Santa Clara University School of Law

Santa Clara High Technology Law Journal

Volume 21 | Issue 1 Article 3

2004

Whacking, Joyriding and War-Driving: Roaming Use of Wi-Fi and the Law

Benjamin D. Kern

WHACKING, JOYRIDING AND WAR-DRIVING: ROAMING USE OF WI-FI AND THE LAW

Benjamin D. Kern†

Nokia, the Finnish mobile phone manufacturer, has referred to roaming Wi-Fi use as "robbing,"[1] while the New York Times ethicist says that it is fine.[2] This article explores the controversial practice of using unencrypted Wi-Fi network connections to the Internet without the prior express approval of the network's operator. Roaming Wi-Fi use creates value for individuals and society through its expansion of the accessibility of high speed Internet connections outside the home or office. However, inconsistency and lack of clarity in current law have created uncertainty among Wi-Fi users that could threaten that value.

Part I introduces Wi-Fi technology and its explosive growth. It then explains that many networks are either intentionally or unintentionally "open," allowing access to the network by a roaming Wi-Fi user. Finally, Part I distinguishes "whackers," or wireless hackers, from roaming Wi-Fi users. Roaming Wi-Fi users include "joyriders" that use an open Wi-Fi connection to access the Internet, "war-drivers," who scan, locate, and map Wi-Fi access points, and accidental users, who unintentionally connect to a Wi-Fi network.

Part II discusses the benefits and costs associated with roaming Wi-Fi use. Use of open Wi-Fi connections to enable access to the Internet should be encouraged because this use will contribute to the continued expansion, flexibility, and "footprint" of the Internet, as

---

† Mr. Kern is an attorney with Gordon & Glickson LLC, a Chicago-based law firm devoted exclusively to providing strategic legal counsel to the IT marketplace. He received his J.D. from Cornell Law School (1997), his M.B.A. from Cornell's Johnson Graduate School of Management (1996) and his B.A. from Indiana University (1992). The author wishes to express his appreciation to Lynn Stram for her intrepid research assistance, to Jennifer Lupfer, Amy Alvarado and the editorial staff of the *Santa Clara Computer & High Technology Law Journal* for their invaluable assistance and suggestions, and to Stacey Kern for her comments, indulgence and tireless support through many evenings and weekends.

1. James Middleton, *Warchalking is theft, says Nokia, at* http://www.vnunet.com/News/1135130 (Sept. 18, 2002).

2. Randy Cohen, *The Ethicist: Wi-Fi Fairness*, N.Y. TIMES MAGAZINE, Feb. 8, 2004, at 22.

well as the development of new networking technologies. Concerns regarding the costs of this use, security risks, and liability risks do not change this conclusion, even in the case of networks that have inadvertently been left open.

Part III examines federal statutes, state statutes, and a common law trespass action, all of which initially appear relevant to roaming Wi-Fi use. While most federal statutes will not apply to roaming Wi-Fi use, application of the laws of many states, and possibly the Federal Computer Fraud and Abuse Act ("CFAA"), to roaming Wi-Fi use depends on whether roaming Wi-Fi use is considered intentional, unauthorized access. Examination of federal, state, and common law decisions reveals four basic approaches to defining intentional, unauthorized access. Most jurisdictions do not provide guidance as to how intentional, unauthorized access is to be interpreted.

Part IV analyzes the four tests for finding intentional, unauthorized use, and concludes that access to an open Wi-Fi network should be considered intentional, unauthorized access only if the network operator has taken affirmative steps to prevent access. This approach provides clarity to Wi-Fi users, facilitates roaming use of Wi-Fi, encourages responsible security practices, and simplifies enforcement of unauthorized computer access statutes. This article concludes by encouraging legislators to consider modeling their statutes after New York's unauthorized computer access statute. Alternatively, under statutes that do not provide clear guidance in interpreting intent and authorization requirements, courts should consider following decisions that find intentional, unauthorized access only if security measures have been adopted. Finally, in cases where statutes already dictate the application of approaches other than the approach advocated in this article, courts should consider the context in which roaming Wi-Fi occurs, as well as the value of facilitating roaming Wi-Fi, in determining whether a user may assume that access to an open network is permissible.

I. INTRODUCTION

Wi-Fi[3] wireless data networking technology has been a great success story in the first few years of the twenty-first century. Wi-Fi (short for "wireless fidelity") is a short-range networking technology that allows computers with Wi-Fi capability to connect to computer networks and the Internet using a radio connection rather than wires. In most cases, Wi-Fi connections take place between a laptop computer with a Wi-Fi card or integrated Wi-Fi capability and a radio "access point" located within approximately 300 feet of the laptop. Wi-Fi equipment has become very popular because it is inexpensive and easy to use.

Use of Wi-Fi networks to access the Internet has become widespread, with tens of millions of users accessing Wi-Fi networks at home or in the office. According to market research firm Pyramid Research, the number of worldwide Wi-Fi users is projected to reach 707 million by 2008.[4] As of 2004, approximately 5% of all Americans have Wi-Fi networks in their homes.[5] Enterprises also have adopted Wi-Fi at a rapid rate, often as a supplement to, or replacement for, existing wired networks. Users who have become accustomed to connecting to the Internet using Wi-Fi in the home or at the office have increasingly searched for ways to continue using Wi-Fi access to the Internet while on the road. As the number of Wi-Fi users has increased, demand for public Wi-Fi access points (known as "hotspots") has grown rapidly.

A variety of entities make Wi-Fi accessible to the public, including telecommunications carriers, municipalities, coffee shops, hotels, airports, and others. Individuals may also often share their home Internet access through Wi-Fi, in the spirit of cooperation, and in the expectation that other individuals will share their networks as

---

3. *See Wi-Fi FAQs*, Wi-Fi Alliance, *at* http://www.wi-fi.org/OpenSection/FAQ.asp?TID=2#WECA (last visited Sept. 20, 2004). The Wi-Fi Alliance, formerly known as the Wireless Ethernet Compatibility Alliance, established the "Wi-Fi" standard for manufacturers, providing requirements and certification for interoperability among devices that comply with the Institute of Electrical and Electronics Engineers ("IEEE") 802.11 standards. Wi-Fi certification was originally available only for 802.11b 2.4 GHz WLANs, but is now available for 802.11a 5GHz networks.

4. *Pyramid Predicts 700 Million Wi-Fi Users by 2008*, Pyramid Research, *at* http://www.pyramidresearch.com/info/press/release_030721.asp (July 21, 2003).

5. Jack Kapica, *Consumers still hazy on Wi-Fi facts: Study*, Globeandmail.com, *available at* http://www.globetechnology.com/servlet/story/RTGAM.20040225.gtwififeb25/BNStory/Technology/ (on file with the *Santa Clara Computer & High Technology Law Journal*) (Feb. 25, 2004).

well. Community groups have formed in New York City, San Francisco, Seattle, Portland, Austin, and other cities to promote sharing of Wi-Fi Internet access.

Some individuals or businesses unintentionally leave their networks unencrypted, allowing roaming users to access the Internet through their networks without the operator's express prior consent,[6] and often without their knowledge. Wi-Fi equipment includes a number of security mechanisms, including encryption, that can easily be used to prevent unknown users from connecting to an access point. Depending on the Wi-Fi equipment vendor, the encryption feature may or may not be turned on by default. Many consumers and businesses do not enable these security measures, because they wish to share access to the Internet with neighbors or the public, because they may not appreciate the risks associated with leaving a network unsecured, or because they appreciate the risks, but determine that the risks are not serious enough to merit taking the additional steps required to secure a network. Unsecured Wi-Fi networks, through which roaming access to the Internet is possible, are referred to as "open" networks.

This article will focus on the application of existing laws to roaming Wi-Fi users who access the Internet through an open Wi-Fi network without obtaining prior express permission from the network's operator. In the colorful lexicon of wireless enthusiasts, roaming users may include "joyriders" and "war-drivers," as well as accidental users, and are to be distinguished from "whackers." "Joyriders" find and use a Wi-Fi connection outside of their home or office for a variety of purposes, including checking e-mail, web surfing, or connecting to a corporate network. "War-drivers" use software to scan the airwaves for "beacon frames" that are broadcast by Wi-Fi networks or other information transmitted by a Wi-Fi access point in response to a probe request.[7] When a network is found, a

---

6. *See Statistics for WWWD3*, *at* http://www.worldwidewardrive.org/ (last visited Sept. 20, 2004). In an annual event termed the "Worldwide WarDrive," participants around the globe spend a week locating and accumulating data about access points. In 2003, participants surveyed 88,122 access points worldwide, and determined that WEP encryption technology, which is included on all Wi-Fi access points, was enabled in only 32.26% of these access points.

7. *See* Patrick S. Ryan, *War, Peace, or Stalemate: Wargames, Wardialing, Wardriving, and the Emerging Market for Hacker Ethics*, 9 VA. J.L. & TECH. 7 (2004), *at* http://www.vjolt.net/vol9/issue3/v9i3_a07-Ryan.pdf (discussing war dialing and war-driving). The term "war-driving" is a play on words based on scenes from the 1983 movie *WarGames*, in which the protagonist randomly dialed numerous telephone numbers to find unsecured or poorly secured computer networks connected by modem to the phone lines. This random dialing was later termed "wardialing." When software tools made it possible to ride in a car and scan for

war-driver may record and publish the location of the network, as well as certain details about the network, including information as to whether encryption has been enabled on the network. However, for purposes of this article, the act of war-driving does not include joyriding or actually connecting to the network. Roaming users may also include those who unintentionally connect to a Wi-Fi network. The popular Microsoft Windows XP operating system software contains a "zero configuration" feature designed to facilitate connecting to Wi-Fi networks, which can cause a user to connect to a network unintentionally. An "accidental user" may joyride on a network without realizing that a connection has been made, or may believe that he or she is connecting to his or her own home or office network when instead he or she is connecting to a third-party's network. This article will focus on joyriders, because most of the laws discussed in this article require that a user engage in some type of intentional "access."[8] War-drivers typically do not meet the "access" requirement, and accidental use does not constitute the "intentional" access required by most statutes. This article, however, will point out a few existing laws that may apply to war-driving or accidental use.

The roaming Wi-Fi users discussed in this article are to be distinguished from "whackers," who, for purposes of drawing a bright line in this article, will be defined as users who intentionally access a Wi-Fi network for destructive, malicious, theft or espionage purposes. The term "hacker" is popularly used in the media to refer to a malicious computer or network user, although use of the term in technology circles is considerably more nuanced.[9] A "whacker" is a hacker that uses wireless technology. Whackers would include those

---

random unsecured Wi-Fi networks, its proponents were quick to note the similarity to wardialing, and thus termed their new activity "war-driving." Software used in war-driving may be "passive," meaning that it collects only information generally broadcast by an access point, or may use varying degrees of active probing.

8. Am. Online, Inc. v. Nat'l Health Care, 121 F. Supp. 2d 1255, 1272–73 (N.D. Iowa 2000) (finding that to "access" means "to exercise the 'freedom or ability to . . . make use of' something," and that "when someone sends an e-mail message from his or her own computer, and the message then is transmitted through a number of other computers until it reaches its destination, the sender is making use of all of those computers, and is therefore 'accessing' them." (citing MIRRIAM-WEBSTER'S COLLEGIATE DICTIONARY 6 (10th ed. 1994)). Using a Wi-Fi network to gain Internet access is therefore likely to be considered "access" to the network. War-drivers who passively scan for access point beacon frames likely do not "access" these access points, although war-drivers who use more active scanning and probing methods may arguably be deemed to engage in "access." Active scanners may be treated more like those this article calls joyriders than like war-drivers.

9. *See* Ryan, *supra* note 7.

who would otherwise be joyriders, but who engage in activities such as spamming, or other independently illegal activities like sharing copyrighted files or accessing illegal pornography. Existing laws apply to whackers in the same way that they apply to any non-wireless user who accesses, steals, modifies, or deletes data, or otherwise takes actions to harm a computer or data. A detailed discussion of laws that apply to hacking behavior is beyond the scope of this article.

II. THE CASE FOR ROAMING WI-FI USE

Roaming Wi-Fi use is an important evolutionary step in the development and expansion of the exchange of information enabled by the Internet. The value of this method of accessing the Internet lies primarily in its enhancement of the timeliness, frequency, convenience, and flexibility of connecting to the Internet. This value is exponentially increased by expansion of the number and distribution of accessible Wi-Fi networks. However, the value of roaming Wi-Fi use must be evaluated in light of the economic costs of this behavior, the security implications of permitting use that has not been expressly authorized, and the idea that a network operator could be held liable for the actions of a roaming Wi-Fi user or whacker that accesses the Internet through the operator's network. Ideally, laws applicable to roaming Wi-Fi use will facilitate and encourage roaming, while deterring destructive behavior and providing remedies to any network operator injured by a malicious or destructive user.

A. Value to Individuals and Society

The primary value of roaming Wi-Fi access lies in its expansion of the number and type of locations from which a user can find immediately accessible high-speed Internet access. In the last decade, the Internet has revolutionized communication, created countless business efficiencies and dramatically accelerated the growth of the body of human knowledge. The Supreme Court has recognized that "[t]he Internet is 'a unique and wholly new medium of worldwide human communication'" through which "at any given time 'tens of thousands of users are engaging in conversations on a huge range of subjects.'"[10] The Supreme Court further recognized that "[t]he Web is thus comparable . . . to both a vast library including millions of

10. Reno v. Am. Civil Liberties Union, 521 U.S. 844, 850, 852 (1997) (*citing* Am. Civil Liberties Union v. Reno, 929 F. Supp. 824, 844 (E.D. Pa. 1996)).

readily available and indexed publications and a sprawling mall offering goods and services," and that the Internet contains content "as diverse as human thought."[11] Congress has found that the Internet offers "a forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity."[12]

Internet access experienced its most dramatic growth to date as it expanded beyond labs and universities to homes and offices. Wireless technologies (primarily Wi-Fi, and for limited but expanding purposes, cellular technologies) have been the primary driving force in the further expansion of Internet access, as they have allowed users to move first to living rooms, kitchens, and conference rooms, and more recently, to public areas including parks, restaurants, coffee shops, airports, and convention centers. This expansion improves many of the advantages that the Internet has already created, by allowing for the more timely, frequent, and convenient exchange of ideas and information. The expansion of Internet access into public places facilitated by Wi-Fi also creates opportunities to use the Internet for new and novel ways of interacting, and new applications.

Open commercial and residential Wi-Fi networks are widespread and common in urban areas. To a business traveler, student, web log (or "blog") author or any other person for whom the Internet is a critical tool, the ability to access a Wi-Fi network, whether for-pay, or shared by a commercial or residential network operator, can add flexibility to a user's schedule, facilitate productive use of otherwise wasted time, and provide for efficient and timely use of information. A user that is able to find and use a Wi-Fi network may be able to avoid the need for a trip back to the office to synchronize e-mail or obtain driving directions. A user forced to wait in a car or in a waiting room where open Wi-Fi signals are available might be able to turn more downtime into productive time. A traveler on the road may be able to obtain updated sales, projection, or pricing information in a more timely way. The aggregate value of this access to Wi-Fi users is difficult to quantify, but research projections anticipate that Wi-Fi users will be prepared to spend $1.4 billion for paid roaming Wi-Fi access in the United States by 2009.[13]

---

11. *Id.* at 852–53.

12. 47 U.S.C.A. § 230(a)(3) (West 2001).

13. *Free Hotspots Restrict Revenues for Wi-Fi Service Providers*, Frost & Sullivan, *at* http://www.frost.com/prod/servlet/press-release.pag?docid=5115637&ctxixpLink=FcmCtx6&ctxixpLabel=FcmCtx7 (July 31, 2003).

