."[47] Violations of the ECPA involve five key elements. An individual must: (1) intentionally (2) intercept, endeavor to intercept, or procure another person to intercept (3) the contents of (4) an electronic communication (5) using a device.[48] As with the CFAA, a court could apply these elements to the context of unauthorized Wi-Fi access quite easily. Again, most systems provide notice in some form making unauthorized access intentional to the extent that the user receives the notice. The user then intercepts the wireless signal by accessing it and inevitably receives the contents of an electronic communication through receipt of standard IP packets. As with the CFAA, prosecutors tend to focus application of the ECPA

42. *See In re* Am. Online, Inc., 168 F. Supp. 2d 1359, 1374 (S.D. Fla. 2001).

43. All fifty states have some form of computer crime legislation, with sanctioned conduct differing from state to state. For a comprehensive list of applicable state statutes, see Galbraith, *supra* note 34, at 327 n.59.

44. 18 U.S.C. § 2511 (2001).

45. *Id*. § 2511(2)(g)(v).

46. *See* Brown v. Waddell, 50 F.3d 285, 294 (4th Cir. 1995) (holding that pager "clones" used to intercept numeric transmissions to digital pagers constituted unauthorized interception under the ECPA); United States v. Davis, 978 F.2d 415, 419–20 (8th Cir. 1992) (holding it unlawful to intentionally intercept commercial satellite programming, particularly with regard to encrypted transmissions).

47. 18 U.S.C. § 2511(1)(a) (2001).

48. *Id*. § 2511(a).

to specific intent crimes, such as accessing another's WAP for the purpose of eavesdropping, rather than simply using another's bandwidth. However, as Wi-Fi use proliferates and plaintiffs begin emerging with claims, attorneys should expect to see a variety of theories, given the unusual combination of elements that wireless Internet access presents. For example, as noted above, Wi-Fi can involve privacy and information security issues, as well as property rights through the fact that it often broadcasts beyond physical property boundaries.[49] Wi-Fi also, through its very nature, potentially implicates radio spectrum issues through its use of the unlicensed 2.4 and 5 GHz radio bands,[50] as well as broadband regulatory schemes and antitrust issues through the fact that WLANs typically expand the use of a product that Internet Service Providers supply to customers on a contractually limited basis.[51]

A practical advantage may lie in using the common law tort of trespass to chattels[52] to impose liability for unauthorized use of Wi-Fi, rather than statutes such as the CFAA,[53] which Congress intended primarily for punishment of theft-related acts.[54] Although outside the scope of this discussion, it remains important to note beyond the Federal laws discussed here, that other Internet uses can trigger criminal sanctions under other laws, among them, Federal laws such as the Copyright Act,[55] the National Stolen Property Act,[56] mail[57] and wire[58] fraud statutes, the Communications Decency Act of 1996,[59] the Child Pornography Prevention Act of 1996,[60] and the U.S.A Patriot Act of 2001.[61] Assorted state laws show a corresponding sensitivity

49. *See* Hines, *supra* note 23.

50. *See* Patrick S. Ryan, *Questioning the Scarcity of the Spectrum*, 9 J. INTERNET L. (forthcoming 2005).

51. *See infra* Part III regarding ISP service terms that limit use of the service to one person per household or business.

52. *See* Thrifty-Tel, Inc. v. Bezenek, 54 Cal. Rptr. 2d 468 (Cal. Ct. App. 1996).

53. 18 U.S.C § 1030 (2001).

54. For a detailed discussion applying the CFAA to cyber-crimes, see Eric J. Sinrod & William P. Reilly, *Cyber-Crimes: A Practical Approach to the Application of Federal Computer Crime Laws*, 16 SANTA CLARA COMPUTER & HIGH TECH. L.J. 177 (2000). For a similarly detailed discussion of the legal and ethical aspects of hacking WiFi networks, see Ryan, *supra* note 27.

55. 17 U.S.C. §§ 101–1332 (2001).

56. 18 U.S.C. §§ 2311–2322 (2001).

57. *Id*. at § 1341.

58. *Id.* at § 1343.

59. 47 U.S.C. §§ 230–231 (2000).

60. 18 U.S.C. § 2256–2260 (2000).

61. 31 U.S.C. § 5318–5332 (2000).

to the wide variety of criminal acts perpetrated on the Internet.

