

Policing the Wireless World: Access Liability in the Open Wi-Fi Era

MATTHEW BIERLEIN*

Burgeoning technological development presents new and ever-evolving challenges for how the law confronts an Internet savvy society. The proliferation of wireless networking exemplifies the tension between promoting technological growth and ensuring legal protection. Wi-Fi enables greater freedom of access, fostering the use of the Internet in an increasing number of everyday tasks. However, open wireless networks can be susceptible to unwanted access by those seeking to hack into a computer on the network or to use the network for an unlawful purpose. Though the law adequately addresses such malevolent access, it remains unclear how the law treats ordinary users who happen across a wireless network to surf the web.

This Note proposes presumptive legal access to open wireless networks as a means to balance technological growth and security. Federal and state laws address access conduct, but the language and degree of enforcement of these statutes differ. This may confuse users and discourage access. Making access to an open wireless network presumptively legal, while at the same time providing protection for secured networks, encourages network providers to take responsibility for enabling security mechanisms, mitigates user confusion, and promotes access. Such a result may represent an appropriate equilibrium of promoting wireless growth and building wireless security.

I. INTRODUCTION

On the night of April 20, 2005, Richard Dinon noticed something strange while taking out his trash.¹ The muted glow of a laptop emanating from an SUV parked outside of his home caught the St. Petersburg, Florida resident's eye.² He walked up to the car and saw a man abruptly close his laptop upon

* J.D., The Ohio State University Moritz College of Law, 2006. B.A., The College of Wooster, 2001. The author is an associate with the law firm of Luper, Neidenthal & Logan. The views expressed herein are those of the author and are not intended to reflect the views of the firm or its clients. I would like to thank Peter Swire and Sol Bermann for the inspiration to pursue this topic and for their guidance and feedback along the way. As always, I owe countless thanks to my parents, Paul and Marlene, for their support throughout law school and life.

¹ Rob Kelley, *Man Charged with Wireless Trespassing*, MONEY, July 7, 2005, http://money.cnn.com/2005/07/07/technology/personaltech/wireless_arrest/index.htm.

² Alex Leary, *Wi-Fi Cloaks a New Breed of Intruder*, ST. PETERSBURG TIMES, July 4, 2005, at 1A.

noticing Richard's presence.³ Richard returned to his house, and at first dismissed the stranger as perhaps someone performing census work.⁴ But when Richard turned on his home computer, he noticed strange icons on his desktop.⁵ These strange icons aroused Richard's suspicion that the man outside may be accessing his computer.⁶ Later that night, when Richard returned from taking his girlfriend home, the SUV remained parked outside his home.⁷ At this point, Richard decided to call the police.⁸

The St. Petersburg police arrested the SUV's driver, Benjamin Smith III, and charged him with violating a state computer crime statute.⁹ Florida law prohibits accessing a computer network without authorization and classifies such conduct as a third degree felony.¹⁰ Although prosecutors are unsure what sentence they will seek, if Benjamin is convicted, he faces a potential five year prison sentence.¹¹

The law's treatment of the relatively new phenomenon of wireless networking reflects important economic and policy decisions regarding the growth and use of the Internet. The Internet has become entrenched in the everyday lives of many Americans.¹² Wireless networking expands the reach and function of the Internet by breaking through physical boundaries; users no longer must physically connect to a network, but may gain access via radio frequencies.¹³ Unfortunately, it remains unclear how exactly the law

³ Kelley, *supra* note 1.

⁴ Leary, *supra* note 2.

⁵ Kelley, *supra* note 1.

⁶ *Id.*

⁷ Leary, *supra* note 2.

⁸ *Id.*

⁹ Kelley, *supra* note 1; *see also* Dave Gussow, *Wireless 'Mooching' Raises Issues of Security, Ethics*, ST. PETERSBURG TIMES, Aug. 1, 2005, at 1D; Henry J. Gomez, *Can't See It, But Stealing's Easy for Wi-Fi Poachers*, CLEV. PLAIN DEALER, July 27, 2005, at C1.

¹⁰ FLA. STAT. ANN. § 815.06 (West 2006).

¹¹ Kelley, *supra* note 1.