The fact that shared Wi-Fi access may be free for a roaming user also contributes to the importance of this method of access. One reason for the Internet's success and for its contributions to higher learning is that it started as a free tool for scientists, academics, and students. Shared Wi-Fi access has great value in allowing this tradition to continue, both in university-sponsored venues and off-campus, as well. A student who chooses to write a paper at a coffee shop or late-night pancake house may be able to continue research while writing if given the ability to connect his or her laptop to the Internet. There are also instances in which roaming use of Wi-Fi could potentially provide high-speed access to populations that wouldn't ordinarily be able to afford this access.

Metcalfe's law, a principle attributed to Dr. Robert Metcalfe, the inventor of Ethernet networking technology, argues that the value of a network increases exponentially with the addition of each additional interconnection to the network.[14] Metcalfe's "law" is based on Metcalfe's anecdotal observation that "[c]onnected 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."[15] Community networking facilitated by laws favorable to roaming Wi-Fi provides an example of exponentially increasing value. Assume that four home Wi-Fi network operators open their networks to allow access by each other. At a minimum, each of these users would then have the ability to access the Internet wirelessly from four locations, instead of one. In the aggregate, the addition of these four operator/users would facilitate sixteen unique access possibilities. Glenn Fleishman, a prominent journalist and blogger on Wi-Fi topics, described an application of Metcalfe's law to Wi-Fi as follows:

> Wireless networks require substantial innovation and expense in developing the basic technology, but then each additional node has substantially less cost associated than with increasing a wireline network, whether in an office or across a city. Wireless reduces the friction in accelerating the density of network, and that rollercoaster ride into exponential power is where speed freaks get their high.[16]

---

14. George Gilder, *Metcalfe's Law and Legacy*, FORBES ASAP 158 (Sept. 13, 1993), *available at* http://www.seas.upenn.edu/~gaj1/metgg.html.

15. Bob Metcalfe, *There Oughta Be a Law*, N.Y. TIMES ON THE WEB, July 15, 1996, *at* http://www.nytimes.com/library/cyber/week/0715laws.html.

16. Glenn Fleishman, *Newsweek's Focus on Wireless*, Wi-Fi Networking News, *at* http://wifinetnews.com/archives/2004_05.html (May 31, 2004).

A recent California Supreme Court decision recognizes the danger posed by restrictions that could serve to decrease free use of the Internet. The court cited Lawrence Lessig's observation that an online marketplace

> benefits greatly from a network that is open and where access is free. It is this general feature of the Net that makes the Net so valuable to users and a source of great innovation. And to the extent that individual sites begin to impose their own rules of exclusion, the value of the network as a network declines. If machines must negotiate before entering any individual site, then the costs of using the network climb.[17]

Wi-Fi access represents one of the latest innovations in the expansion of the power of the Internet. Other new networking technologies, such as mesh networking and the use of ad hoc networks between individual computing devices facilitated by wireless technologies, promise to continue this expansion by allowing computing devices to instantly establish communications with a minimum of formality and overhead. It is important to recognize that resolution of the controversy surrounding opportunistic Wi-Fi use, from both technological and legal perspectives, could impact the growth of future technologies.

The Internet may prove to be the most significant factor in enabling the growth of human knowledge since the printing press. It has also created efficiency and expanded opportunities in countless business and personal situations. Roaming use of Wi-Fi connections promises to enhance the value of the Internet to many users, and may create invaluable new opportunities. Laws must recognize and encourage this value creation.

B. Economic Cost

A roaming Wi-Fi user obtains broadband Internet access service, a valuable resource, without paying compensation. However, the marginal cost of the bandwidth used by a roaming Wi-Fi user to the business or individual operator of the Wi-Fi network is typically negligible. Many broadband connections are offered on a flat-fee basis for a given amount of bandwidth, which places *no* practical restriction on the total amount of data that may be transferred using the connection during a given month, but restricts the amount of data that could be transmitted at one time. A typical broadband customer

17. Intel Corp. v. Hamidi, 71 P.3d 296, 310–11 (2003) (*citing* LAWRENCE LESSIG, THE FUTURE OF IDEAS: THE FATE OF THE COMMONS IN A CONNECTED WORLD 171 (2001)).

uses only a fraction of the bandwidth allocated to the customer in a given month. Use of a Wi-Fi network on an itinerant basis for reasonable e-mail and web surfing consumes only a small amount of bandwidth, and therefore should not disrupt the operator's use of his own network in any way.

Calling roaming Wi-Fi access "free," however, does not take into consideration the cost to the Internet service provider that makes service available to a Wi-Fi network operator. Regardless of whether the network operator pays a fixed cost for access, additional usage of the Internet service could have an impact on the Internet service provider's capacity and infrastructure usage and planning. Sharing an Internet connection can increase the level of usage beyond what is anticipated or economical for an Internet service provider. In addition, it is possible that someone who discovers an accessible Wi-Fi connection from his or her residence or business may forego obtaining service individually, and instead rely on using his or her neighbor's service. It is important to note, however, that roaming Wi-Fi use typically does not provide a user with a substitute for home or office access. T-Mobile USA, one of the largest hotspot operators in the United States, has reported that 90% of its Wi-Fi service subscribers have high-speed Internet access at home.[18]

For these reasons, many Internet service providers provide service subject to terms of use or acceptable use policies that impose rules about how a connection may be used, including restrictions on sharing. Internet service providers have the ability to structure terms of service to permit or prohibit sharing, as appropriate to meet their individual economic models and experience with bandwidth usage. Providers can also use terms of service as a way to differentiate their services from their competitors' services. Several service providers have taken prominent positions in this respect. Time Warner Cable has made its prohibition of Wi-Fi connection sharing clear by sending cease and desist letters to a number of its subscribers who had listed their open Wi-Fi networks in a database maintained for the NYCWireless users' group.[19] Conversely, Speakeasy, a Seattle-based Internet service provider, advertises that it expressly permits Wi-Fi

18. *T-Mobile, Comcast team on hot-spot service* (Feb. 2, 2004), RCR Wireless News, *at* http://www.rcrnews.com/cgi-bin/news.pl?newsId=16736.

19. Letter from Gregory Powell, Abuse & Security, Supervisor, High Speed Online Services, Time Warner Cable of NYC (June 25, 2002), *available at* http://www.serebin.com/ben/wireless/TWC_Wireless_Response.jpg.

connection sharing, and in fact, supports billing of third-parties in the event that a network operator wishes to charge for shared access.[20]

Responsibility for complying with a service provider's terms of use must lie with the network operator, who has the opportunity to read and understand a service provider's terms of service, and to choose a provider with terms that meet the operator's needs. A roaming user, whether intentionally or unintentionally provided access by a Wi-Fi network operator, will have no way to know whether the connection sharing was permitted by the operator's Internet service provider.

Roaming Wi-Fi access could also have an impact on the operators of for-pay hotspots. In some cases, this impact has come in the form of healthy competition. Some for-pay operators have begun to offer additional valuable services to justify the additional cost of a for-pay hotspot. For example, for-pay operators can offer more visibility and certainty in being able to locate a hotspot. These operators may offer a higher quality of service and user support. Some hotspot operators offer value-added services including streaming music or video, higher and more dependable bandwidth levels, and security features. In many cases, however, free and for-pay networks do not compete. For-pay hotspots are typically located in highly-traveled areas, while shared hotspots can be located anywhere. Part of the value in supporting the use of open Wi-Fi networks is that open networks may permit a roaming Wi-Fi user to get Internet access from places that have not been identified as prime locations by commercial Wi-Fi providers.

Sharing a connection with roaming Wi-Fi users, or operating an unsecured network that is accessible to roaming Wi-Fi users, often will not cost the operator anything out-of-pocket, and is not likely to noticeably reduce the operator's available bandwidth or performance. In the event that the network operator experiences adverse effects from sharing, the operator can easily enable encryption on its network or otherwise control access to its network. A service provider can protect itself by creating terms of service that appropriately reflect its expectations regarding its customers' use of its service. The direct economic costs of roaming Wi-Fi usage do not, therefore, present a compelling justification for prohibiting roaming users from accessing open Wi-Fi connections.

---

20. Duffy Hayes, *Speakeasy not only encourages connection sharing. . .It promotes it*, About Speakeasy, *at* http://www.speakeasy.net/press/news/news111902.php.

C. Security Concerns

Some people argue that roaming Wi-Fi use should be prohibited because it creates security risks. Open Wi-Fi networks can, under some circumstances, provide network access to a person who uses that access to intercept data traveling over the network, to read, copy, delete, or modify files in shared directories on the network, or to engage in other whacking behavior. In one recent case, several men pled guilty to violations of the CFAA and other statutes after accessing credit card information stored in the computer systems of Lowe's hardware store by accessing a store's open Wi-Fi network from the parking lot of the store.[21]

Because the defendants in the Lowe's case caused damage via an open Wi-Fi network, it may seem that an adequate solution is to restrict roaming Wi-Fi access. However, laws prohibiting roaming Wi-Fi access could actually undermine network security on a large scale. Laws that purport to protect networks may give network operators a false sense of security. A network operator who relies on the law to protect his or her network against unwanted access may not take reasonable or appropriate technical measures to secure the network.

The New York legislature determined that the best approach to encouraging network security was to impose a certain level of responsibility on network operators. New York's statute prohibiting unauthorized computer use provides protection only if the computer or network operator has implemented security measures.[22] This requirement was included in the statute "'in order to encourage greater self-protection on the part of the computer industry.'"[23] As a New York court considering this provision summarized, "The legislative history of the statute makes clear that this requirement was included on the ground that '[s]uch protective devices provide the

21. *See* Bill of Indictment, United States v. Salcedo et al., (No. 5.03cr53-MCK) (W.D.N.C. Nov. 19, 2003); Criminal Docket for Case #: 03-CR-53-ALL, *available at* http://pacer.ncwd.uscourts.gov/dc/cgi-bin/pacer250.pl?puid=01094528557 (last visited Sept. 16, 2004); Entry and Acceptance of Guilty Plea (Rule 11 Proceeding), United States v. Salcedo, (No. 5:03cr53-McK) (W.D.N.C. June 4, 2004); Entry and Acceptance of Guilty Plea (Rule 11 Proceeding), United States v. Botbyl, (No. 5:03cr51-V) (W.D.N.C. June 7, 2004).

22. *See generally*, N.Y. PENAL LAW § 156.05 (McKinney 1999).

23. People v. Angeles, 687 N.Y.S.2d 884, 886 (N.Y. Crim. Ct. 1999) (*citing* WILLIAM C. DONNINO, MCKINNEY'S CONSOLIDATED LAWS OF NEW YORK Book 39 at 284, PRACTICE COMMENTARY TO PENAL LAW ARTICLE 156 (1999)).

first line of defense against unauthorized intrusion into a computer system.'"[24]

An operator that desires to prevent roaming users from accessing the Internet through its network can easily turn on encryption, which would prevent such access, or can implement alternative methods of security that would allow access to some, but not all, of the operator's network. All access points that bear Wi-Fi certification are capable of supporting a basic encryption method called WEP ("Wired Equivalent Privacy") with a few keystrokes. Although WEP has proven vulnerable, the use of WEP still provides protection against all but serious attackers, and clearly indicates to prospective users that access is to be prohibited. Successors to WEP, such as WPA ("Wi-Fi Protected Access"), and a new standard called 802.11i, provide improved security measures. An operator may alternatively leave portions of his or her network open and instead implement measures to secure sensitive data using virtual local area networks ("VLANs"), firewalls, or other security devices.

Several areas of law, in addition to New York's unauthorized computer use statute, promote responsible security practices by providing protection only when a user has taken security measures. The Fourth Amendment's protection against unreasonable search and seizure, for example, requires that a user have a reasonable expectation of privacy in materials in order for those materials to be protected. Another example of a statutory approach that requires a user to take steps for his or her own protection is found in the Uniform Trade Secrets Act, which provides protection only for information that "is the subject of efforts that are reasonable under the circumstances to maintain its secrecy."[25]

Expecting network operators to configure their networks with an appropriate level of security does not place an unreasonable additional burden on these operators. Most Wi-Fi network operators also have broadband connections to the Internet. Broadband connections, like Wi-Fi networks, may open a network to access by others, and require that a user take some level of security measures to protect sensitive data on the network. In fact, in the context of applying the Fourth Amendment, one court held that a computer user does not have a reasonable expectation of privacy in information contained on a computer that is connected to a shared broadband

24. *Id.* (citing Mem. of the Att'y Gen., 1986 N.Y. Legis. Ann. 232, 233 (supporting L.1986, ch. 514).

25. UNIFORM TRADE SECRETS ACT, § 1(4)(ii)(1985).

network, and on which file and print sharing are enabled.[26] A Wi-Fi network operator will typically either already have implemented security measures on the network, and will be familiar with basic security concepts prior to adding Wi-Fi access to the network, or will have a network that already allows a certain amount of access to data. In the latter case, an open Wi-Fi network would provide an additional means of accessing such data, but would not make otherwise secure data insecure. A law that prohibits access to open networks will be far less effective in improving security than a law that encourages a network operator to adopt security practices appropriate for protecting its sensitive data.

A recent law review article entitled *War, Peace, or Stalemate: Wargames, Wardialing, Wardriving, and the Emerging Market for Hacker Ethics* additionally suggests that war-driving, like other forms of "ethical" hacking, can be used as a tool for improving network security.[27] By finding and publishing lists of open access points, a war-driver may alert the operator of a network to vulnerabilities that were not intended, and had not previously been appreciated.

D. Liability Risks

Another justification for preventing roaming Wi-Fi use is the possibility that a network operator might face liability for the unlawful acts of a third-party that accesses the Internet through the operator's network. This justification is largely without merit because Internet-related legislation has clarified that those who provide access to the Internet to third-parties are not liable for the acts of these third-parties.

Time Warner Cable, in a letter sent to subscribers of its high-speed Road Runner service who shared the service using Wi-Fi, stated, "Individuals using the Road Runner system in this manner to carry out criminal activity, would be able to do so in an anonymous manner. In such circumstances, when law enforcement attempted to trace such activity, the trail would end with your account."[28] The media has reported instances in which Wi-Fi networks were used to access or distribute illegal materials over the Internet. A Wi-Fi network operated by an AT&T Wireless subscriber was reportedly

26. U.S. v. Kennedy, 81 F. Supp. 2d 1103, 1110 (D. Kan. 2000).

27. *See* Ryan, *supra* note 7.

28. Gregory Powell, Abuse & Security, Supervisor, High Speed Online Services, Time Warner Cable of NYC (June 25, 2002), *available at* http://www.serebin.com/ben/wireless/TWC_Wireless_Response.jpg.

used by a neighbor of the subscriber to distribute an illegally copied version of a movie.[29] In Canada, a man was arrested for allegedly accessing child pornography from his car, using a Wi-Fi network from a nearby house.[30] A "war spammer" reportedly reached a deal with Federal prosecutors to plead guilty to violations of the Federal CAN-SPAM Act after allegedly sending large volumes of commercial e-mail through open Wi-Fi access points.[31]

That open Wi-Fi access points have been used in connection with the commission of crimes is unfortunate, but warrants neither a restriction on use of open connections nor the imposition of liability on a network operator who leaves a connection open. Like the Internet, roaming use of Wi-Fi expands the ways in which information may be used and distributed, and creates new opportunities for criminal behavior and anonymity. A North Dakota District Court summed up the argument as follows:

> On the one hand, the ability of individual users to log onto the Internet anonymously, undeterred by traditional social and legal restraints, tends to promote the kind of unrestrained, robust communication that many people view as the Internet's most important contribution to society. On the other hand, the ability of members of the public to link an individual's online identity to his or her physical self is essential to preventing the Internet's exchange of ideas from causing harm in the real world. The legislative resolution of these issues will, indirectly, shape the content of communication over the Internet. For now, the [sic] §230 of the Communication Decency Act errs on the side of robust communication . . . .[32]

Use of Wi-Fi connections for criminal purposes, like use of the Internet for such purposes, should be addressed by targeting the underlying criminal behavior, rather than by restricting the otherwise valuable means by which the crime was accomplished.