C. Trespass to Chattels

Under California law, an action for trespass to chattels arises when an intentional interference with the possession of personal property causes injury.[62] Courts have found the basic elements of trespass to chattels (with the exception of damages) satisfied in many different types of unauthorized computer access cases.[63] Most notably, a case involving an ex-Intel worker who e-mailed thousands of messages critical of his former employer to staffers at work advanced to the California Supreme Court on the issue of damages.[64] In *Intel v. Hamidi*, the court held that trespass to chattels in California "does not encompass, and should not be extended to encompass, an electronic communication that neither damages the recipient computer system nor impairs its functioning."[65] Nonetheless, the court offered relevant examples of what has constituted damages in other cases involving unauthorized computer access, including overburdening or interference with the efficient functioning of computer systems[66] and *threatened* harm in the potential for others to imitate the defendant's activity.[67] With respect to the first example, a neighbor's teenager's use of another neighbor's Wi-Fi to download large media files to play video games could result in overburdening or interference with the efficient functioning of the neighbor's computer system, especially involving the speed of data transfer. Another increasingly probable scenario involves the use of VoIP in the same context, where a neighbor could make phone calls using another's wireless access point. In regard to the second example, again it seems likely that the trespassing teenager would share his discovery with friends in the neighborhood about the "free" wireless Internet access

62. *See* Thrifty-Tel, Inc. v. Bezenek, 54 Cal. Rptr. 2d 468, 473 (Cal. Ct. App. 1996).

63. *Id.* (finding that evidence of automated searching of a telephone carrier's system for authorization codes constitutes a cause of action for trespass to chattels); *see also* Am. Online, Inc. v. LCGM, Inc., 46 F. Supp. 2d 444, 451–52 (E.D. Va. 1998); Am. Online, Inc. v. IMS, 24 F. Supp. 2d 548, 550–51(E.D. Va. 1998); Hotmail Corp. v. Van$ Money Pie, Inc., 47 U.S.P.Q.2d (BNA) ¶ 38 (N.D. Cal. 1998); CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1020–23 (S.D. Ohio 1997).

64. Intel Corp. v. Hamidi, 71 P.3d 296 (Cal. 2003).

65. *Id.* at 300.

66. *See, e.g.*, Thrifty-Tel, Inc. v. Bezenek, 54 Cal. Rptr. 2d 468 (Cal. Ct. App. 1996) (involving automated searching of a telephone carrier's system for authorization codes).

67. *See, e.g.*, eBay, Inc. v. Bidder's Edge, 100 F. Supp. 2d 1058, 1071–72 (N.D. Cal. 2000) (finding that eBay was entitled to an injunction where defendant's auction aggregation site accessed eBay's web site 100,000 times per day).

available down the block. This might in turn encourage *threatened* harm in the potential for others to imitate the defendant's activity, which, at least under California law, may provide the basis for an injunction against the defendant.

Another likely result involves use of the unsuspecting neighbor's broadband to power the trespasser's computer in peer-to-peer ("P2P") systems, which, according to the Federal Trade Commission,

> differ from others in that they support the decentralized discovery and delivery of content from published directories, or shared folders, posted on networked devices interconnected by means of compatible software programs. Technologies that use central servers require end users to access their databases first to search for content and then to download it. By eliminating the needs for centralized indices and storage capacity for content, P2P technology allows for faster file transfers and conserves bandwidth. [68]

In this respect, a Wi-Fi interloper conducting activities on a P2P network (such as file sharing) would leverage the computing power and bandwidth of the unsuspecting neighbor who operates the trespassed Wi-Fi.

Among the several defenses to trespass to chattels, *apparent consent* appears most likely to arise given current trends in the implementation of Wi-Fi, particularly with regard to private residences. Under the Restatement, "[i]f words or conduct are reasonably understood by another to be intended as consent, they constitute apparent consent and are as effective as consent in fact."[69] Lack of log-in procedures, encryption, or other forms of security may create a privilege in the would-be trespasser of apparent consent to use another's Wi-Fi network. This scenario seems plausible under a reasonable person standard given the fact that Wi-Fi routers usually come equipped with safeguards, such as log-in procedures and encryption, that the owner can choose whether or not to deploy. A regular Wi-Fi user, whose laptop may automatically detect the presence of a WLAN, would come to expect to find such safeguards in place, and then, not seeing these protections, reasonably assume that the plaintiff WLAN owner has granted some form of apparent

68. *See* Marty Lafferty, *Peer-to-Peer File-Sharing Technology: Consumer Protection and Competition Issues*, DISTRIBUTING COMPUTING INDUSTRY ASSOCIATION, *available at* http://www.ftc.gov/os/comments/p2pfileshare/OL-100012.pdf (Nov. 14, 2004).