¹² *See* Richard Drezen, Editor's Note, *A Dot-Com World; In Just 5 Years, the Internet has Gone from the Strange to the Standard*, WASH. POST, May 17, 2000, at G1 (noting the "Internet's profound impact on everyday life, from how we work and play to what we wear and even what we dream about"); Mark Baechtel, *The Internet: What a Mesh!*, WASH. POST, Aug. 27, 1996, at B6 ("For a huge and ever-growing number of people, the Internet has become . . . so necessary a part of everyday life that it's easy to take for granted."); Tom Zeller Jr., *The Internet's Future? It Depends on Whom You Ask*, N.Y. TIMES, Jan. 10, 2005, at C4. *See generally* THE INTERNET IN EVERYDAY LIFE (Caroline Haythornthwaite & Barry Wellman eds., 2002); JAMES E. KATZ & RONALD E. RICE, SOCIAL CONSEQUENCES OF INTERNET USE: ACCESS, INVOLVEMENT, AND INTERACTION (2002).

¹³ *See infra* Part II for a description of wireless networking technology.

treats wireless access. This confusion reflects the difficulties of defining how the law applies to new technologies and the potential complications caused by making this determination.

The Benjamin Smith case raises significant questions about the legality of wireless access, the appropriate relationship between the law and emerging technology, and, in a much broader sense, the practical implications of regulating technology in an Internet society. While the average person will not likely feel much sympathy for Benjamin Smith's predicament—that he parked his SUV outside a stranger's home feels a bit unsavory¹⁴—his case has far-reaching implications for casual wireless users.¹⁵ If Benjamin Smith is subject to prosecution, what happens to those average Americans who unknowingly log in to their neighbor's network or happen across a wireless signal at a park, hotel, or other public space?

The legality of access presents the most pressing question to Benjamin Smith. His case turns on whether the law classifies access of an open wireless network as criminal conduct.¹⁶ Such access may fall under the auspices of federal and state statutory law (as well as common law doctrines in the case of civil liability).¹⁷

Federal and state laws in the area of unauthorized access present a confusing regime of statutes with varying scope. At the federal level, the Computer Fraud and Abuse Act¹⁸ may be construed to encompass unauthorized access conduct. State laws vary significantly; some states appear to absolve users from liability for open wireless access, while other states set a low threshold of conduct for liability to attach.¹⁹ But the majority of state statutes remain unclear as to users' culpability for accessing an open

¹⁴ Gussow, *supra* note 9 (Smith “doesn't appear to be the best poster child for Wi-Fi freedom.”).

¹⁵ See Michel Marriott, *Hey Neighbor, Stop Piggybacking My Wi-Fi*, N.Y. TIMES, Mar. 5, 2006, § 1, at 1. (“Piggybacking, the usually unauthorized tapping into someone else's wireless Internet connection, is no longer the exclusive domain of pilfering computer geeks or shady hackers cruising for unguarded networks. Ordinarily upstanding people are tapping in. As they do, new sets of Internet behaviors are creeping into America's popular culture.”). Interestingly, in identifying open wireless access as a pertinent social issue, Marriott presupposes that using an open wireless network is unauthorized; see also Steve Hargreaves, *Stealing Your Neighbor's Net*, MONEY, Aug. 10, 2005, http://money.cnn.com/2005/08/08/technology/personaltech/internet_piracy/index.htm.

¹⁶ In Benjamin's case, the court's only concern lies with the application of Florida law, as prosecutors charged him with violation of state unauthorized access law; no charges were brought under federal law. See Kelley, *supra* note 1.

¹⁷ See *infra* Part VI (discussing the application of the law to open Wi-Fi access).

¹⁸ Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1030 (2000 & Supp. II 2002).

¹⁹ See *infra* Part VI.B.

wireless network.²⁰ The common law further complicates matters—some courts have shown a willingness to extend doctrines that have traditionally applied solely to tangible property, to encompass a variety of conduct on the Internet.²¹

The inconsistent legal response to open wireless access leads to user confusion and may negatively impact technological development. Typically, hardware providers ship wireless access points with a default setting disabling security.²² Hardware companies have little incentive to alter default settings, or further, expend significant resources developing an appropriate security regime amidst a climate of contradictory laws.²³ New technologies such as WiMax,²⁴ which will allow wireless access over a significantly greater range, could further exacerbate this confused security environment.