Legislators have recognized that entities providing access to the Internet should not be liable for the crimes committed through such

---

29. Ben Charny, *Wi-Fi users warned of pirates*, CNET News, *at* http://news.com.com/2100-1033_3-947496.html (July 31, 2002).

30. Richard Shim, *Wi-Fi arrest highlights security dangers*, CNET News, *at* http://news.com.com/2100-1039-5112000.html (Nov. 28, 2003).

31. *See* Kevin Poulsen, *Plea deal in 'war spamming' prosecution*, SecurityFocus, *available at* http://www.securityfocus.com/news/9453 (Sept. 3, 2004).

32. PatentWizard, Inc. v. Kinko's, Inc. 163 F. Supp. 2d 1069, 1071-72 (D.S.D. 2001) (citing LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 14–17, 24–29 (Basic Books (2000)).

access. The types of behavior most often identified as creating potential liability are transmission of copyrighted materials, transmission or receipt of pornography, and spamming. The Digital Millennium Copyright Act ("DMCA")[33] and Communications Decency Act ("CDA")[34] both include safe harbors that clarify that Internet service providers are not liable for content transmitted through their services, potentially including all of the types of content referred to above. While the DMCA has certain requirements that typically will not be met by operators of open networks, pre-DMCA case law makes clear that network operators that do not have knowledge of the content passing through their networks have little danger of being liable for copyright infringement. The Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 ("CAN-SPAM")[35] clarifies that liability for spam sent by a user of an open Wi-Fi network would rest with the user, not the network operator.

The DMCA[36] provides that an entity offering connections for digital online communications will not be liable for copyright infringement damages with respect to materials transmitted through the network, provided that certain conditions are fulfilled. These conditions include that: (i) the transmission of the material is initiated at the direction of a person other than the service provider; (ii) the transmission is carried out through an automatic technical process without selection of the material by the service provider; (iii) the service provider does not select the recipients of the material; (iv) no copy of the material is maintained on its system or network; and (v) the material is transmitted without modification of its contents.[37] This safe harbor is available, however, only if the service provider adopts policies that provide for termination of service to repeat infringers and informs subscribers and account holders of such policies.[38] Section 512(l) clarifies that a failure to comply with this safe harbor does not adversely affect any other defense a service provider may have to liability for copyright infringement.[39]

Even without the safe harbor, it is unlikely that an operator of an open Wi-Fi network could be held liable for direct, contributory, or

33. 17 U.S.C.S. § 512 (West Supp. 2004).
34. 47 U.S.C.S. §§ 201 *et seq.* (LexisNexis Supp. 2004).
35. 15 U.S.C.S. §§ 7701 *et seq.* (LexisNexis Supp. 2004).
36. 17 U.S.C.A. § 512 (West Supp. 2004).
37. *Id.* § 512(a).
38. *Id.* § 512(i).
39. *Id.* § 512(l).

vicarious copyright infringement. Direct infringement requires that a person actually engage in the conduct causing infringement.[40] Contributory infringement requires that a network operator have knowledge that infringing materials are being transmitted, and that the operator induce, cause, or materially contribute to the infringing conduct.[41] Vicarious liability would require that a network operator have the ability to supervise the infringing activity and have a financial interest in the exploitation of copyrighted materials.[42]

Because the operator of an open Wi-Fi network would generally have no knowledge of what materials are transmitted over the network, and no participation in the behavior of users of its network or opportunity to supervise such behavior, the operator will likely not face liability for copyright infringement.

Section 230(c)(1) of the CDA[43] provides that "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." This section has been broadly interpreted to prevent a service provider from being liable for a range of non-intellectual property-related state law claims, including negligence, defamation, interference with prospective business relationships, obscenity and child pornography, waste of public funds, nuisance, premises liability, and unfair business practices.[44] If an operator of an open network constitutes a provider of an "interactive computer service," which expressly includes a service or system that provides access to the Internet,[45] then the operator presumably is immune to a broad range of claims (other than intellectual property claims) based on the actions of the users of its network.

---

40. CoStar Group, Inc. v. LoopNet, Inc., 373 F.3d 544, 550 (4th Cir. 2004).

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

42. *CoStar Group, Inc.*, 373 F.3d at 550; Shapiro, Bernstein & Co. v. H.L. Green Co., 316 F.2d 304, 307 (2d Cir. 1963).

43. 47 U.S.C.A. § 230(c)(1) (West 2001).

44. *See e.g.*, Ben Ezra, Weinstein and Co., Inc. v. Am. Online, Inc., 206 F.3d 980, 984 (10th Cir. 2000) (barring state law claims for negligence and defamation); Zeran v. Am. Online, Inc., 129 F.3d 327, 330 (4th Cir. 1997) (regarding defamation); PatentWizard, Inc. v. Kinko's, Inc. 163 F. Supp. 2d 1069, 1071 (D.S.D. 2001) (barring state law claims for defamation, negligence and interference with prospective business relationships); Blumenthal v. Drudge, 992 F. Supp. 44 (D.D.C. 1998) (barring claims for negligence and defamation); Kathleen R. v. City of Livermore, 104 Cal. Rptr. 2d 772, 775–76 (Cal. Ct. App. 2001) (wasting of public funds, nuisance and premises liability); Stoner v. eBay Inc., 56 U.S.P.Q.2d (BNA) 1852 (Cal. Super. Ct. 2000) (discussing unfair business practices); Doe v. Am. Online, Inc. 718 So. 2d 385, 389 (Fla. Dist. Ct. App. 1998) (regarding negligence, obscenity and child pornography).

45. 47 U.S.C.A. § 230(f)(2) (West 2001).

A recent California state court decision, *Grace v. eBay, Inc.*, interpreted the immunity provided by the CDA narrowly, in conflict with decisions of the Fourth, Tenth, and D.C. Circuits.[46] The California court held that the CDA immunity protects those traditionally classified as "publishers" because of their editorial involvement in making materials available, but it does not protect "distributors" who merely forward materials, in the event that the distributor becomes aware that it is distributing injurious content.

The *Grace* case suggests that an operator could potentially face liability if the operator is notified of the transmission of injurious content through its network, but does not take measures to block future access by the party transmitting such material. Similarly, *Stoner v. eBay, Inc.*, a case in which eBay was notified that illegally copied audio materials were being distributed on its marketplace, but failed to prevent such material from being distributed, suggests that an operator may face liability for infringing content transmitted through its network, if it has knowledge of such content.[47] The California Superior Court's opinion in *Stoner* stated that:

> There is, to be sure, some point at which the existing immunity would no longer apply. Although the limits of the immunity have not yet been clearly defined, any limitation placed on the immunity presumably would begin at the point at which providing otherwise lawful goods or services with knowledge that they are being put to an illegal use becomes the commission, or the aiding and abetting, of a crime. Criminal liability in such circumstances normally requires the intent to further or facilitate the crime.[48]

The Federal CAN-SPAM Act of 2003,[49] which supersedes state spam legislation, creates liability for the transmission of unsolicited commercial e-mail. Among other things, CAN-SPAM prohibits the knowing and intentional initiation of multiple e-mail messages from a computer or network that has been accessed without authorization,[50] the knowing relay or retransmission of multiple e-mail messages with

---

46. Grace v. eBay Inc., 16 Cal. Rptr. 3d 192, 198–99 (Cal. Ct. App. 2004). *But see Ben Ezra, Weinstein and Co., Inc.*, 206 F.3d 980; *Zeran*, 129 F.3d at 330; *Blumenthal*, 992 F. Supp. at 52–53.

47. 56 U.S.P.Q.2d (BNA) 1852 (Cal. Super. Ct. 2000)

48. United States v. Blankenship, 970 F.2d 283, 287 (7th Cir. 1992); People v. Beeman, 674 P.2d 1318, 1325 (1984); *Stoner*, 56 U.S.P.Q.2d (BNA) at 1855 (*citing* People v. Lauria, 59 Cal. Rptr. 628, 631 (Cal. Ct. App. 1967).

49. 15 U.S.C.A. §§ 7701–13 (West Supp. 2004).

50. *Id.* § 7704(a)(2).

the intent to deceive others as to the origin of such messages,[51] and the knowing relay or retransmission of various types of fraudulent e-mail from a computer that has been accessed without authorization.[52] Initiation is expressly defined to exclude "transmission, routing, relaying, handling, or storing, through an automatic technical process, of an electronic mail message for which another person has identified the recipients or provided the recipient addresses."[53] While it appears that a user of an open network could be held responsible for sending spam under this Act, a network operator will neither initiate the transmission of messages nor knowingly forward spam. Federal prosecutors recently reached a plea bargain with a spammer who allegedly used open networks to distribute spam in violation of CAN-SPAM.[54]

Whether or not the CDA, DMCA, and CAN-SPAM Acts expressly apply to all materials that may be transmitted through an open Wi-Fi network, courts have recognized that Congressional intent to absolve service providers has been very broad. As the Fourth Circuit observed:

> Congress made a policy choice . . . not to deter harmful online speech through the separate route of imposing tort liability on companies that serve as intermediaries for other parties' potentially injurious messages . . . . Section 230 was enacted, in part, to maintain the robust nature of Internet communication and, accordingly, to keep government interference in the medium to a minimum.[55]

III. APPLICATION OF EXISTING LAW

An e-mail distributed in July of 2002, and attributed to an FBI Special Agent stated that:

> Identifying the presence of a wireless network may not be a criminal violation, however, there may be criminal violations if the network is actually accessed including theft of services, interception of communications, misuse of computing resources, up to and including violations of the Federal Computer Fraud and

51. *Id.* § 7704(a)(1).
52. *Id.* § 7704(b)(3).
53. *Id.* § 7702(9), (15).
54. *See* Poulsen, *supra* note 31.
55. Zeran v. Am. Online, Inc., 129 F.3d 327, 330–31 (4th Cir. 1997).

> Abuse Statute, Theft of Trade Secrets, and other federal violations.[56]

This e-mail differentiates between war-driving and other types of roaming Wi-Fi use, but does not distinguish between using a connection solely for Internet connectivity and using a connection to gain access to data. This statement will likely have a chilling effect on users' willingness to use open Wi-Fi networks to obtain an Internet connection, including networks that are intentionally shared.

This article has argued that the law should continue to encourage the development and expansion of the Internet and the general accessibility of the Internet from new venues that will enhance the Internet's value to users. The utility of roaming Wi-Fi to users and the value of encouraging expansion of the Internet's accessibility, even when considered in light of the economic cost of this access, security concerns, and potential liability of network operators, suggest that the law should not unreasonably restrict the use of open Wi-Fi networks or contain ambiguity that would deter users from using these networks. This section of the article will explore the treatment of roaming Wi-Fi use under federal and state statutes and the common law. While many of these laws do not appear to apply to roaming Wi-Fi use, some statutes may apply, depending on whether such use is considered intentional, unauthorized use. This section identifies four approaches courts and legislators have taken to determining whether use is intentional and unauthorized, and applies each of these tests to roaming Wi-Fi use.

A. Federal Law

1. The Computer Fraud and Abuse Act of 1986

The Computer Fraud and Abuse Act of 1986 ("CFAA")[57] prohibits unauthorized access to a computer or network in a number of specific situations. In order to violate the most widely applicable provisions of the CFAA, a user must intentionally access a network without authorization, and must either obtain information or cause damage and a loss exceeding a threshold amount. This section will examine several approaches to determining whether a user has intentionally accessed a network without authorization. This section concludes that it is possible that a joyrider could be considered to

---

56. E-mail from Bill Shore, Special Agent, FBI (July 8, 2002), *available at* http://www.stumbler.net/fbi.php.

57. 18 U.S.C. § 1030 (2000).

intentionally access a network without authorization under some tests used by courts. While it is possible that a court could hold that a user met the other requirements of the CFAA—that the user obtain information or cause damages and $5,000 of loss—this result is unlikely.

The CFAA is a wide-ranging statute that contains prohibitions on specific types of computer access, including access that threatens national security,[58] furthers fraud or extortion,[59] compromises financial records, or transmits computer viruses or other destructive code.[60] Most of these types of prohibited access are targeted squarely at the activities of hackers and whackers.

The CFAA does, however, contain more broadly-applicable provisions. Among other things, the CFAA prohibits intentional, unauthorized access to a computer or network, where the person accessing the computer obtains information or causes damage. This article will discuss Sections 1030(a)(2) and 1030(a)(5)(A) of the CFAA. Section 1030(a)(2) applies to anyone who:

> (2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains— . . . (C) information from any protected computer if the conduct involved an interstate or foreign communication . . . .[61]

Section 1030(a)(5) imposes penalties on anyone who:

> (5)(A)(i) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;
>
> (ii) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or
>
> (iii) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage; and
>
> (B) . . . caused . . . (i) loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value. . . .[62]

---

58. *Id.* § 1030(a)(1).

59. *Id.* § 1030(a)(4).

60. *Id.* § 1030(a)(5)(A).

61. *Id.* § 1030(a)(2).

62. 18 U.S.C. § 1030(a)(5)(A) (2000 & Supp. 2004). Subsections 1030(a)(5)(A)(ii) and (iii) appear redundant, in that any activity that violates clause (ii) would necessarily violate

The application of the CFAA to roaming Wi-Fi users requires a more detailed analysis of the following factors: (i) whether the user's conduct involved intentional, unauthorized access; (ii) whether the person obtained information from a protected computer; and (iii) whether the person's conduct caused damage and a loss exceeding a $5,000 threshold. The generally-applicable portions of the CFAA require intentional access to a "protected computer," which would appear to include any computer (and its associated network) connected to the Internet.[63] Before examining these requirements in detail, it is helpful to consider the background assumptions and context underlying the concept of authorization.

a. Distinguishing Between Authorized and Unauthorized Access

Determining whether a user has engaged in intentional, unauthorized access is critical to an analysis of whether a roaming Wi-Fi user is likely to face liability under the CFAA, many state laws, and the common law tort of trespass to chattels. For purposes of this inquiry, it is helpful to examine both the CFAA and the common law, as courts have looked to common law principles in determining whether access should be considered authorized under the CFAA.[64]

Before the Internet and wireless networking technologies became widely-used means of transmitting data, networks were generally private. Someone accessing a network or computer typically had to gain physical access to network components by entering a facility and using an on-premises computer, or by tapping a network cable.[65] Remote access to private networks usually had to be

---

clause (iii). These sections are separated in the statute because more stringent penalties apply to clause (ii), which requires a "reckless" state of mind.

63. See 18 U.S.C. § 1030(e) (2000 & Supp. 2004) which defines a "protected computer" as a computer "used in interstate or foreign commerce or communication"; *see also* A. HUGH SCOTT, COMPUTER AND INTELLECTUAL PROPERTY CRIME: FEDERAL AND STATE LAW 90 (BNA 2001) ("This broad definition of protected computer combined with the ever-expanding use of the Internet has brought a considerable number of computers, including home computers with online access, within the CFAA's reach. Although no court has interpreted this language, it appears that connecting a computer to the Internet would make the computer one used 'in interstate or foreign communications.'").

64. *See* Theofel v. Farey-Jones, 341 F.3d 978, 982–86 (9th Cir. 2003) (analyzing common law trespass principles in holding that a user's access was unauthorized under the Stored Communications Act and under CFAA). *But see* In re Am. Online, Inc., 168 F. Supp. 2d 1359, 1370–71 n.8 (S.D. Fla. 2001) ("[T]he 'cluster of ideas' associated with common law 'trespass' cannot be imported into CFAA.").