69. RESTATEMENT (SECOND) OF TORTS, § 892 (1977).

consent.[70] However, according to Prosser, "[t]he defendant's privilege is limited to the conduct to which the plaintiff consents, or at least to acts of a substantially similar nature."[71] Here, a court may turn to custom[72] to help determine whether a scope of privilege rebuttal applies in this context. For instance, the defendant could cite evidence that those who piggy-back off of other's WLANs typically do so only to perform relatively unobtrusive Internet activities, such as checking e-mail or surfing Web pages. In turn, plaintiff can cite, probably more persuasively, that those who piggy-back typically engage in activities that take up considerable bandwidth, such as downloading music files.[73] Plaintiff could also try invoking *Zefer*[74] by arguing that the defendant's default status remains unauthorized in the absence of some form of explicit or implicit agreement. In addition to rebutting this view by interpreting plaintiff's open WAP as a form of implicit agreement, defendant may also try to turn the tables by calling into question plaintiff's potential liability for providing any open wireless Internet access to those outside plaintiff's residence.[75]

This brief analysis certainly does not end the application of tort principles to the hypothetical at issue or other factual permutations. For instance, contributory liability may apply to those who make others aware of open WLANs. The phenomenon of "warchalking" comes to mind in this respect, whereby Wi-Fi enthusiasts provide notice of available WAPs and HotSpots by marking hieroglyphics in

70. A scenario with parallels to the discussion above exploring whether unsecured WLANs serve as invitations to an implicit agreement regarding access, acceptance of which constitutes authorization under the CFAA.

71. W. PAGE KEETON ET AL., PROSSER & KEETON ON THE LAW OF TORTS, § 18 (5th ed. 1984).

72. *See* RESTATEMENT (SECOND) OF TORTS, § 892 cmt. d (1977):

> In determining whether conduct would be understood by a reasonable person as indicating consent, the customs of the community are to be taken into account. This is true particularly of silence or inaction. Thus if it is the custom in wooded or rural areas to permit the public to go hunting on private land or to fish in private lakes or streams, anyone who goes hunting or fishing may reasonably assume, in the absence of a posted notice or other manifestation to the contrary, that there is the customary consent to his entry upon private land to hunt or fish.

73. Sandeep Junnarkar, *One Way to Get Online: Piggyback*, N.Y. TIMES, Aug. 26, 2004, at G5.

74. *See* EF Cultural Travel BV v. Zefer Corp., 318 F.3d 58, 62–63 (1st Cir. 2003).

75. *See* Nick Langley, *The Demise of the Warchalkers*, COMPUTERWEEKLY.COM, June 24, 2003, *at* http://www.computerweekly.com/Article122783.htm. Courts and commentators continue to debate the wisdom of applying trespass to chattels to the cyberspace context generally. *See* Dan L. Burk, *The Trouble With Trespass*, 4 J. SMALL & EMERGING BUS. L. 27, 37 (2000).

chalk on adjacent sidewalks.[76] In considering how liability could extend to such acts, note that defendants in the *Salcedo* case[77] discovered the unsecured wireless network which they later hacked into, while driving around charting wireless networks on their laptops (a geek sport known as "wardriving" — a variant of "warchalking").[78] Assuming prosecutors could have charged certain defendants involved in locating the open WLAN with aiding and abetting the target CFAA violation, systematic dissemination of information on where to find open WAPs could provide a basis for seeking contributory liability to the extent that such activity encourages unauthorized use of others' Wi-Fi networks.[79]

III. ACCESS POINT LIABILITY

Internet service providers typically include in the written terms and conditions certain provisions that restrict service to one business or household per modem.[80] For instance, the terms of service for SBC Yahoo! contain the following provision under the "Resale of Service" section:

> *Restricted Use.* You agree not to permit anyone else to use your Member Account and that each Sub Account may only be used by one member of your household or business.[81]

Similarly, Verizon's personal DSL agreement states that "[y]ou may not resell the Broadband Service, use it for high volume purposes, or engage in similar activities that constitute resale (commercial or non-commercial), as determined solely by Verizon."[82] Assuming that ISPs police such activity,[83] a provider could

76. *See* Langley, *supra* note 75.

77. *See* Bill of Indictment at 1–2, United States v. Salcedo, (W.D.N.C. Nov. 19, 2003) (No. 5.03cr53-MCK); Criminal Docket for Case #: 03-CR-53-ALL, *available at* http://pacer.ncwd.uscourts.gov/dc/cgi-bin/pacer250.pl?puid=01094528557; *see also* Pierce, *supra* note 11.