If courts construe the law to render open wireless access illegal, it may stunt a significant means of access to the Internet, thereby diminishing the Internet's overall value. The value of Internet content and the efficiency of the Internet's functioning directly relate to the number of its users.²⁵ If users could be criminally or civilly liable for open wireless access, it could create a disincentive for logging on to the network and contributing in the Internet arena—even the mere specter of illegality may negatively impact the value of the Internet.

Open wireless access constitutes one aspect of a growing debate over the control of the Internet. Increased use of the Internet has revealed a range of stakeholders in Internet content and infrastructure, beyond internet service providers and users. For example, several municipalities seek to provide free or low cost wireless access via city-wide wireless networks.²⁶ Additionally, telecommunications companies are beginning to balk at the idea that customers use their fiber optic cable and broadband pipe, the foundation for communication over the Internet, without concern for compensation for the

²⁰ See *infra* Part VI.B.

²¹ See *infra* Part VI.C.

²² James Coates, *Wi-Fi Hackers Find Routes Easily; Path Tough to Block*, CHI. TRIB., July 10, 2005, § 5, at 2; Alan S. Key, *WiFi's Widening World*, WASH. POST, Dec. 22, 2002, at H7.

²³ See Jonathan Krim, *WiFi is Open, Free and Vulnerable to Hackers*, WASH. POST, July 27, 2003, at A1. Krim notes a T-Mobile spokesman who states that the company does not use encryption, but instead encourages individuals to use firewall software or other forms of protection. *Id.*

²⁴ See Henry Fountain, *Pre-N's and MIMO's: The Lingo of Wireless*, N.Y. TIMES, May 4, 2005, at G3.

²⁵ GEORGE GILDER, *TELECOSM: HOW INFINITE BANDWIDTH WILL REVOLUTIONIZE OUR WORLD* 73 (2000) (citing Metcalfe's law, which holds that "[t]he value of a network rises in proportion to the power of all the machines attached to it").

²⁶ See *infra* note 37.

heavy amount of data transmitted.²⁷ Answering the question of the legality of open wireless access requires consideration of a key question germane to the broader debate of Internet control: should “owners” of wireless networks be afforded property rights in these networks or should wireless networks remain in the commons, with open access to the public at large?

This Note argues in favor of presumptively legal access for open wireless networks. Keeping wireless networks open fosters technological development and furthers Internet growth by giving users absolute clarity about the legality of their access. In turn, these technological gains and Internet growth provide substantial value to society. The current regime of federal and state statutory provisions, as well as common law doctrines, is muddled at best. This unintelligible mix of pertinent law may hinder the development of wireless technology and stunt the accompanying social benefits this technology may bring.

Before addressing the issue of open wireless access, one must consider what the term means. Part II examines the wireless world in which we live. Wireless networking represents an emerging technology that already fundamentally alters how the Internet permeates people’s daily lives. This Part provides the basics of wireless networking: the technological underpinnings of wireless, the types and functions of wireless networks, security issues, and the various types of wireless network users. This foundation becomes important in understanding the law and policy surrounding wireless networking.

The next three Parts address the law surrounding unauthorized access to wireless networking. Part III examines the Computer Fraud and Abuse Act and Part IV considers the state statutory law pertinent to the issue of open wireless access. The federal government and all fifty states have enacted laws that in some way address unauthorized access.²⁸ However, these laws differ in important ways that create confusion regarding the culpability of users for open wireless access. Part V focuses on the common law doctrine of trespass to chattels and how it relates to open wireless access. Although rooted in tort law, courts have shown a willingness to construe trespass to chattels to include electronic trespass.

²⁷ Arshad Mohammed, *Verizon Executive Calls for End to Google’s ‘Free Lunch,’* WASH. POST, Feb. 7, 2006, at D1 (quoting Verizon senior vice president and deputy general counsel John Thorne as stating “[t]he network builders are spending a fortune constructing and maintaining the networks that Google intends to ride on with nothing but cheap servers. It is enjoying a free lunch that should, by any rational account, be the lunch of the facilities providers.”). Such rhetoric is part of the growing debate on network neutrality, which focuses on whether telecommunications companies may charge different prices to different users for access to the companies’ networks. Jeffrey H. Birnbaum, *No Neutral Ground in this Internet Battle*, WASH. POST, June 26, 2006, at D1.

²⁸ See *infra* Parts III, IV.