65. *See* N. Tex. Preventive Imaging, L.L.C. v. Eisenberg, No. SA CV 96-71AHS(EXX), 1996 WL 1359212, at *5 (C.D. Cal. Aug. 19, 1996) ("Thus while the pre-1994 CFAA was

enabled by a technical professional and required a login mechanism or password. The lines between authorized and unauthorized access were fairly clear, except with respect to service providers and former service providers who exceeded authorized access,[66] or with users who obtained authorization to access through fraudulent means.[67] In enacting the CFAA, Congress distinguished between access by "outsiders" or "outside hackers" and by "insiders," as a proxy for determining which users were unauthorized and which were authorized.[68] This straightforward distinction reflects the physical nature of pre-Internet and pre-wireless networking. It becomes confusing, however, when applied to public networks. Courts have attempted to apply the insider/outsider distinction to website access.[69] Courts have alternately shown some confusion as to this approach,[70] or acknowledged that amendments to the statute may have implicitly made this approach obsolete.[71]

Publicly accessible networks, which were not common or widely used when the CFAA was enacted in 1986, have become prominent with the rise of the Internet. Most recent cases dealing with allegedly unauthorized access to Internet websites have recognized that access to publicly-accessible areas of the Internet can be considered

---

directed towards the unauthorized 'access' of a computer system, presumably by modem or by direct keyboard entry, the post-1994 CFAA is directed towards a broader range of conduct by which a person knowingly 'causes' the 'transmission' of a program, information, code, or command to a computer.").

66. EF Cultural Travel BV v. Zefer Corp., 318 F.3d 58, 62 (1st Cir. 2003); Pac. Aerospace & Elecs., Inc. v. Taylor, 295 F. Supp. 2d 1188, 1194 (E.D. Wash. 2003); Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1124 (W.D. Wash. 2000).

67. *See In re Am. Online, Inc.*, 168 F. Supp. 2d at 1370.

68. S. REP. NO. 104-357, at 11 (1996).

69. *See* Am. Online, Inc. v. Nat'l Health Care, 121 F. Supp. 2d 1255, 1273 (N.D. Iowa 2000) ("Similarly, is the member converted from an 'insider' to an 'outsider' for purposes of the CFAA by violating AOL's policies? On the other hand, if AOL members are 'outsiders,' then why would AOL's membership policies apply to them at all?").

70. *See Shurgard Storage Ctrs., Inc.*, 119 F. Supp. 2d at 1127 ("The defendant also maintains the CFAA is limited to 'outsiders' or 'hackers,' and not 'insiders' (employees). Though the original scope of the CFAA was limited to the concerns addressed by the defendant, its subsequent amendments have broadened the scope sufficiently to cover the behavior alleged in this case.").

71. *See id.*; Am. Online, Inc. v. Nat'l Health Care, 121 F. Supp. 2d 1255, 1273 (N.D. Iowa 2000), ("Similarly, is the member converted from an 'insider' to an 'outsider' for purposes of the CFAA by violating AOL's policies? On the other hand, if AOL members are 'outsiders,' then why would AOL's membership policies apply to them at all?").

unauthorized only if the website's terms of use expressly prohibit the type of access the website operator finds objectionable.[72]

As a consequence of the inaccessibility of traditional networks to "outsiders," one might presume that access by someone without a pre-existing relationship with a network operator would be considered unauthorized unless authorization or consent are affirmatively given. By contrast, courts considering access to websites have implicitly assumed that access is authorized unless expressly prohibited. Access to Wi-Fi networks does not fit squarely within either the traditional network model or the website model. Like a website, an open Wi-Fi network can be easily accessed. However, Wi-Fi networks perform some private functions, comparable to the function of a private, wired network, as well as public functions.

Wi-Fi access to the Internet is provided by thousands of individuals, businesses, and governmental bodies without direct compensation.[73] Grass-roots organizations like NYCWireless and Personal Telco (in Portland, Oregon) provide information and resources to individuals who choose to share their own Internet connections using Wi-Fi, with the expectation that they will be able to use networks provided by others when out of their homes or offices. Some coffee shops, restaurants, airports, convention centers, and other venues offer free Wi-Fi access as an amenity or as a means to attract visitors or encourage visitors to stay longer. Cities and other governmental bodies make Wi-Fi Internet access available in public places as a service to their constituents.

Public statements regarding the permissibility of access to open Wi-Fi networks have been mixed. A number of prominent groups have issued public warnings intended to encourage adoption of security practices. Some have intended to discourage joyriding, including the FBI agent quoted above, and Nokia, in characterizing joyriding as "bandwidth robbing."[74] Many groups, primarily companies in the telecommunications business for whom readily accessible free networks represent a threat, have also tried to discourage use of open networks. The *New York Times*' ethicist

72. Register.com, Inc. v. Verio, Inc., 356 F.3d 393, 401–02 (2d Cir. 2004); EF Cultural Travel BV v. Zefer Corp., 318 F.3d 58, 63 (1st Cir. 2003); eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058, 1070 (N.D. Cal. 2000); CompuServe Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1024 (S.D. Ohio 1997).

73. The Wireless Node Database Project, which maintains a publicly-available database of network operators, expressly allows free access to their network comprising 10,072 nodes as of September 23, 2004. *See* www.nodedb.com/unitedstates/?.

74. Middleton, *supra* note 1.

characterized these efforts as the "natural reaction of some institutions . . . to clamp down," but continued, "[b]ut that does not create a moral imperative to defer to those who do. Rather, you may use but not overuse Wi-Fi hot spots you encounter."[75] Assuming that these opposing views provide a fair reflection of the inconsistency in general public perception, a user could reasonably believe that a network operator who leaves its network open intends or expects that roaming users may use the network to access the Internet. At the same time, some roaming users may justifiably be concerned that federal or state laws could criminalize such access.

Because access to Wi-Fi networks falls into an area that does not have obvious parallels under existing law, and because general perceptions as to the permissibility of accessing open Wi-Fi networks are mixed, there is considerable ambiguity as to what constitutes "unauthorized" access to an open Wi-Fi network. An expectation that access to a network is unauthorized only if security measures have been enabled is reasonable. At the same time, ambiguity as to the permissibility and legality of accessing an open network has a chilling effect that may prevent users from accessing intentionally shared networks.

b. The CFAA's Intent Requirement

The CFAA requires a "wrongful intent" in accessing a network for a user to be convicted under the statute.[76] Courts interpreting the statute assess the culpability of the person accessing a computer or network by determining whether the user had the requisite intent or mental state, often characterized as *mens rea* or *scienter*.

In order to fall within the purview of subsection (a)(5)(A)(i) of the CFAA, a user must intend to cause damage. In addition, this subsection was amended in 2001 by the USA Patriot Act to require that a user cause a loss of more than $5,000.[77] This section will not apply to roaming Wi-Fi users, who access a network with the intent to use an Internet connection, but without the intent to cause damage to the operator of the network.

Under subsections (a)(2)(C) and (a)(5)(A)(ii) and (iii) of the CFAA, unauthorized access to a network must be intentional, but

75. Cohen, *supra* note 2.

76. U.S. v. Sablan, 92 F.3d 865, 869 (9th Cir. 1996).

77. USA Patriot Act, Pub. L. No. 107-56, § 814(d)(8), (11)(a)(i), 2001 U.S.C.C.A.N. (115 Stat. 383–84).

intent to cause damage is not required.[78] Subsection (a)(5)(A)(ii) requires that the user "recklessly" cause damage, while (5)(A)(iii) imposes strict liability, with no *mens rea* requirement with respect to the damage requirement. Subsection (a)(2)(C) does not require that the user cause damage. The language in the statute requiring a user to "intentionally" access a network replaced language that had earlier required a user to "knowingly" access a network, as a means of ensuring that the statute was triggered only by "intentional acts of unauthorized access—rather than mistaken, inadvertent or careless ones."[79]

Subsections (a)(2)(C), (a)(5)(A)(ii) and (a)(5)(A)(iii) each require intentional access without authorization (or in the case of (a)(2)(C), exceeding authorization). Implicit in the requirement that a user access a network without authorization, is a *scienter* requirement with respect to the unauthorized nature of the user's access. In other words, if a user has no way of knowing that access is unauthorized, the user cannot be deemed to have intentionally engaged in unauthorized access. In *U.S. v. Morris*, the Second Circuit provides support for this position, in holding that an "intentionally" *scienter* requirement applied to the phrase "accesses a Federal interest computer without authorization," but that this *scienter* requirement did not apply to later language in the statute.[80] The court's reference to the entire "accesses phrase," as opposed to simply the word "accesses" suggests that the court recognized a *scienter* element with respect to the "without authorization" requirement. Prior to the amendment of the CFAA in 2001, courts devoted a good deal of consideration to whether the pre-amendment "intentionally" language applied to the damage element of the statute. However, courts have not given the same consideration to the CFAA's implicit *scienter* requirement with respect to the unauthorized nature of a user's access. This is likely because the question of whether a user has authorization to access traditional networks and websites can generally be answered by a user. By contrast, the ambiguity and inconsistency in existing law and the variety of public perceptions regarding roaming Wi-Fi use creates uncertainty among users as to whether access to an open network should be considered unauthorized.

---

78. *See generally Sablan*, 92 F.3d at 868; U.S. v. Morris, 928 F.2d 504, 509 (2nd Cir. 1991); Am. Online, Inc. v. Nat'l Health Care Discount, Inc., 174 F. Supp. 2d 890 (N.D. Iowa 2001); *In re* Am. Online, Inc., 168 F. Supp. 2d 1359 (S.D. Fla. 2001).

79. S. REP. NO. 99-432, at 5 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2483.

80. *Morris*, 928 F.2d at 507(2d Cir. 1991); *see also Sablan*, 92 F.3d at 868.

Application of this implicit *scienter* requirement could determine whether a user intentionally accessed a network without authorization. The next section of this article, which considers the "without authorization" requirement in more detail, will show that the implicit *scienter* requirement favors a test to determine authorization that requires an express indication that access is not authorized. As will be discussed below, this *scienter* requirement is made explicit in some state statutes and in some common law decisions.

c. Access Without Authorization Under the CFAA

Courts have applied several different tests to determine whether access is "without authorization" for purposes of the requirement of subsections (a)(2)(C), and (a)(5)(A)(ii) and (iii) of the CFAA. This section of the article will examine several relevant reported decisions that form the basis for this article's observation that at least four approaches have been suggested by courts or legislators in determining whether access is unauthorized.

The Second Circuit, in *Morris*, a case relating to the first computer virus, found access to be "without authorization" when Morris transmitted a virus that exploited bugs in features on third-party computers and networks. The court held that Morris' access was unauthorized because he used certain software features of the third-party computers in a way that was not "in any way related to their intended function."[81]

This test could be applied in several different ways to Wi-Fi use. An individual may purchase an access point with the intent to use the access point to surf the Internet and print documents over the user's network without wired connections. Another individual, however, might buy an access point with the idea that the user will both use the access point for his or her personal use, and will use it to provide access to his or her community, as part of a community network. The first network operator could reasonably argue that the intended purpose of the device he or she purchased was to enable flexibility and mobility on the user's network. The second operator's personal use of the access point and connection sharing are also within the intended purpose of the device. When applied to Wi-Fi, therefore, a test that looks at the intended purpose of an access point must rely on the subjective intent of the network operator.

81. *Morris*, 928 F.2d at 510.

The First Circuit, in *EF Cultural Travel BV v. Zefer Corp.*, considered whether software that collects information from websites did so "without authorization."[82] The First Circuit held that a website operator would need to show an express or implied prohibition on authorization in order to support an action under the CFAA. As an example of an implied prohibition on authorization, the court referred to password protection, which "limits authorization by implication (and technology), even without express terms."[83] The First Circuit rejected a test applied by the District Court that held conduct to be without authorization only if it is not "'in line with the reasonable expectations'" of the website owner and its users," but stated that a reasonable expectations test might be useful "in other contexts where there may be a common understanding underpinning the notion."[84]

d. Four Tests for Finding Intentional Unauthorized Access

The legislative history of the CFAA, *Morris*, and *EF Cultural Travel* illustrate four tests that may be used to determine whether a user has intentionally accessed a network without authorization: (i) a test that presumes access by any "outsider," as contemplated by the legislative history of the CFAA, to be unauthorized, absent express authorization; (ii) a subjective test that looks at the intent of the network operator to determine whether access is unauthorized; (iii) a more objective test that looks at the reasonable expectations of the network operator to determine whether access was unauthorized, or at the reasonable expectations of a user to determine intent; and (iv) an objective test that looks at the network operator's actions to determine whether the operator expressed or implied prohibition on access, which prohibition would conclusively show that access was unauthorized. For purposes of this article, we will refer to the four tests identified in this paragraph as, respectively, the "express authorization test," the "subjective expectations test," the "reasonable expectations test," and the "express prohibition test."

The express authorization test reflects Congress' statements in enacting the CFAA, to the effect that portions of the CFAA that apply to "unauthorized" access apply to "outsiders," while portions of the CFAA that apply to "exceeding authorized access" (such as Section

82. 318 F.3d 58 (1st Cir. 2003).

83. *Id.* at 62–63.

84. EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 582 n.10 (1st Cir. 2001); *EF Cultural Travel BV*, 318 F.3d at 63.

1030(a)(2)(C)) apply to "insiders." Anyone who is not an "insider"—meaning anyone who does not have a prior relationship with the network operator—would be presumed "unauthorized" under this test. At least one court has used the outsider/insider distinction as a factor in determining whether access was unauthorized, while others have refused to strictly follow the insider/outsider delineation because this delineation does not appear in the statute itself.[85] Colorado's Computer Crime statute, discussed below, presents another example of an application of the express authorization test.

The subjective expectations test is derived from the *Morris* court's determination that access was unauthorized if the computer accessed was used in a way that is not in any way related to its "intended function." Ultimately, the "intended function" of a Wi-Fi access point depends on the network operator's subjective intent in adding the access point to the network. A court applying the subjective expectations test could find that a roaming Wi-Fi user's access was unauthorized because the operator of a network did not intend to grant Internet access through its network to a roaming user. As discussed above, the prohibition of Section 1030(A)(v)(ii) and (iii) contains an implicit *scienter* requirement with respect to the unauthorized nature of the user's access. Depending on how this requirement was applied, a user could potentially become subject to prosecution even if the user did not actually know (but, according to a court, constructively knew or should have known) that access was unauthorized.

The reasonable expectations test is a shorthand way of referring to two separate but closely-related concepts. The first concept, applied by the District Court and rejected by the appellate court in *EF Cultural Travel*, examines the reasonable expectations of a network operator in determining whether access is unauthorized. This test is presumably like the subjective expectations test, but would not consider an operator's subjective expectations dispositive as to whether access was unauthorized if such expectations were unreasonable.[86] The second concept, implicit in the CFAA and

85. *See In re* Am. Online, Inc., 168 F. Supp. 2d 1359, 1370 (S.D. Fla. 2001) (determining that "§§ 1030(a)(5)(B) and (C) are intended to apply to outsiders who access a computer"). *But see* Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1127 (W.D. Wash. 2000) (refusing to use the insider/outsider distinction in determining whether CFAA should apply).

86. *EF Cultural Travel BV*, 318 F.3d at 62–63. The Fourth Amendment applies a test similar to the "reasonable expectations" test, in protecting communications in which a speaker has a "reasonable expectation of privacy". The Supreme Court has stated that this test has two

explicit under many state statutes and common law decisions, examines the reasonable expectations of a user in determining whether the user intends to engage in unauthorized access.

The reasonable expectations test was rejected by the *EF Cultural Travel* appellate court as "highly imprecise, [and] litigation-spawning," in the absence of a "common understanding underpinning the notion" of what is reasonable in a given context.[87] The reason for the First Circuit's rejection of the reasonable expectations test applies equally when trying to determine whether an operator's expectations as to restricting access are reasonable and when trying to determine whether a user's expectations as to the permissibility of access are reasonable. The controversy surrounding roaming use of Wi-Fi demonstrates that there is no common understanding among users of open networks, prospective users of open networks, operators who intentionally share access, and operators who inadvertently leave their networks open.