78. The term "wardriving" derives from the old hacker practice called wardialing, which the actor Matthew Broderick made famous in the 1983 film "WarGames." Broderick's character hacked into a military computer by wardialing through a telephone-based modem, and nearly triggered a nuclear war with Russia. *See* Kern, *supra* note 29, at 104 n.7.

79. *See* Wifinder, *supra* note 5.

80. *See* Junnarkar, *supra* note 73.

81. *See SBC Yahoo! Terms of Service*, *supra* note 31.

82. *See Verizon Internet Access Terms of Service*, Verizon, *available at* http://www2.verizon.net/policies/tos.asp (last visited Dec. 03, 2004).

83. Although at least one ISP has admitted that they do not "actively" police Wi-Fi piggy-backing (*see* Junnarkar, *supra* note 73), another ISP has acknowledged that it has actively searched open wireless access points that are shared in violation of its service contracts. *See*

presumably terminate the contract of a customer who violates these kinds of provisions. Certain state laws may also impose liability on WAP operators who provide access in violation of ISP terms of service. Maryland, for example, prohibits the use of a "device, technology, [or] product . . . used to provide the unauthorized access to . . . transmission [of], or acquisition of a telecommunication service provided by a telecommunication service provider."[84] Delaware, Florida, Illinois, Michigan, Virginia and Wyoming all have laws on the books that may invoke similar liability.[85] Delaware law, for instance, prohibits "the unauthorized acquisition or theft of any telecommunication service or to receive, disrupt, transmit, decrypt, acquire or facilitate the receipt, disruption, transmission, decryption or acquisition of any telecommunication service without the express consent or express authorization of the telecommunication service provider."[86]

Wireless access operators could also incur liability to the extent that they make access available, and in doing so, facilitate activities that damage others. Continuing the earlier hypothetical, if someone downloads unauthorized copies of music files using another's WLAN, and thereby commits copyright infringement, vicarious liability for the infringement may attach to the WAP operator. As demonstrated in the *A&M Records, Inc. v. Napster, Inc.*[87] decision, which involved vicarious copyright infringement liability of a peer-to-peer network provider, courts limit such liability to cases where the peer-to-peer network has "the right and ability to supervise the infringing activity and also has a direct financial interest in such activities."[88] Regarding the right and ability to supervise, home-based WAPs typically do not come packaged with monitoring mechanisms that would facilitate the tracking of potentially infringing activity (assuming operators have a right to supervise such activity). In addition, although WAPs typically feature technology that allows the operator to block certain users, these types of functions usually

Langley, *supra* note 75.

84. *See* MD. CODE ANN., CRIM. L. § 7-313 (2002).

85. *See* Mark Rasch, *WiFi High Crimes*, SECURITY FOCUS, May 3, 2004, *at* http://www.security focus.com/columnists/237.

86. DEL. CODE ANN. tit. 11, § 850(a)(1)(a) (2001).

87. *See* A&M Records, Inc. v. Napster, Inc., 284 F.3d 1091, 1098 (9th Cir. 2002) (affirming District Court's authority to force Napster to use filter mechanisms to police copyrighted works).

88. *See* Gershwin Publ'g Corp. v. Columbia Artists Mgmt., Inc., 443 F.2d 1159, 1162 (2d Cir. 1971).

require the operator to implement security options that the average user would probably avoid due to complexity and lack of automation.[89] Regarding direct financial interest, given that those who deploy Wi-Fi residentially do so primarily to make the Internet more accessible within their own homes, it seems unlikely that home-based WAP operators would have any financial interest in infringing activities. Commercial HotSpot operators may have some indirect financial interest to the extent that infringing users may run up more access fees in their attempts to download infringing media files. Still, prevailing reluctance[90] to impose responsibility on ISPs for harmful conduct committed by end users would probably protect these parties from contributory liability in this context.

IV. CONCLUSION—AVOIDING LIABILITY, SEEKING REMEDIES, CONSIDERING POLICY

As a general matter, until the courts and legislatures better define the legal status of Wi-Fi arrangements, the piggy-backing Wi-Fi user should simply stop the practice of accessing others' open WLANs, absent an explicit agreement or notice. If a Wi-Fi interloper must continue, he or she should avoid heavy downloading activity (music, games, movies, etc.) that has a tendency to overburden the network and may amount to recoverable damages. Similarly, sapping a residential neighbor's Internet service in lieu of paying for one's own seems potentially more culpable than accessing signals in a business area while on a lunch break. On the other hand, those for whom piggy-backing supplies the only practicable means of obtaining residential high-speed Internet access may want to seek out services that provide Wi-Fi sharing arrangements, through which ISPs pass through service payments from end users on to WAP operators.[91]

89. The Linksys Wireless-G Access Point (product number WAP54G) provides features that allow the operator to control who has access to the WLAN, but the product does not support the ability to track or monitor Internet activity.