Part VI addresses how federal and state statutory law and the common law may apply to open wireless access. On the statutory side, user culpability depends on the interpretation of the terms “access” and “authorization,” as well as damage determinations. The viability of the tort of trespass to chattels depends largely on a court’s willingness to extend the doctrine to electronic conduct. After considering how these laws could apply, the next Part turns to the more important question—how should the law apply to open wireless access?

Part VII provides a thoughtful consideration of the policy and economic issues surrounding open wireless access. From a theoretical perspective, wireless networking technology falls somewhere on a continuum of conduct. At one end of the continuum lies activity such as listening to the radio; at the other end lie physical property conceptions such as looking in a homeowner’s window. The challenge arises in determining where wireless networking fits on this continuum. Finally, Part VII sets forth and analyzes a model unauthorized access statute that provides for the presumptive legal access of open wireless networks.

II. THE WIRELESS WORLD

Wi-Fi (short for wireless fidelity)²⁹ represents a relatively new and rapidly growing technology. Wi-Fi refers to wireless local area networks,³⁰ or WLANs, which connect users to the Internet by means of radio or infrared frequencies.³¹ These networks require the network operator to install a short-range radio tower, referred to as a wireless access point (“WAP”),³² which sends and receives data to and from user devices that are equipped with hardware capable of receiving the signal from the access point.³³

²⁹ See Fountain, *supra* note 24. Originally, Wi-Fi did not stand for wireless fidelity. The Wi-Fi Alliance, in conjunction with the Interbrand Corporation, coined the term to describe WLAN products based on IEEE 802.11 standards. Wi-Fi is a trademark of the Wi-Fi Alliance, which is a trade organization that certifies equipment for compliance with wireless standards. Wikipedia.org, WiFi, <http://en.wikipedia.org/wiki/Wi-fi> (last visited Sept. 8, 2006).

³⁰ For the purposes of this Note, Wi-Fi, wireless network, WLAN, and hotspots, *see infra* note 36, will be used interchangeably.

³¹ *Wi-Fi: Unplugging Devices*, CNET NEWS.COM, Nov. 3, 2003, http://news.com.com/Wi-Fi:+Unplugging+devices/2100-7351_3-5072011.html; *see also* KAVEH PAHLAVAN & PRASHANT KRISHNAMURTHY, PRINCIPLES OF WIRELESS NETWORKS 18–19 (2002).

³² Patrick S. Ryan, *War, Peace, or Stalemate: Wargames, Wardialing, Wardriving, and the Emerging Market for Hacker Ethics*, 9 VA. J.L. & TECH. 7, 20 (2004), <http://www.vjolt.net/archives/php?issue=19> [hereinafter *War, Peace or Stalemate*].

³³ *Id.*

Wi-Fi networks typically operate on common standards set by the Institute of Electrical and Electronics Engineers (“IEEE”). These standards, 802.11b, 802.11a, and 802.11g, all use free unlicensed radio frequencies, allowing users to connect to Wi-Fi networks for free.³⁴

Wi-Fi networks may be implemented by a variety of operators and in a variety of contexts. Private residences and businesses deploy wireless networks for use in the home or office. Other businesses directly provide wireless networks in public areas such as airports, coffee shops, hotels, and convention centers.³⁵ Collectively, these networks create “hotspots” in suburban areas and business districts, which provide wireless access to the public.³⁶ Beyond hotspots, several municipalities currently offer or have begun to explore plans to provide public Wi-Fi access.³⁷

³⁴ These standards dictate the rate of data transfer, with 802.11b allowing a maximum transfer rate of eleven megabits per second (“mbps”) rate, and 802.11a and 802.11g allowing transfer at a fifty-four mbps rate (although the effective transfer rate stands at approximately half of these maximums). *Id.* New standards are in development, notably WiMax, an IEEE 802.16e standard for wireless broadband. *See* Fountain, *supra* note 24; *see also* Michael Singer, *Intel Pushes WiMax Around the Globe*, CNET NEWS.COM, Nov. 10, 2005, http://news.com.com/Intel+pushes+WiMax+around+the+globe/2100-7351_3-5944874.html.

³⁵ Robert V. Hale II, *Wi-Fi Liability: Potential Legal Risks in Accessing and Operating Wireless Internet*, 21 SANTA CLARA COMPUTER & HIGH TECH. L.J. 543, 543–44 (2005).