The express prohibition test, applied by the *EF Cultural Travel* court, as well as by courts considering whether access to websites is unauthorized for purposes of trespass to chattels claims, implicitly recognizes the open nature of Internet websites, and prohibits access only if a network operator has indicated that access is prohibited, in website terms of use, by enabling password protection or otherwise.[88] The express prohibition test would provide a clear delineation of authorized versus unauthorized access by roaming Wi-Fi users. A network operator can clearly indicate that his network is not to be accessed by implementing WEP, WPA, 802.11i, or other common Wi-Fi security measures.

---

components. The speaker must establish 1) that he held "an actual (subjective) expectation of privacy," and 2) that this expectation of privacy is "one that society is prepared to recognize as 'reasonable.'" *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

87. *EF Cultural Travel BV*, 318 F.3d at 63 (*discussing* the Fourth Amendment's reasonable expectations test, addressed in Parts II.C and III.A.2.(b) of this article, as an example of a context where such a common understanding might be found).

88. *See also* Southwest Airlines Co. v. Farechase, Inc. 318 F. Supp. 2d 435, 439 (N.D. Tex. 2004) (holding that access was unauthorized under CFAA because Southwest posted terms of use and expressly communicated to Farechase that use of "scrapers" was unauthorized.); I.M.S. Inquiry Mgmt. Sys., Ltd. v. Berkshire Information Sys., Inc., 307 F. Supp. 2d 521, 523 (S.D.N.Y. 2004) (alleging that defendant obtained a username and password issued to a third-party). *But see* Physicians Interactive v. Lathian Sys., Inc., 69 U.S.P.Q.2d (BNA) 1981, 1987 (E.D. Va. 2003) (calling an argument that a website without posted terms of use was open for any purpose "an extravagant assertion" that "appears to circumvent the spirit of the CFAA, and any other type of statute designed to protect website owners against computer hackers").

e. Obtaining Information

Section 1030(a)(2)(C) requires that a user obtain information. One commentator, a former leader of the Justice Department's computer crime unit, has suggested that a roaming Wi-Fi user could face prosecution under Section 1030(a)(2)(C) because a roaming user accesses data packets containing routing and IP addressing information, which could be considered "information" for purposes of the statute.[89] While the language of the statute could support this argument, this reading would be at odds with the intent of the statute.

The legislative history of Section 1030(a)(2) indicates that "the premise of this subsection is privacy protection."[90] Analyzing the impact of a roaming Wi-Fi user's behavior on the privacy of the network operator requires an examination of whether the nature of the information accessed has an impact on the operator's desire for privacy, and on whether roaming Wi-Fi use compromises this privacy.

The right to privacy has been summarized by the Supreme Court as a person's "right to be let alone by other people," a right which is separate and distinct from the right to protection of property.[91] Privacy protection is primarily concerned with protecting information which, if discovered by a third-party, could be used to contact, embarrass, or harass the person to whom the information relates. It is not concerned with preventing someone else's temporary use of the owner's property.

The routing and IP addressing information used by a roaming Wi-Fi user is technical information that is useful for the specific purpose of allowing the transmission and receipt of other information. When a roaming Wi-Fi user's computer connects to an open network, the computer requests the temporary assignment of an address that is internal to the accessed network. The computer also requests information about where to send information to have it routed through the Internet (a "gateway" address), and information obtained from a domain name server that is used to translate human-friendly Internet addresses into the numerical IP addresses understood by the Internet's infrastructure ("DNS" information). Unlike an external IP address,

89. Mark D. Rasch, *WiFi High Crimes*, SecurityFocus, *at* http://www.securityfocus.com/columnists/237 (May 3, 2004).

90. S. REP. NO. 99-432, at 6 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2484; *see* Doe v. Dartmouth-Hitchcock Med. Ctr., No. CIV. 00-100-M., 2001 WL 873063, *4 (D.N.H. July 19, 2001).

91. *Katz*, 389 U.S. at 350.

which can be used to identify a computer or user on the Internet, the internal IP address is session-specific information, useful primarily for purposes of routing requested information to the correct computer while the computer is connected to the network. Gateway information, DNS information, and other information transmitted to a computer in connection with roaming use likewise provide information that facilitates the routing of information, but is not designed to allow connections to a network from the Internet. This information could, however, be useful to a hacker because it would provide some information about the internal configuration of the operator's network.

The information obtained by a roaming Wi-Fi user's computer is used only for purposes of routing information. This information is invisible to the user unless the user specifically runs a program or command to view the information for purposes of confirming or troubleshooting a connection. In most cases, a roaming user could argue that he or she did not actually "obtain" any information, because the user did not personally view any of the information used by the user's computer. In no event does a roaming Wi-Fi user use information to contact, embarrass, or harass a network operator. Because the purpose of Section 1030(a)(2)(C) is to protect privacy, not to protect property, it is clear that mere use of an open connection is not the type of action that Section 1030(a)(2)(C) is designed to prevent.

f. Damage and Loss

The Section 1030(a)(5) provisions discussed in this article require both that the unauthorized access cause "damage" and that the conduct causes "loss" aggregating at least $5,000 in value. Likewise, in order to maintain a civil claim under Section 1030(a)(2), a plaintiff must also show a loss exceeding this threshold.[92] It is possible that a user who transmitted large amounts of data through an open Wi-Fi network could cause damage as defined by the statute. It is also theoretically possible that a network operator who had unintentionally left a network open could incur losses exceeding $5,000 in assessing whether access had caused the network operator harm, but allowing a network operator to recover for the expense of securing its network in this situation would reward the operator's negligence.

92. Register.com, Inc. v. Verio, Inc., 356 F.3d 393, 439–40 (2d Cir. 2004).

The term "damage" means any impairment to the integrity or availability of data, a program, a system, or information. It is conceivable, though unlikely, that a roaming Wi-Fi user could cause "damage" by causing an impairment to the availability of a system, in the event that the user's actions significantly reduce the amount of bandwidth available to the network operator. As described in Part II.B. above, any such "damage" would likely be negligible.

> [T]he term "loss" means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service . . . .[93]

The cost of bandwidth used by a roaming Wi-Fi user would practically never exceed $5,000. It is possible for a network operator to argue that the costs of securing a network constitute a "loss" triggered by a roaming user's access to a network. If a network operator incurred security-related costs after discovering that a roaming Wi-Fi user had accessed the operator's network, these costs might properly be classified as costs of responding to an offense and conducting a damage assessment.

The cost of implementing security measures were included in the calculation of "loss" in the prosecution of Stefan Puffer, in what might have been the first Wi-Fi related prosecution under the CFAA. In that case, Puffer, a former technology consultant to the Harris County, Texas District Clerk's office was prosecuted for allegedly using an open Wi-Fi connection to demonstrate the security risks presented by the configuration of the computer systems maintained by the District Clerk's office. Based on Puffer's demonstration to the District Clerk and to a reporter for the Houston Chronicle, the District Clerk's office hired security professionals to address these risks. Puffer was then charged with causing the transmission of codes or commands in violation of Section 1030(a)(5)(A)(i), of causing loss aggregating at least $5,000 under Section 1030(b)(i), and of causing damage to a computer system used by a government entity in furtherance of the administration of justice under Section 1030(b)(v) (a section not discussed in detail above because it relates to specific circumstances that will not typically be applicable to roaming Wi-Fi use).[94] The prosecution's theory was that the need for consulting

93. 18 U.S.C.A. § 1030(e)(11) (West Supp. 2004).

94. Grand Jury Indictment, United States v. Puffer, (CR H-02-388) (S.D. Tex. 2002).

services prompted by Puffer's demonstration could be included in the amount constituting the District Clerk's loss for purposes of the $5,000 threshold. Puffer was acquitted because the jury found he did not intentionally cause damage, as required by Section 1030(a)(5)(A)(i).[95]

U.S. v. Middleton and *In re Doubleclick Inc. Privacy Litigation*,[96] two cases decided prior to an amendment to the CFAA that defined "loss," suggest that the costs of repairing damage and resecuring systems can be considered losses under the CFAA, but that costs of improving a system other than to prevent further damage may not be included. Incurring $5,000 of loss in preventing roaming users from accessing a Wi-Fi network seems excessive (except on large or complicated networks), and more likely to represent the cost of improvement than repair. A Wi-Fi network may be secured against access by enabling features included on any access point. At least one case has refused to find a "loss" when a simple security option was available. In *Doubleclick*, the Southern District of New York held that the "loss" requirement of the CFAA was not met when the plaintiff did not show any damage to its computer systems or data that could require economic remedies, and when the accessed computer systems could easily and at no cost be secured against the type of intrusion of which the plaintiff complained.[97] While it would certainly be possible for a network operator to spend $5,000 in consulting fees to enable security measures on its network, Wi-Fi networks can typically be secured to prevent roaming users from accessing the network using features included in standard equipment.

Additionally, an interpretation of the CFAA that would allow a network operator to sue a roaming Wi-Fi user for the cost of securing the operator's network seems unfair. Given widespread public warnings from a variety of sources urging Wi-Fi network operators to secure their networks, as well as warnings published in the instruction manuals and elsewhere for most access points, a network operator who wishes to prevent access but does not enable security should be considered negligent. It is unreasonable to hold a roaming user responsible for a network operator's negligence, and to thereby reward such negligence.

---

95. *See* John Leyden, *Ethical wireless hacker is innocent*, The Register, *at* http://www.theregister.co.uk/2003/02/24/ethical_wireless_hacker_is_innocent/ (Feb. 24, 2003).

96. United States v. Middleton, 231 F.3d 1207, 1213 (9th Cir. 2000); *In re* DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497, 524–25 (S.D.N.Y. 2001).

97. *In re DoubleClick*, 154 F. Supp. 2d at 524–25.

g. The CFAA Is Unlikely to Apply to Roaming Wi-Fi Use

The generally-applicable provisions of the CFAA discussed in this article require that a user intentionally access a network without authorization, and that the user either obtain information or cause damage and a loss aggregating $5,000. Although it is possible that the CFAA could be applied to roaming Wi-Fi use, application of the "obtaining information" provisions of the statute would be inconsistent with the intent of the statute, and application of the "damage and loss" portions would reward a network operator's failure to implement security measures reflecting its expectations regarding access to its network.

A roaming Wi-Fi user engages in intentional access, but likely does not intend to engage in unauthorized access. An open network typically provides no indication to a user that access is unauthorized. It is reasonable for a user to assume that access to an open network is not prohibited.

Whether access to an open network is considered unauthorized under the CFAA is unclear, as courts have applied a variety of tests. Under the express authorization test, roaming Wi-Fi use would be unauthorized unless specifically authorized by a network operator. The subjective expectations test would rely on a network operator's intent in determining whether access is unauthorized. The reasonable expectations test applicable to authorization should recognize that an open network cannot reasonably support an expectation of security or a finding that access was unauthorized under the CFAA. The express prohibition test would deem access unauthorized only if a network operator has indicated that access is prohibited, through implementation of security measures or otherwise.

The language of Section 1030(A)(2) is broad enough to suggest that, by accessing routing and addressing information, a roaming Wi-Fi user "obtains information" for purposes of the statute. However, the legislative history of this section makes clear that the statute is intended to protect privacy. Accessing routing and addressing information as part of roaming use of the Internet through an open Wi-Fi connection does not provide a threat to a network operator's privacy. In fact, because a user never actually has to view the information necessary to use an Internet connection, a roaming user could argue that he or she did not actually obtain information.

Bandwidth-intensive roaming use of a network could theoretically cause "damage" under the CFAA by reducing the

amount of bandwidth available to the network operator. Although it is possible that roaming Wi-Fi use could prompt a network operator to incur consulting costs to enable security, and such costs could reach $5,000, this result would essentially allow a negligent operator to improve its network at a roaming user's expense. This would be an unjust result, and should be rejected by any court considering this situation.

It is unlikely that a roaming user will have the requisite intent to implicate the CFAA. Although a user could be considered to obtain information under the CFAA, this reading would be inconsistent with the intent of the statute. Finally, the damage and loss requirements under Section 1030(a)(5) would only be met under extreme circumstances. For these reasons, it is unlikely, though possible, that the CFAA will apply to roaming Wi-Fi use.

2. The Electronic Communications Privacy Act

The Electronic Communications Privacy Act ("ECPA"),[98] part of the Federal Wiretap Act, is intended to protect against the unauthorized interception of electronic communications, and to protect stored electronic communications and transactional records from unauthorized access.[99] While the ECPA could potentially apply to whackers and other Wi-Fi users, it is clear that the ECPA does not apply to roaming Wi-Fi users who access the Internet through open Wi-Fi connections. In the context of electronic radio communications, the ECPA applies only to the intentional interception of encrypted content.

Title I of the ECPA amended the Federal Wiretap Act to prohibit the intentional interception of the contents of any electronic communication (specifically including any radio communication). As amended, the Federal Wiretap Act is a difficult statute that one appeals court has called "famous (if not infamous) for its lack of clarity."[100] Title II of the ECPA prohibits unauthorized access to stored electronic communications or transactional records. Title III of the ECPA provides certain requirements for the installation and use of pen registers and trap and trace devices (discussed below).

Three key elements of the ECPA are relevant in showing that the ECPA does not apply to roaming Wi-Fi users—intent, encryption,

98. 18 U.S.C. §§ 2701–11 (2000).

99. S. REP. NO. 99-541, at 1, 3 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3557.

100. Steve Jackson Games, Inc. v. United States Secret Service, 36 F.3d 457, 462 (5th Cir. 1994).

and content. A user must intentionally intercept encrypted content of a communication in order to violate the ECPA. These three elements will be discussed below.

a. Intent of User

The ECPA protects communications only from intentional access or interception. The legislative history of the ECPA shows that the intentional (as opposed to "willful") state of mind requirement was implemented specifically to address the concern of radio operators who use radio scanners to receive public communications, who could inadvertently tune through a private communication in the course of scanning through frequencies.[101] The "intentional" requirement was specifically implemented by the ECPA to clarify that inadvertent interceptions are not covered by the ECPA.[102] While an accidental user may "willfully" take actions, such as enabling a "zero configuration" option on a laptop, that result in a network connection, an accidental user does not intend to access the network. Courts have further clarified the intent requirement to require that the user act purposefully, and that the interception be the product of the user's conscious objective, rather than a product of mistake or accident.[103] The intent requirement elucidates that a user does not violate the ECPA by accidentally connecting to a network, but case law suggests that the intent requirement may be met if a user continues a connection after realizing that an inadvertent connection has been made.[104] An accidental user may therefore become a joyrider if he checks his e-mail after realizing that he has accidentally connected to the wrong network.

b. Encryption

The ECPA protects communications on a Wi-Fi network only when the network operator has enabled or implemented a method of encrypting data transmissions. As discussed in more detail below, this encryption requirement is a result of the application of the ECPA to the actions of law enforcement officials. For purposes of this article, we focus on roaming Wi-Fi users that use only open, or unencrypted networks.

---

101. S. REP. NO. 99-541, at 6 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3560.

102. *Id.*

103. United States v. Townsend, 987 F.2d 927, 930–31 (2d Cir. 1993).

104. Tapley v. Collins, 41 F. Supp. 2d 1366, 1372 (S.D. Ga. 1999), *rev'd in part, appeal dismissed in part*, 211 F.3d 1210 (11th Cir. 2000).

The ECPA, as part of the Federal Wiretap Act, is intended to define the circumstances under which a law enforcement agent must obtain a search warrant before intercepting or accessing a communication. This Act provides statutory protection in accordance with the Fourth Amendment's prohibition on unreasonable searches and seizures. Courts have interpreted the Fourth Amendment to protect communications where a reasonable expectation of privacy exists.[105] Underlying the ECPA, therefore, is a form of the reasonable expectations test that looks at the reasonable expectations of a network operator with respect to the privacy and protection of its information.