90. *See* Doug Lichtman & Eric Posner, *Holding Internet Service Providers Accountable*, UNIVERSITY OF CHICAGO, JOHN M OLIN LAW & ECONOMICS WORKING PAPER NO. 217 (2ND SERIES), (July 2004), *available at* http://ssrn.com/abstract= 573502. In addition to citing ISP immunity provisions in the Communications Decency Act of 1996 and the Digital Millennium Copyright Act of 1998, the authors note that "Courts interpreting these provisions have reinforced this apparent trend away from ISP liability by, among other things, interpreting these statutes to preempt state laws that would otherwise have encouraged ISPs to take due care." *Id*. at 4.

91. Speakeasy Broadband Services, LLC, a Seattle-based ISP, provides such a service. *See WiFi NetShare Service*, Speakeasy Broadband Services, *available at* http://www.speakeasy.net/netshare/learnmore/ (last visited Jan. 4, 2005).

The WAP operator can mitigate liability by implementing a secure network through the use of password protection and encryption. To the extent that the operator can identify any interlopers, the operator should take steps to exclude such users from the network.[92] Unfortunately, as mentioned above, the difficulty involved both in securing and monitoring WLANs adds confusion to the issue of the operator's potential liability. As manufacturers strive to create simple, "plug-and-play" Wi-Fi kits, home users become increasingly less likely to attain the necessary network administration skills that proper Wi-Fi security and maintenance require. A manufacturer's recent offering of Wi-Fi security paint, containing compounds which effectively block all radio signals, illustrates the apparent futility of implementing secure wireless networks.[93] In response to these difficulties, Wi-Fi equipment makers such as Linksys and Hewlett-Packard recently announced plans to create a push-button security system for home wireless product entitled, "SecureEasySetup."[94] Of course, the Wi-Fi sharing arrangement mentioned above also provides an apparently legal option for the WLAN operator to share the signal with others while defraying monthly service costs.

Despite the difficulties involved in securing and monitoring Wi-Fi networks, operators seeking statutory or common law remedies for damages caused by interlopers may need to develop the necessary technical skills in order to support a cause of action. For instance, in moving a claim forward, the plaintiff will need to provide proof that the alleged interloper accessed plaintiff's WLAN, as well as evidence of damages. In doing so, the plaintiff will need to produce log files that identify the defendant and other evidence that shows the defendant's activity interrupted the network to such an extent as to justify damages. Also, the plaintiff's case would certainly benefit from providing proof that he or she implemented appropriate security measures and attempted to exclude the defendant from access, which would tend to demonstrate a form of notice in establishing the defendant's unauthorized access.

From a policy perspective, recent efforts by municipalities to provide free Internet access to the public[95] highlight contrasting views

92. See Kern, *supra* note 29 for an expanded discussion of the policy implications associated with implementing security measures on Wi-Fi networks.

93. *See* Jim Nash, *Startup Markets Wireless-Security Paint*, INFORMATIONWEEK, Dec. 28, 2004, *at* http://informationweek.com/story/showArticle.jhtml?articleID=56200676.

94. *See* Hines, *supra* note 23.

95. *See Philly: Let Wi-Fi Ring*, *supra* note 4.

about whether such services should evolve as radio and television (services which still offer free access) rather than as a private commodity. The concept of free public Internet access as a desired goal may tend to influence people with Wi-Fi equipped devices to use wireless access freely wherever and whenever they can access it. Also, the fact that Wi-Fi operates on unlicensed radio frequencies may invite further analogies to conventional radio, giving rise to presumptions that open broadcast signals from Wi-Fi networks exist in the public domain, irrespective of origin. In the meantime, in addition to the public, virtually all the major Internet industry players, including ISPs, equipment manufacturers, content providers and government continue to become increasingly dependent on expanding broadband availability and capacity. In this respect, rather than pursuing WAP operators who violate terms of service with open access points, ISPs may find more success in encouraging such activity as much as possible and allowing ensuing demand to drive appropriate pricing structures in the brave new world of Wi-Fi. Until then, or perhaps irrespective of market solutions, novel legal issues with respect to Wi-Fi will most likely continue to arise.