³⁶ *Id.* Wi-Fi networks accessible to the public are commonly known as “hotspots”; several websites provide listings of the hotspots available in a given locale. *See* WiFinder, <http://www.wifinder.com> (last visited Sept. 8, 2006); JiWire, <http://www.jiwire.com> (last visited Sept. 8, 2006); WiFiMaps, <http://www.wifimaps.com> (last visited Sept. 8, 2006); Wi-FiHotSpotList.com, www.wi-fihotspotlist.com (last visited Sept. 8, 2006).

³⁷ Esme Vos, *Second Anniversary Report*, MuniWireless.com, July 2005 at 5–7, <http://muniwireless.com/reports/docs/July2005report.pdf>. The report identifies several regions and municipalities that already make use of publicly accessible Wi-Fi networks, as well as others planning projects. Municipal Wi-Fi is a complex issue, encompassing technology, economics, privacy, and a variety of other interests. Municipalities must determine whether Wi-Fi will be provided free of charge or at a cost. For example, the Wireless Philadelphia project plans to offer residents service for twenty dollars a month (with low income residents paying ten dollars a month). Richard Siklos, *What We Have Here is a Failure to Communicate*, N.Y. TIMES, Oct. 30, 2005, § 3, at 3. San Francisco is considering proposals from twenty-six companies, including Google and MetroFi; both have offered to construct a WiFi network for free. Ryan Kim, *Wireless System is Closer; S.F. Officials Ready to Request Proposal from 26 Vendors*, S.F. CHRON., Nov. 9, 2005, at D3. In turn, telecoms have asserted that municipal wireless may constitute unfair competition and have begun to lobby for legislation limiting or banning such projects. *See* Michael Hiltzik, *Fed-Up Cities Seek to Provide Net Access*, L.A. TIMES, Oct. 20, 2005, at C1; Bob Keefe, *EarthLink: Latest Deal Raises Profile; Anaheim to Get*

Since its introduction, Wi-Fi usage has seen significant growth. One survey estimates that home wireless use will jump from around 9 million in 2004 to approximately 28 million in 2008.³⁸ Outside the household, industry analysts estimate that by 2008, around 22 million users will log on to over 53,000 available hotspots within the United States.³⁹ These statistics indicate the degree to which wireless has, and will, become a fundamental component of many Americans' lives.⁴⁰

This Note examines a particular aspect of the Wi-Fi landscape: the legality of user access to an open wireless network. An open wireless network consists of an unsecured wireless network that allows users to have roaming access to the Internet.⁴¹ Wireless networking equipment allows consumers to password protect, encrypt, or otherwise disguise their individual Wi-Fi network. Users have the option of either encrypting the wireless signal (which would require someone attempting to access the network to have the encryption key) or implementing password protection (which would require a potential user to enter a password to gain access). Additionally, consumers can change or hide the network name.⁴² These settings provide options for the consumer to secure his or her wireless network.

Despite the added security these options present, the factory settings for wireless equipment typically do not activate these protections and consumers

'Showcase' *Wireless Net*, ATLANTA J.-CONST., Oct. 27, 2005, at F1; Thomas Ott, *Cleveland Heights Wants to Offer Wireless Internet*, CLEV. PLAIN DEALER, Sept. 11, 2005, at B3; Vikas Bajaj, *Legislature Could Revamp Telecom Policy*, DALLAS MORNING NEWS, May 13, 2005, at 1D. The economics and legality of municipal wireless deserves exploration in its own right and is outside the scope of this Note.

³⁸ Rebecca Lieb, *Wi-Fi Moves In*, CLIKZ NETWORK, Oct. 4, 2004, <http://www.clickz.com/stats.old/markets/wireless/article.php/3416331>; see also PAHLAVAN & KRISHNAMURTHY, *supra* note 31, at 432–33 (noting that “the number of home networks . . . is expected to almost double every year”).

³⁹ Matthew Yi, *Wi-Fi Hits the Spot: Businesses Find Wireless Internet Connection Entices Customers to Stay and Pay a Little Longer*, S.F. CHRON., Aug. 25, 2003, at E1.

⁴⁰ One observer has also raised questions about the impact of Wi-Fi on the “third place,” public spaces that wireless may transform into conduits for virtual communities. Stephanie Shapiro, *Out Working*, BALTIMORE SUN, Apr. 18, 2004, at 1N; see also K. DANIEL WONG, WIRELESS INTERNET TELECOMMUNICATIONS 1–3 (2005).