Congress has attempted to provide some "bright line" tests for when an expectation of privacy is not reasonable within the context of the ECPA. The ECPA therefore expressly does not apply to communications made through an electronic communication system that is configured to be "readily accessible to the general public."[106] Under the ECPA, an electronic communication made through a radio system is "readily accessible to the general public" if it falls into one of a number of categories, including communications that are not "scrambled or encrypted" and are not "transmitted using modulation techniques whose essential parameters have been withheld from the public with the intention of preserving the privacy of such communication."[107] This exception to the ECPA removes all Wi-Fi networks that do not use encryption from the ECPA's protection. In light of the ECPA's clarification that use of an unencrypted radio network does not support a reasonable expectation of privacy, it is more appropriate to classify the ECPA as a statute that applies the express prohibition test than the reasonable expectations test.

c. Content

The ECPA prohibits interception and access of the "contents" of a communication,[108] which is defined as "any information concerning the substance, purport or meaning of that communication."[109] A whacker may intercept "content," but joyriders, war-drivers, and

105. Katz v. United States, 389 U.S. 347 (1967); S. REP. NO. 99-541, at 4 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3558.

106. 18 U.S.C. § 2511(g)(i) (2000).

107. *Id.* § 2510(16).

108. *Id.* § 2510(4).

109. *Id.* § 2510(8).

accidental users interact only with administrative components of a network.

The ECPA has a counterpart statute, Chapter 206 of Title 18,[110] that governs "pen registers" and "track and trace devices," which are designed to intercept addressing and transactional information relating to messages, rather than content. This statute is designed to allow law enforcement to intercept this "transactional" information with a court order, rather than requiring a full warrant. The relevant definitions of "pen register" and "track and trace devices" are as follows:

> (3) the term ''pen register'' means a 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 . . .
>
> (4) the term ''trap and trace device'' means a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication . . . .[111]

While a roaming Wi-Fi user's computer may receive and use certain addressing information in order to establish and maintain a connection with a network, it is clear that the intent of the pen register and trap and trace statutes is to regulate how addressing information can be used in connection with obtaining information about specific communications. Roaming Wi-Fi users will not collect specific information about other communications taking place on the network.

d. The ECPA Does Not Apply to Roaming Wi-Fi Use

The ECPA prohibits the intentional interception of the contents of electronic communications. The ECPA contains an express exception to its prohibitions for radio communications that are not encrypted. This exception makes the ECPA inapplicable to roaming Wi-Fi use, although it may still apply to whacking. In addition, roaming Wi-Fi use does not involve the interception of the contents of communications for purposes of the statute. For these reasons, the ECPA does not apply to roaming Wi-Fi use.

110. 18 U.S.C.S. § 2511(2)(h)(i) (LexisNexis 2004).

111. 18 U.S.C.S. § 3127(3), (4).

3. Section 633 of the Communications Act

Section 633 of the Communications Act of 1934, titled "Unauthorized reception of cable services," provides penalties for any person who willfully receives "any communications service offered over a cable system, unless specifically authorized to do so by a cable operator or as may otherwise be specifically authorized by law."[112] Although this section appears as though it could be relevant to roaming use of a Wi-Fi signal for which Internet connectivity is provided by cable modem, the section has been interpreted to apply only to the reception of services at the point at which such services are actually being distributed over the cable system. Section 633, therefore, does not apply to roaming Wi-Fi use.

Although cable modem providers have asserted that connecting an open Wi-Fi access point to a cable modem may constitute a violation of Section 633 of the Communications Act,[113] this statute likely does not apply to Wi-Fi users who connect to these access points. The legislative history of Section 633 states that

> The [Energy & Commerce] Committee intends the phrase "service offered over a cable system" to limit the applicability of this section to theft of a service from the point at which it is actually being distributed over a cable system. Thus, situations arising with respect to the reception of services which are transmitted over-the-air (or through another technology), but which are also distributed over a cable system, continue to be subject to resolution under section 605 to the extent reception or interception occurs prior to or not in connection with, distribution of the service over a cable system.[114]

"Communications Service" is not defined in the Communications Act, but the legislative history for this section indicates that the term is intended to mean "any communications service," including, for example, audio, video, textual, data, or other service offered over a cable system, including any material transmitted to or from a subscriber over a cable system that has interactive capability. This definition would likely be interpreted to include cable modem service, because cable modem service is a data service offered over a cable system.

---

112. 47 U.S.C.A. § 553 (West 2001).

113. *See* Letter from Gregory Powell, Abuse & Security, Supervisor, High Speed Online Services, Time Warner Cable of NYC (June 25, 2002), *available at* http://www.serebin.com/ben/wireless/TWC_Wireless_Response.jpg.

114. H.R. REP. NO. 98-934, at 83 (1984), *reprinted in* 1984 U.S.C.C.A.N. 4655, 4720.

The Federal Communications Commission ("FCC") and several courts have found that cable modem service is not "cable service" for purposes of the Communications Act.[115] The FCC further stated that cable modem service is not governed by Title VI of the Communications Act, which includes Section 633.[116] However, portions of the FCC's ruling that strictly classified cable modem service as an "information service" rather than a "telecommunications service" were later overruled by the courts, and in making the foregoing statement, the FCC was not specifically considering Section 633. In light of these facts, it is reasonable to assume that cable modem service may still be considered a "communications service offered over a cable system."

Courts have cited the legislative history provision excerpted above for the proposition that Section 633 governs reception of communications while being transmitted over cable, but that Section 605 of the Communications Act (which provides for more severe penalties) applies to reception of communications while being transmitted by radio. The legislative history, as well as the cases citing it, contemplates the transmission of communications initially by radio, and subsequently by cable. However, the legislative history also reflects that Section 633 is not intended to apply to reception occurring "not in connection with distribution . . . over a cable system." Reception of a signal from a Wi-Fi connection is not reception in connection with distribution over a cable system, even if such connection's Internet connectivity is provided through a cable modem system.

Section 633 of the Communications Act prohibits the willful reception of communications services offered over a cable system. Cases make clear that Section 633 applies only to information while it is being transmitted over a cable system. This section, therefore, does not apply to roaming Wi-Fi use.

4. Section 605 of the Communications Act

The cases discussed above pointed out that Section 605 of the Communications Act prohibits unauthorized publication or use of

115. Brand X Internet Svcs. v. FCC, 345 F.3d 1120, 1132 (9th Cir. 2003); In the Matter of Inquiry Concerning High-Speed Access to the Internet Over Cable and Other Facilities, 17 F.C.C.R. 4798, 4833 (2002).

116. In the Matter of Inquiry Concerning High-Speed Access to the Internet Over Cable and Other Facilities, 17 F.C.C.R. 4798, 4838 (2002).

radio communications,[117] but Section 605 probably does not apply to roaming Wi-Fi users. Although the language of the statute is very broad, courts interpreting the statute have imposed a requirement that communications that implicate this statute must be the subject of a reasonable expectation of privacy as defined under the ECPA.

Section 605 contains two prohibitions potentially applicable to roaming Wi-Fi users: (i) it prohibits any person who receives a radio communication that is not intended for the use of the general public from publishing the existence of the radio communication; and (ii) it prohibits a recipient of a radio communication to which such recipient is not "entitled" from using such communication for his or her own benefit, or for the benefit of a third-party.

The prohibitions of Section 605 apply "except as authorized by [the ECPA]."[118] Federal Appeals Courts have interpreted this exception to mean that communications that would be subject to both the ECPA and Section 605 are subject to the same Fourth Amendment restrictions under each statute.[119] As discussed above, the ECPA's application to radio communications is limited by the Fourth Amendment to communications that are encrypted or are otherwise "not readily accessible to the general public." At least one Federal District Court has also found that Section 605 is subject to the same limitation.[120] Consequently, Section 605 is unlikely to apply to roaming Wi-Fi use of open networks.

At first glance, it could appear that a war-driver's publication of a map of access points, including both encrypted and open access points, could constitute publication of the existence of a radio communication within the meaning of Section 605. Because war-driving maps contain information about encrypted communications, one could argue that they should be considered outside the ECPA's "readily accessible to the general public" exception. However, the information collected by a war-driver is typically transmitted in clear text, even on encrypted networks. Consequently, Section 605 should not apply to war-driving.

---

117. 47 U.S.C.A. § 605 (West 2001).

118. *Id.*

119. United States v. Hill, 459 U.S. 828 (1982); Edwards v. State Farm Ins. Co., 833 F.2d 535, 537–40 (5th Cir. 1987); United States v. Basey, 816 F.2d 980, 992–93 (5th Cir. 1987); United States v. Rose, 669 F.2d 23, 25–27 (1st Cir. 1982), *cert. denied sub nom.*

120. United States v. Gass, 936 F. Supp. 810, 811–12 (N.D. Okla. 1996). *But see* Cal. Satellite Sys. v. Seimon, 767 F.2d 1364, 1366 (9th Cir. 1985) (decided before the enactment in 1986 of the ECPA).

B. State Laws

1. Statutes Prohibiting Access to or Use of Networks

Most states have statutes that prohibit intentional, unauthorized access to, or use of, computer networks. These statutes are often similar to the CFAA, but have certain critical differences. For example, some of these statutes do not require that a user actually cause damage. Whether these statutes apply to roaming Wi-Fi use depends in many cases on whether the user intentionally engaged in unauthorized access. Unlike the CFAA, some state statutes provide express requirements as to the unauthorized element of this inquiry, as well as the intent element. Some states support the express authorization test or the express prohibition test for determining authorization. Other state statutes focus on the user's *mens rea* with respect to authorization, using either the reasonable expectations test or other standards to determine whether the user had the requisite intent.

a. Statutes Supporting Express Authorization Test

Colorado's Computer Crime statute prohibits the knowing and unauthorized use of any computer network.[121] This statute defines "authorization" as express consent.[122] On its face, this statute would prohibit roaming Wi-Fi use. No reported cases in Colorado indicate an interpretation to the contrary.

As discussed in Part III.B.5 below, the California Attorney General's office has taken an aggressive enforcement position with respect to its unauthorized access and theft statutes. California Penal Code Section 502[123] prohibits users from "knowingly" and "without permission" accessing or using a network. The Attorney General's office has indicated that such access would be considered "without permission" absent express permission.[124]

b. Statutes Supporting Express Prohibition Test

State statutes supporting the express prohibition test should not apply to roaming Wi-Fi use. These statutes require that a network operator take affirmative actions to prohibit access. Roaming Wi-Fi

121. COLO. REV. STAT. § 18-5.5-102(1)(a) (2003).

122. *Id.* § 18-5.5-101(1).

123. CAL. PENAL CODE § 502 (West 2004).

124. Telephone Interview with Robert Morgester, Cal. Deputy Att'y Gen., (June 22, 2004).

use that involves simply accessing the Internet through an open network will therefore not violate these statutes.

New York requires as an element of its Unauthorized Use of a Computer statute that the computer or computer service accessed be "equipped or programmed with any device or coding system, a function of which is to prevent the unauthorized use of said computer or computer system."[125] Under this statute, roaming access to Wi-Fi networks would be prohibited only if a network operator has enabled encryption or other security. New York also has a theft of services provision that likely does not apply to roaming Wi-Fi use, as discussed in Part II.B.2 below.

Likewise, the Unauthorized Computer Access provisions of Nebraska's Computer Crimes Act require that a user penetrate a computer security system,[126] defined as

> a computer program or device that:
>
> (a) Is intended to protect the confidentiality and secrecy of data and information stored in or accessible through the computer system; and
>
> (b) Displays a conspicuous warning to a user that the user is entering a secure system or requires a person seeking access to knowingly respond by use of an authorized code to the program or device in order to gain access . . . .[127]

While this provision would not prohibit use of an open Wi-Fi network, Nebraska's Computer Crimes Act contains two other provisions that may apply to roaming Wi-Fi users. The first is a provision prohibiting intentional access with knowledge that such access was not authorized[128] (discussed in Part II.B.1(c) below), and the second is a theft of services provision[129] (discussed in Part II.B.2 below).

Illinois,[130] Michigan,[131] and Massachusetts[132] have statutes that presume that use is unauthorized if the network operator has put security measures in place. These statutes do not have an equivalent

125. N.Y. PENAL LAW § 156.05 (McKinney 1999).
126. NEB. REV. STAT. § 28-1343.01 (1995).
127. *Id.* § 28-1343(5).
128. *Id.* § 28-1347.
129. *Id.* § 28-1344.
130. *See* 38 ILL. COMP. STAT. ANN. 16D-7 (West Supp. 1992).
131. *See* MICH. COMP. LAWS ANN. § 752.797 Sec. 7(6)(c) (West Supp. 2004).
132. *See* MASS. GEN. LAWS ANN. ch. 266, § 120F (West 2000).

presumption that use is authorized if the network operator does not use security measures. However, these statutes imply that silence does not indicate a lack of authorization. If silence rendered access unauthorized, the express presumption that adoption of security measures renders access unauthorized would be unnecessary. These states' statutes, therefore, support application of the express prohibition test to roaming Wi-Fi users.

Many state statutes, as well as the CFAA, prohibit intentional unauthorized access, but do not clarify what level of *mens rea* applies to the unauthorized nature of the user's access. A number of states, including Connecticut, Delaware, Maine, and Nebraska, expressly require that a user know that access to a Wi-Fi network is unauthorized in order for computer access or use statutes to apply.[133] Given the ease with which an open network may be accessed, and public support for roaming Wi-Fi use, a user will typically only know that access to the Internet through a Wi-Fi network is unauthorized if security measures have been enabled on the network. A literal reading of these statutes would therefore lead to a result similar to that achieved by the express prohibition test: a user would be deemed to engage in intentional unauthorized access only if a network operator had taken affirmative steps to indicate that access was unauthorized.

c. Statutes Supporting Reasonable Expectations Test

As demonstrated in the preceding paragraph, some statutes apply an express *mens rea* requirement to the unauthorized nature of a user's access. Statutes requiring actual knowledge that access is unauthorized effectively employ the express prohibition test. Other states look to the reasonable belief of the user, rather than knowledge, in determining whether computer access or use is unlawful. These statutes provide good examples of the reasonable expectations test. The reasonable expectations test should not prohibit roaming use of Wi-Fi, as widespread custom and public perceptions support a reasonable belief that an open network may be accessed. However, courts considering application of these statutes could reach contrary conclusions. It is, therefore, unclear as to whether statutes applying the reasonable expectations test will prohibit roaming use of Wi-Fi.

Alabama's Computer Crime Act expressly does not apply when a defendant has reasonable grounds to believe that he has

133. CONN. GEN. STAT. ANN. § 53a-251(b)(1) (West 1994); DEL. CODE ANN. tit. 11 § 932 (2001); ME. REV. STAT. ANN. tit. 17-A, § 357(1) (West 1964 & Supp. 2003); NEB. REV. STAT. § 28-1344 (1995).

authorization to access a network.[134] Arkansas,[135] Nevada,[136] and Ohio[137] add to this defense, that a defendant must either reasonably believe he or she had authority, or reasonably believe that the network operator would have authorized the use of the network. Similarly, the unlawful access or use statutes in Alaska[138] and Missouri[139] prohibit access when a user does not have any reasonable ground to believe that such user has the right to access a network. In each of these cases, a user could presumably defend against prosecution by arguing that the custom and common practice of network operators making their networks available to the public free of charge could support a reasonable belief that a roaming Wi-Fi user's access to a network is or would be authorized.

It is an affirmative defense to New Hampshire's Computer Related Offenses statute[140] and to West Virginia's Computer Crime and Abuse Act[141] to show that a user reasonably may not have known that his or her access was unauthorized. A Wi-Fi user could typically argue that he or she could not determine from the information available with respect to a given open Wi-Fi network, whether access is intended to be authorized or not. However, this standard seems to require a higher level of inquiry than a knowledge-based standard. A sophisticated user could make an educated guess in some circumstances as to whether a network was likely left open by design or by mistake.

New Hampshire's legislature was the first to consider directly addressing the topic of roaming Wi-Fi use. House Bill 495,[142] which was ultimately not passed by the legislature, provided,

The owner of a wireless computer network shall be responsible for securing such computer network. It shall be an affirmative defense to a prosecution for unauthorized access to a wireless computer network if the unauthorized access meets the following requirements: (1) The person reasonably believed that the owner of the computer or computer network, or a person empowered to license access thereto, had authorized him or her to access; or (2) The person reasonably

134. *See* ALA. CODE § 13A-8-102 (2003).
135. ARK. CODE ANN. § 5-41-203(d) (Michie Supp. 2003).
136. NEV. REV. STAT. ANN. § 205.477 (Michie 2001 & Supp. 2003).
137. OHIO REV. CODE ANN. § 2913.03(C) (Anderson 2003).
138. ALASKA STAT. § 11.46.740(a) (Michie 2002).
139. MO. ANN. STAT. § 569.099 (West 1999 & Supp. 2004).
140. N.H. REV. STAT. ANN. § 638:17(I)(c) (1996 & Supp. 2003).
141. W. VA. CODE ANN. § 61-3C-17(a)(1) (Michie 2000).
142. N.H. H.B. 495 (LexisNexis 2003).

believed that the owner of the computer or computer network, or a person empowered to license access thereto, would have authorized the person to access without payment of any consideration; or (3) The person could not have reasonably known that his or her access was unauthorized.[143]

The New Hampshire bill was introduced by Representative Richard "Stretch" Kennedy, in response to the threatened prosecution of one of Rep. Kennedy's constituents.[144] Brian Williams, a technology professional, was threatened by a municipal official with prosecution under New Hampshire's "Computer Related Offenses; Network Security" statute after inadvertently discovering that a local governmental office operated an open network, and alerting the office to the security risks presented by the office's network configuration. House Bill 495 was intended to place the burden of securing a wireless network on the network owner, and to make clear that negligent or otherwise inadvertent access to a wireless network would not violate the statute. The bill was passed by the New Hampshire House of Representatives, but was abandoned without significant discussion in the Senate.

In threatening prosecution against Mr. Williams, the municipal official alleged that Mr. Williams reasonably should have known that access was unauthorized, given his extensive experience in the information technology industry and his familiarity with the municipality and its technical competence. After an exchange of correspondence with Mr. Williams' attorney, the municipality ultimately determined not to pursue prosecution of Mr. Williams.

d. No Guidance

More than thirty states have laws that apply when a network is accessed without authorization or without consent, but do not provide any additional guidance as to how authorization or consent is to be interpreted. These statutes create uncertainty among roaming Wi-Fi users that threatens to deter use of open networks, regardless of whether the network operator intends to afford access to roaming users.

143. *Id.*

144. Telephone Interview with Brian Williams (Mar. 12, 2004).

2. Theft of Services Statutes

Theft of computer services statutes in some states could potentially apply to roaming Wi-Fi use. Like other statutes that prohibit access to computers and networks, many of these statutes require intentional unauthorized access. Theft of services statutes present a few issues in addition to those described in the preceding section. A number of theft of services statutes require that the services accessed be services that are typically available only for compensation. Some theft statutes also require that services be obtained by threat, deception, or fraud.

While unauthorized access statutes typically are intended to protect networks operated by individuals and businesses, state theft of services statutes are additionally intended to protect services provided by cable operators and Internet service providers. Some state theft of services statutes apply to services that are known to be available only for compensation,[145] are available only for compensation,[146] or are offered on a subscription or other basis for monetary consideration.[147]

Many individuals and businesses make Wi-Fi access to the Internet available free of charge. Many other entities provide pay-per-use or subscription Wi-Fi access. An entity that offers Internet access for compensation, whether an individual, coffee shop or other business, or traditional Internet service provider, generally will implement a login mechanism to allow the provider to collect its compensation. A roaming Wi-Fi user of the type discussed in this article only accesses open networks without security mechanisms or encryption.

However, a traditional Internet service provider may provide subscription-based Internet service to a business or individual who then intentionally or unintentionally makes this Internet service available to roaming Wi-Fi users over an unencrypted Wi-Fi connection. A roaming Wi-Fi user may access a compensated

145. *See, e.g.*, ALASKA STAT. § 11.46.200(a)(1) (Michie 2002); ARIZ. REV. STAT. ANN. § 13-1802(A)(6) (West 2000); D.C. CODE ANN. § 22-3211(c) (2001); KY. REV. STAT. ANN. § 514.060 (Michie 1999); ME. REV. STAT. ANN. tit. 17-A, §357 (West 1964 & Supp. 2003); N.J. STAT. ANN. § 2C:20-8 (West 1995 & Supp. 2004).

146. MD. CODE ANN. CRIM. L. § 7-104(e) (applying only if the access is with knowledge that the services are provided without the consent of the person providing them); OR. REV. STAT. § 164.125 (2003) (applying only if person accessing has intent to avoid payment, and if services are obtained by force, threat, deception or other means to avoid payment for the services).

147. MASS. GEN. LAWS ANN. ch. 266, § 33A (West 2000) (requiring intent to defraud).

service, but will have no way to know whether the service provider's acceptable use policy authorizes sharing of the service.

Most of the statutes cited above require that the compensated services be obtained by deception, force, threat, or other means,[148] intent to defraud,[149] or intent to avoid payment.[150] Theft of services statutes in Arizona, the District of Columbia, and Maryland appear to apply only if the user knows that the ultimate service provider would not have allowed use of the connection.[151]

Several states, including Nebraska, have statutes that are similar to unauthorized access statutes, except that they require that the user intentionally deprives another person of services or obtains "property or services of another." Nebraska's statute defines "services" to include, but not be limited to, computer time, data processing, and storage functions. If Internet connectivity were included within "services," analysis of the application of this statute, like most unauthorized access statutes, would likely depend on whether a roaming Wi-Fi user's access was considered to be "without authorization." Nebraska provides no further guidance on this point.

A theft of services statute can usually be analyzed in the same way as other unauthorized use or access statutes. However, application of theft of services statutes may also depend on whether Wi-Fi Internet connectivity falls within the services protected by the statute. In some cases, statutes apply only to services that a user knows are provided only for compensation, and will generally not apply with respect to a roaming Wi-Fi user's access to a private network. Likewise, neither this type of statute nor most unauthorized access statutes will apply to a roaming user's access to a service provider's services because the user will not knowingly or intentionally access the services in violation of the service provider's terms of service.

3. Statutes Prohibiting Interruption or Degradation of Services

Several states have statutes prohibiting interruption or degradation of computer services. Because use of an Internet

148. ALASKA STAT. § 11.46.200(a)(1) (Michie 2002); KY. REV. STAT. ANN. § 514.060 (Michie 1999); ME. REV. STAT. ANN. tit. 17-A, § 357 (West 1964 & Supp. 2003); N.J. STAT. ANN. § 2C:20-8 (West 1995 & Supp. 2004); OR. REV. STAT. § 164.125 (2003).

149. MASS. GEN. LAWS ANN. ch. 266, § 33A (West 2000).

150. N.Y. PENAL LAW § 165.15(11) (McKinney 1999).

151. ARIZ. REV. STAT. ANN. § 13-1802(A)(6) (West 2000); D.C. CODE ANN. § 22-3211(b) (2001); MD. CODE ANN. CRIM. L. § 7-104(e)(2).

connection could degrade the speed of the connection for other users of the connection, it is possible that this type of statute could apply to a roaming Wi-Fi user. In most cases, however, these statutes contain a requirement that the disruption be intentional.[152] Connecticut's statute also prohibits recklessly (rather than intentionally) degrading service, and could potentially apply to a roaming Wi-Fi user.[153]

4. Statutes Prohibiting Interception of Communications

A few states, including Delaware, Florida, Kansas, New Jersey, Pennsylvania, Texas, and Utah, have enacted statutes prohibiting interception of communications.[154] These states are similar to the ECPA, and typically will not apply to roaming Wi-Fi because, like the ECPA, they are intended to prohibit interception of the content of messages and because they are expressly inapplicable to transmissions that are configured to be accessible to the general public. It is not clear whether courts in these states would adopt the same "bright line" rule applied by the ECPA, which permits interception of unencrypted communications.

The interception of communications statutes of Kansas and Pennsylvania suggest that communications systems that are readily accessible will be exempt from the statutes only if they are intended to be readily accessible. These statutes therefore could potentially apply a version of the subjective expectations test that looks to whether the operator intentionally or inadvertently failed to enable security on its network.

5. Statutes Prohibiting Facilitation of Access to Networks

California Penal Code Section 502(c)(6) imposes criminal penalties on anyone who "[k]nowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or computer network."[155] California Deputy Attorney General Robert Morgester posted a warning to at least one war-driving website that publishes information about the location and

152. DEL. CODE ANN. tit. 11, § 934 (2001); W. VA. CODE ANN. § 61-3C-8 (Michie 2000).

153. CONN. GEN. STAT. ANN. § 53a-251(d) (West 1994).

154. *See* DEL. CODE ANN. tit. 11 § 2402 (Supp. 2001); FLA. STAT. ANN. § 934.03 (West 1999); KAN. STAT. ANN. § 22-2514 (1995); N.J. STAT. ANN. § 2A:156A-3 (West 1995 & Supp. 2004); 18 PA. CONS. STAT. ANN. § 5703 (2000); TEX. PENAL CODE ANN. § 16.02 (Vernon 2003 & Supp. 2004); UTAH CODE ANN. § 77-23a-4 (2003).

155. CAL. PENAL CODE § 502(c)(6) (West 2004).

encryption status of Wi-Fi networks, that publication of such information violates Section 502(c)(6).[156]

At the time Mr. Morgester posted this warning, no war-driver had been prosecuted under Section 502(c)(6). However, it is clear that a war-driver who posts information about access points discovered while war-driving may be subject to prosecution in California. It is not as clear that a court would agree that the statute applies to war-driving itself.

Enforcement of Section 502 to prohibit posting of access point information could potentially invoke concerns regarding the war-drivers' First Amendment rights to free speech. Discussion of whether application of this statute runs afoul of the Constitution is beyond the scope of this article.

The draft Model Communications Security Legislation (commonly known as the "Super-DMCA"), which has been adopted in several forms in a number of states, also imposes penalties for selling devices that are designed to allow for unauthorized access to a service provider's network.[157] However, the Super-DMCA clearly applies only to services that are offered for compensation.

C. Common Law

The tort of trespass to chattels traditionally provided remedies to a livestock owner for intentional injury to the owner's sheep or cattle. This tort has recently been revived as a method of combating spam and other Internet-related issues. Recent expansion and adaptation of this tort to electronic "trespasses" make this tort potentially applicable to some types of network access through Wi-Fi, particularly whacking activities. However, it is unlikely that roaming Wi-Fi access to the Internet will meet the intent and damage requirements necessary to support an action for trespass to chattels.

The common law tort of trespass to chattels provides remedies "where an intentional interference with the possession of personal property has proximately caused injury."[158] While tangible contact was traditionally necessary to support a cause of action for trespass, courts have recently applied the tort to computer-related activities by adopting the view that the transmission of electronic signals can meet

156. *See* Posting of Robert M. Morgester, Cal. Deputy Att'y Gen., *at* http://wigle.net/phpbb/viewtopic.php?t=193 (Sept. 12, 2003) (posting of this item was confirmed in a telephone interview with Robert Morgester (June 22, 2004)).

157. *See* MODEL COMMUNICATIONS SEC. LEGISLATION (Draft April 11, 2003).

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

the tangible contact requirement.[159] Trespass to chattels has increasingly been applied to behavior on the Internet, including the use of website "robots"[160] and the transmission of unsolicited commercial e-mail (spam).[161] Using the logic of these recent cases, a network operator could argue that a roaming Wi-Fi user's use of bandwidth constituted an interference with the operator's network.

Recent decisions applying trespass to chattels to electronic communications have required that the plaintiff establish: (i) that the defendant intentionally and without authorization interfered with the plaintiff's interest in the computer system; and (ii) defendant's unauthorized use proximately resulted in damage to the plaintiff.[162] These requirements, relating to intent, authorization, and damages, mirror requirements found in many of the statutory sections discussed above. Although this section will show that a trespass to chattels action based on a roaming user's activities is unlikely to succeed, the analysis applied by courts to the various elements of a trespass to chattels claim provide a helpful context in considering the application of the CFAA and state statutes to roaming Wi-Fi use.

1. Intentional Use

A New York court has clarified that "intentional" use requires action "with the intention of interfering with the property or with knowledge that such interference is substantially certain to result."[163] Part III.C.3 below explains that a roaming Wi-Fi user's activities are unlikely to represent the type of interference required to support a trespass to chattels action unless the user consumes a great deal of bandwidth. Even with sustained high-bandwidth usage of an open network, a trespass to chattels claim will not succeed unless the user intended to interfere with the operator's use of bandwidth, or knew that his or her usage was substantially certain to cause interference.

At least one court has also considered the specific *mens rea* required with respect to the unauthorized nature of a user's access. In *CompuServe, Inc. v. Cyber Promotions, Inc.*, an Internet service provider brought a trespass to chattels claim in order to stop spamming activities. The District Court for the Southern District of

159. *Id.*

160. eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058, 1070 (N.D. Cal. 2000).

161. CompuServe Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1020–21 (S.D. Ohio 1997).

162. *eBay, Inc.*, 100 F. Supp. 2d at 1069–70.

163. Sch. of Visual Arts v. Kuprewicz, 771 N.Y.S.2d 804, 808 (N.Y. Sup. Ct. 2003).

Ohio stated, "To prove that a would-be trespasser acted with the intent required to support liability in tort it is crucial that defendant be placed on notice that he is trespassing."[164] This statement makes express the implicit *scienter* requirement discussed above with respect to the CFAA. This statement also provides a good example of an application of the express prohibition test for determining when access is unauthorized.

Both the requirement that a user intentionally cause interference and the requirement that a user be notified that access is unauthorized make it unlikely that a trespass to chattels action would be successful against a roaming Wi-Fi user.

2. Unauthorized Use

Courts have framed the "unauthorized" requirement for a trespass to chattels action in a variety of ways. For instance, the Restatement (Second) of Tort, does not require that a trespasser be unauthorized, but instead provides privileges, which would defeat a trespass to chattels claim, to users who have obtained consent, or who reasonably use the facilities of a public utility.[165]

In *CompuServe*, the Southern District of Ohio considered both the consent privilege and the public utility privilege with respect to the activities of Cyber Promotions. The court dismissed the argument that an Internet Service Provider could be considered a public utility for purposes of the privilege. The court acknowledged, however, that CompuServe may have provided "a tacit invitation for anyone on the Internet" to use its computers for the purposes of forwarding e-mail, but that any consent CompuServe may have given was revoked when CompuServe expressly notified Cyber Promotions that its spamming activities were not authorized.[166]

Trespass to chattels had been an infrequently-used tort until "a few courts . . . breathed new life into the common law cause of action for trespass to chattels by finding it viable online,"[167] in *CompuServe*, *eBay, Inc. v. Bidders' Edge, Inc.*, and *Intel Corp. v. Hamidi*. In virtually all of the prominent recent Internet-related trespass to chattels cases, courts have examined website terms of use or other statements by the network or computer owner indicating to users that the type of disruptive access involved in the cases was not

164. *CompuServe Inc.*, 962 F. Supp. at 1024.

165. *See generally*, R.2d Torts §§ 217 *et seq.* (Lexis 2004).

166. *Id.* at 1023.

167. Register.com, Inc. v. Verio, Inc., 356 F.3d 393, 436 (2d Cir. 2004).

authorized.[168] These cases provide examples of application of the express prohibition test.