⁴¹ See Benjamin D. Kern, *Whacking, Joyriding and War-Driving: Roaming Use of Wi-Fi and the Law*, 21 SANTA CLARA COMPUTER & HIGH TECH. L.J. 101, 104 (2004).

⁴² The network name, or SSID (Service Set Identifier), identifies the wireless signal broadcast by the consumer. The default setting typically labels the network “default” or the brand name of the wireless equipment. James Coates, *Wi-Fi Hackers Find Routes Easily*, CHI. TRIB., July 10, 2005, § 5, at 2. If a consumer chooses not to broadcast the network name, a user must know the name of the network in order to gain access.

rarely enable these features.⁴³ Consumers may choose not to engage the security measures for a variety of reasons: (1) technological intimidation,⁴⁴ (2) a desire to share Internet access with neighbors or the general public,⁴⁵ (3) a lack of awareness of the risks associated with an unsecured network,⁴⁶ or (4) a lack of concern for the risks that an unsecured network presents.⁴⁷ When the manufacturer or consumer does not enable these protective mechanisms, the wireless network remains unsecured. Regardless of their reasons, a majority of users leave their Wi-Fi networks unsecured, allowing access by a variety of different users.⁴⁸

Popular culture has provided a colorful lexicon for the various users that may access open Wi-Fi networks, including: joyriders, wardrivers, accidental users, and hackers. Joyriders use Wi-Fi connections outside of their home or business to engage in typical Internet activities such as web surfing and email.⁴⁹ Wardrivers use software that is freely available on the Internet to actively search for homes and businesses that provide an open wireless signal beyond the walls of their establishments, then chart or post these hotspots on the Internet.⁵⁰ In some instances, the wardriving software functions in a manner whereby the user does not technically access the wireless network. In others, the wardriver engages in essentially the same level of access as a joyrider. Accidental users quite literally access an open wireless network by happenstance, often thinking they are accessing their own home or office

⁴³ One survey notes that by 2007, upwards of eighty percent of U.S. residential WLANs will be unsecured. Matt Hines, *Worried About Wi-Fi Security?*, CNET NEWS.COM, Jan. 19, 2005, http://news.com.com/Worried+about+Fi+security/2100-7347_3-5540969.html?tag=nefd.lede.

⁴⁴ *Id.*

⁴⁵ See Marriott, *supra* note 15. Marriott interviews one Chicago Internet subscriber who describes leaving her network open as “sticking it to the man.” *Id.*; see also Kern, *supra* note 41, at 104.

⁴⁶ See Kern, *supra* note 41, at 104.

⁴⁷ *Id.* Consumers generally misunderstand or are apathetic toward wireless security. *Id.* However, security risks are cause for concern. For instance, using freely available software, one wardriver was able to connect to an unsecure corporate wireless network and freely access email, user names, passwords, and other company information. Corilyn Shropshire, *Hot Spots for Hackers: Wireless Networks*, PITTSBURGH POST-GAZETTE, Mar. 27, 2005, at C1.

⁴⁸ See Hines, *supra* note 43.

⁴⁹ *Id.*

⁵⁰ See Gomez, *supra* note 9; War, *Peace or Stalemate*, *supra* note 32, at *22–23. The author places wardrivers into the following categories: “(1) they innocently wish to gain free wireless access in their neighborhoods, perhaps at a local coffee shop; (2) they have commercial motivations and hope to sell security services; or (3) they have dishonest motives and hope to surreptitiously access networks [sic] information, send anonymous spam, or acquire illegal data.” *Id.* at *23–24.

network.⁵¹ All of these users may be distinguished from hackers, who access wireless networks for a destructive or malicious purpose, such as data theft, spamming, or other illegal conduct.⁵² This Note focuses on joyriders—those who intentionally access the Internet to engage in normal Internet activities.⁵³ Federal and state statutory law, as well as the common law, may implicate joyriding.

III. FEDERAL STATUTORY LAW: THE COMPUTER FRAUD AND ABUSE ACT

At the federal level, the Computer Fraud and Abuse Act (“CFAA”)⁵⁴ criminalizes certain acts of unauthorized internet access.⁵⁵ The CFAA prohibits specific conduct relating to financial records, nonpublic

⁵¹ See Kern, *supra* note 41, at 104–05.