3. Damages

Traditionally, trespass to chattels claims have required a showing that interference with an interest in property must have caused actual damage to the property or deprived the owner of its use for a substantial period.[169] In *eBay v. Bidder's Edge*, Bidder's Edge used Internet "spiders," which consumed a portion of eBay's bandwidth and server capacity by sending 80,000 to 100,000 requests to eBay's computers systems per day. eBay had unsuccessfully tried many different business and technical methods of preventing Bidder's Edge from accessing its website. In granting equitable relief to eBay, the Northern District of California, held that "even if, as [Bidder's Edge] argues, its searches use only a small amount of eBay's computer system capacity, [Bidder's Edge] has nonetheless deprived eBay of the ability to use that portion of its personal property for its own purposes."[170] The court further held that failing to provide a legal remedy to prevent Bidder's Edge from using spiders could encourage others to engage in the same types of activities.[171] Some interpreted this decision as eliminating the requirement that actual damage or deprivation of use for a substantial period of time be shown.[172]

However, the California Supreme Court, in the 2003 case *Intel*, interpreted the eBay decision to have retained the requirement that damage or substantial deprivation of use be shown, but to have provided that this requirement may be met in circumstances where many entities may engage in the same behavior and, in the aggregate, cause the functionality of the owner's system to be impaired. The California Supreme Court held that temporary use of a portion of computer processors was not sufficient to support a claim for trespass. The court went on to state that "an actionable deprivation of use must be for a time so substantial that it is possible to estimate the loss caused thereby. A mere momentary or theoretical deprivation of use is not sufficient unless there is a dispossession . . . ."[173] The *Intel*

168. *Id.* at 402; EF Cultural Travel BV v. Zefer Corp., 318 F.3d 58, 63 (1st Cir. 2003); *eBay, Inc.*, 100 F. Supp. 2d at 1070; *CompuServe Inc.*, 962 F. Supp. at 1024.

169. *See* Zapata v. Ford Motor Credit Co., 615 S.W.2d 198, 201 (1981).

170. *eBay, Inc.*, 100 F. Supp. 2d at 1071.

171. *Id.*

172. *Id.* at 1058.

173. Intel Corp. v. Hamidi, 71 P.3d 296, 306 (2003) (*citing* RESTATEMENT (SECOND) OF TORTS § 219 cmt i (1965)).

court cited the Restatement (Second) of Torts for the proposition that a property owner is protected against lesser forms of interference by the owner's legal privilege to use reasonable force to protect the property.

Roaming Wi-Fi use will not typically deprive a network operator of bandwidth for a substantial or even noticeable period of time, unless the user were to engage in substantial downloading of media files, uploading of spam, or other high-bandwidth activities. Nor is there a substantial risk that permitting one roaming Wi-Fi user to use an open connection could encourage others to do the same. A network operator displeased by the use of his or her open network by a roaming user could simply enable encryption or some other form of security on the network, blocking future access by all roaming users. Other courts, considering spamming activities, have recognized that, in trespass to chattels actions, "the implementation of technological means of self-help, to the extent that reasonable measures are effective, is particularly appropriate in this type of situation and should be exhausted before legal action is proper."[174]

D. Common Law Trespass is Unlikely to Apply to Roaming Wi-Fi Use

To support a trespass to chattels claim, a network operator would have to show that a roaming user intentionally and without authorization interfered with the operator's interest in its network, and that this unauthorized use proximately resulted in damage to the operator.

The intent component of this cause of action requires that a roaming user knew or was reckless as to whether his or her access would cause a disruption of the operator's service. Unless a roaming user consumes a great deal of bandwidth, he or she is unlikely to expect that his or her usage could cause a disruption or other damage.

The intent component has also been interpreted to require that a user be notified that access is prohibited. Practically speaking, only by enabling security measures will a network operator provide notice to a user that access is prohibited. On an open network, a user will not have notice that access is prohibited.

Most courts considering whether access to a website is unauthorized for purposes of a trespass to chattels claim have applied the express prohibition test, by relying on the terms of use posted by a

174. *CompuServe Inc.*, 962 F. Supp. at 1023.

network operator to determine whether access is authorized. It is not clear that a court would use this test with respect to a roaming Wi-Fi user, because a Wi-Fi network may in some cases have more of a private character than a website.

Although courts have found that a network operator can suffer damage for purposes of a trespass to chattels claim, even without proof of a quantifiable diminution in bandwidth, other courts have reiterated that a substantial interference with an operator's interest in its network is necessary to support a claim. Roaming use of Wi-Fi is unlikely to cause this type of damage. This type of damage could also easily be prevented by self-help measures.

A network operator is unlikely to be able to support a trespass to chattels claim because the operator will typically not be able to show that a user possessed the requisite intent, or that a user caused the requisite damages.

IV. PERMITTING ROAMING USE OF WI-FI UNDER EXISTING LAW

The value of roaming Wi-Fi use is threatened by ambiguity and inconsistency in existing law. Much of this ambiguity and inconsistency results from application of the concept of intentional, unauthorized access to opportunistic methods of network access such as Wi-Fi. Roaming use of Wi-Fi to access the Internet does not clearly fit into the legal models used to analyze traditional network access and access to websites. This section analyzes four tests that can be used to determine whether access is intentional, unauthorized access, and concludes that the most efficient test is one that requires a network operator to take action reflecting a prohibition on roaming access in order for such access to be considered "unauthorized." This section further recommends statutory models and case law precedent that can be used in implementing the express prohibition test.

A. Summary of Tests for Finding Intentional Unauthorized Access

The express authorization test, implicitly suggested by Congress in enacting the CFAA and embodied in Colorado's Computer Crime statute, treats all access to open Wi-Fi networks as unauthorized unless a network operator expressly indicates that access is authorized. This approach discourages usage of intentionally shared networks, as many of these networks do not have readily visible means of indicating that access is authorized, other than that the network is left open. Typically, there are only a few ways in which a

user may be affirmatively notified that a network operator intends to provide access. A network operator may provide signage in a facility, or may list his or her network in a publicly accessible directory. An operator may also provide an electronic login or sign-up screen to expressly indicate that access is shared, but a user must actually connect to an open network and launch his or her web browsing software in order to see this screen. This test should be rejected by courts and legislatures as outdated and a barrier to progress.

The subjective expectations test, implicitly suggested by the Second Circuit in *Morris* (and possibly applied in some state interception of communications statutes), would prohibit access to a network if the network's operator intended for the network to be private. A user would be forced to guess at a network operator's intentions, and could be criminally liable if he or she guessed wrong. This approach provides no guidance to a user as to whether access is unauthorized, and would likely discourage roaming use of Wi-Fi because it creates uncertainty. This test should likewise be rejected.

The reasonable expectations test, applied by the District Court in *EF Cultural Travel*, and echoing the Fourth Amendment's "reasonable expectation of privacy" standard, would prohibit access if the network operator subjectively intended for its network to be private, provided that the operator's expectations as to access are reasonable. While this approach does not provide certainty to a user, a user could make a strong argument that an operator cannot reasonably expect that an open network will be treated as private.

The court in *EF Cultural Travel* rejected the reasonable expectations test as "a highly imprecise, litigation-spawning standard."[175] However, the court in *EF Cultural Travel* allowed that the test could be proper in certain contexts, citing a case applying the Fourth Amendment standard. Under the ECPA, and by extension, Section 605 of the Communications Act, the Fourth Amendment's "reasonable expectation of privacy" standard has been clarified and codified. Unencrypted radio communications are not protected under the ECPA, because a network operator is statutorily deemed to not have a reasonable expectation of privacy in these communications. The ECPA's version of the reasonable expectations test is essentially equivalent to the express prohibition test, and provides clarity and facilitates the roaming use of Wi-Fi.

175. EF Cultural Travel BV v. Zefer Corp., 318 F.3d 58, 63 (1st Cir. 2003).

Many state laws implement a different version of the reasonable expectations test that looks to the expectation of a user as to whether access is authorized. This test makes express the *scienter* requirement implied, but not clarified, under the CFAA. An analysis of these state statutes reveals the type of weaknesses and ambiguity that caused the *EF Cultural Travel* court to reject the reasonable expectations test. The ease of accessing an open Wi-Fi network and media statements in favor of allowing roaming Wi-Fi use would support a reasonable expectation that accessing open networks is permissible. However, media statements and public perceptions could easily support an opposite conclusion as well—hence the controversy addressed by this article. To borrow language used by the *EF Cultural Travel* court, there is currently no "common understanding underpinning" the expectations of operators and roaming users, partially because the law is unsettled. While the reasonable expectations test (as applied to a roaming user's *mens rea*) should ideally be rejected for these reasons, this test has already been codified in a number of states, and is unlikely to change quickly. The responsibility for determining whether a user's expectations as to accessing open networks are reasonable will be borne by courts.

The express prohibition test, applied by the First Circuit in *EF Cultural Travel*, the Southern District of Ohio in *CompuServe*, and by New York's Unauthorized Use of a Computer statute, would deem access unauthorized, and a user's access to such network intentional, only if the network operator enabled security or otherwise indicated that its network was not to be accessed by roaming users. Under this approach, access to an open Wi-Fi network for purposes of using an Internet connection would not be considered intentional unauthorized use.

B. Advantages of Express Prohibition Test

The express prohibition test contains a number of clear advantages over the other tests discussed in this article. This test provides clarity to users and promotes roaming Wi-Fi use, encourages responsible security practices, and provides a bright line for enforcement of restrictions on access to Wi-Fi networks.

Unlike the subjective expectations test and the reasonable expectations test, the express prohibition test would allow a Wi-Fi user to determine quickly whether access to a network was unauthorized. Adoption of this test would dispel the chilling effect currently created by ambiguity as to what constitutes legally

unauthorized usage of a Wi-Fi network. A reduction of this chilling effect would promote the use of roaming Wi-Fi, and could support an important step in the expansion of the Internet and the growth of new networking technologies.

The express prohibition test also provides clarity in the law that would encourage the adoption of appropriate security measures by network operators. Clarifying that a network is not protected from access unless access is expressly discouraged would prompt network operators to be responsible in their approach to security. Once an indication that access is prohibited has been shown, the law would protect the operator's network from undesired access.

Finally, the express prohibition test would provide advantages in enforcing laws prohibiting unauthorized access. A user who accessed a secured network or secured portions of the network would be presumed to have intentionally accessed the network or secured portion without authorization. Use of the software tools necessary to defeat WEP or other security means would also assist law enforcement officials and prosecutors in proving a violation of the statute.

C. Implementing the Express Prohibition Test

Legislators and courts can improve existing law by consistently implementing the express prohibition test. Legislators should consider amending existing statutes applicable to Wi-Fi access to apply only if security measures have been implemented. Courts interpreting unauthorized access statutes that do not provide guidance on how to interpret intentional unauthorized access should consider precedent implementing the express prohibition test. With respect to statutes that require the application of the reasonable expectations test, courts should consider the context in which roaming Wi-Fi use occurs in determining whether a user's access should be considered unauthorized.

The New York unauthorized access to computers statute provides a model statute for legislators. This statute does not apply unless security measures have been taken. Requiring security measures as a condition to application of the statute is straightforward and provides a bright-line test for what access is prohibited.

This article has identified several other statutory approaches to the express prohibition test. Some states provide an affirmative defense to a charge of unauthorized access if a user did not know that access was unauthorized. As stated above, a user will typically know

that access was unauthorized only if security has been enabled. However, this implementation of the express prohibition test could be watered down to a test resembling the reasonable expectations test, if a court were to find a user had constructive knowledge that access was unauthorized.

Statutes have also implemented the express prohibition test as a presumption that access is not authorized if security measures have been implemented. Logically, the reverse presumption, that access is not unauthorized if security measures have not been implemented, should be true as well. However, because this presumption is not explicit in these statutes, the statutes remain a bit ambiguous.

Because it is not realistic to expect widespread amendment of statutes to implement the express prohibition test, judicial approaches to implementing this test are also important. *EF Cultural Travel* provides precedent for a finding that access to a network should not be considered unauthorized absent an indication to that effect by the network operator. *CompuServe* could be viewed as precedent for finding that a user did not have the intent required to support a finding of intentional, unauthorized access unless the user had been expressly or implicitly notified that his or her access was not authorized. While *CompuServe* interpreted the common law tort of trespass to chattels, *Theofel v. Farey-Jones*[176] indicates that courts may look to common law trespass cases in interpreting the CFAA and other federal statutes.

Some state statutes have implemented the reasonable expectations test that looks to a user's reasonable expectations in determining whether a user intentionally accessed a network without authorization. Courts should consider the context in which roaming Wi-Fi takes place in determining whether a user reasonably knew or should have known that access was unauthorized. Open networks are easy to access, and are, in fact, commonly shared with the public. General public perception and the media's treatment of roaming Wi-Fi could support a reasonable belief that access to an open network is permissible. Conversely, public warnings about the accessibility of open networks would not support a network operator's reasonable belief that an open network is secure. Finally, a court should consider the value of roaming Wi-Fi to society and to its users, in light of the low cost of this practice to network operators, in determining whether an open network user's expectations as to permissibility of access are reasonable.

176. 341 F.3d 978 (9th Cir. 2003).

V. CONCLUSION

Roaming use of Wi-Fi provides a valuable direction for growth and development of the Internet. Expansion of the area from which the Internet may be accessed by increasing the footprint of nationwide Wi-Fi network accessibility has the potential to contribute greatly to the expansion of current and future networking technologies. Negative aspects of roaming Wi-Fi use, including aspects associated with the use of networks that are unintentionally shared, are minimal and easily mitigated. Because of this value and the minimal associated risk, the law should encourage the roaming use of Wi-Fi.

Current federal and state laws may apply to the use of Wi-Fi networks for whacking activities, and to roaming use of open Wi-Fi networks for purposes of accessing the Internet, and, at least in California, to war-driving. Many statutes are unclear as to whether roaming Wi-Fi use is illegal. In a number of states, and potentially under the Federal Computer Fraud and Abuse Act, application of computer access statutes depends on whether a user intentionally accesses a Wi-Fi network without authorization. Statutory and case law defining intentional access without authorization is inconsistent and ambiguous. A lack of clarity and consistency among existing laws threatens to have a chilling effect on this important direction of future growth for the Internet.

Legislators and courts should consider that the sharing of Internet connections using Wi-Fi is a common and widespread practice. It is often difficult or impossible for a user to determine whether a connection has been shared intentionally or inadvertently. In contrast, it is typically easy for a network operator to enable basic security measures on a Wi-Fi network. The substantial benefits to society of roaming Wi-Fi use are higher than the minimal costs associated with access to an inadvertently open network.

Roaming use of Wi-Fi would be facilitated if legislators and courts were to implement an express prohibitions test, which would prohibit access to a Wi-Fi network for purposes of accessing the Internet only if a network operator has enabled security on his or her network. New York provides a model statute using this approach. Courts may also look to precedent under the CFAA and cases interpreting the common law of trespass to chattels in implementing this approach. Courts may be restricted from implementing this approach by existing statutes that prescribe the use of a test that looks to a user's reasonable expectations regarding whether access is authorized. In these cases, courts should consider that the context in

which roaming Wi-Fi use occurs would support a user's reasonable belief that access to an open network is not considered unauthorized.

The rapid rise and evolution of networking technologies continues to have a profound impact on the assumptions underlying many aspects of law. Like the Internet, whacking, joyriding, and war-driving challenge legislators and courts to find solutions that protect a property owner's rights while encouraging the free flow of information. By prohibiting use of a Wi-Fi network only when the network operator has implemented security measures, courts and legislators will encourage the development and use of this valuable technology. Simultaneously, this approach will promote sensible security practices, and protect network operators who have indicated their access preferences. To summarize—in terms that may have made the title of this article appear almost nonsensical—the law must condemn whacking, while recognizing the value in joyriding and war-driving.