⁵² *Id.*

⁵³ Non-hacking wardrivers essentially engage in the same conduct as joyriders, making the distinction between the two categories functionally irrelevant. Similarly, accidental users typically engage in approximately the same conduct and thus are encompassed by the analysis of joyriders.

⁵⁴ Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1030 (2000 & Supp. II 2002).

⁵⁵ User access of an open Wi-Fi network represents conduct that intuitively seems to fall under a range of federal laws. However, many provisions regulating internet use target specific conduct, such as the Child Pornography Prevention Act, the Communications Act, and copyright law.

Perhaps most pertinent to the discussion of Wi-Fi is the Electronic Communications Privacy Act (“ECPA”). Electronic Communications Privacy Act, 18 U.S.C. § 2511 (2000). The ECPA amended the Federal Wiretap Act to provide protection against the unauthorized interception of electronic communications. Specifically, the ECPA imposes criminal and civil sanctions on any person who “intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication.” § 2511(1)(a). On its face, this provision would seem to apply to Wi-Fi network access. See Hale, *supra* note 35, at 550–52. *But see* Kern, *supra* note 41, at 136–40.

However, the ECPA provides numerous exceptions, and goes on to state that it shall not be unlawful “for other users of the same frequency to intercept any radio communication made through a system that utilizes frequencies monitored by individuals engaged in the provision or the use of such system, if such communication is not scrambled or encrypted.” 18 U.S.C. § 2511(2)(g)(v) (2000). A Wi-Fi network protected by encryption is by definition no longer an open Wi-Fi network. Thus, this provision enables access to unprotected, and hence open, wireless networks. Going even further, if open wireless networks are assumed public, the ECPA allows any person “to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public.” § 2511(2)(g)(i).

government computers, and viruses, among others.⁵⁶ The most generally applicable provisions require that a user intentionally access a network without authorization.⁵⁷ The two provisions most pertinent to the issue of open Wi-Fi networks are Sections 1030(a)(2) and 1030(a)(5)(A).

Section 1030(a)(2) creates liability for whoever “(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.”⁵⁸ Section 1030(a)(5)(A)(iii) criminalizes whoever “intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage.”⁵⁹ These provisions present two threshold questions⁶⁰: (1) did the user’s conduct constitute intentional, unauthorized access, and (2) did the user’s conduct result in information sharing sufficient to satisfy the terms of section 1030(a)(2)(C) or damage sufficient to satisfy the terms of Section 1030(a)(5)(A)(iii)?

⁵⁶ See 18 U.S.C. §§ 1030(a)(2)(A), 1030(a)(3), 1030(a)(5)(A)(i) (2000 & Supp. II 2002).

⁵⁷ See §§ 1030(a)(2), 1030(a)(5)(A).

⁵⁸ 18 U.S.C. § 1030(a)(2).

⁵⁹ 18 U.S.C. § 1030(a)(5)(A)(iii). This statute in its entirety holds accountable whomever:

(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) by conduct described in clause (i), (ii), or (iii) of subparagraph (A), *caused* (or, in the case of an attempted offense, would, if completed, have caused)—(i) *loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least \$ 5,000 in value . . .*

18 U.S.C. § 1030(a)(5) (emphasis added). Sections 1030(a)(5)(i) and (ii) focus more on conduct akin to hacking rather than joyriding.

⁶⁰ The question of whether a Wi-Fi network constitutes a protected computer appears unlikely to arise. As presently interpreted, the CFAA encompasses conduct on the Internet, which indicates that accessing a Wi-Fi network constitutes conduct within the limits of the statute. See *infra* note 61 (defining “computer”).

A. *Intentional, Unauthorized Access*

The CFAA requires that a user engage in intentional, unauthorized access before liability can attach to the user's conduct. This breaks down into two lines of analysis: whether users have the requisite criminal intent and whether users engage in unauthorized access.

Users must have the requisite mens rea to be culpable under the CFAA. Sections 1030(a)(2) and 1030(a)(5)(A)(iii) require that users *intentionally* access a computer⁶¹ without authorization.⁶² It is unclear whether the intentionality language applies solely to the word "access" or if it extends to encompass the whole phrase "access a computer without authorization."⁶³ What is clear is that the mens rea applies only to one of these phrases; the intentional mens rea does not apply to the damages language of the statute.⁶⁴

Users must engage in unauthorized access to be liable for an offense under the CFAA.⁶⁵ Unfortunately, the CFAA leaves this phrase undefined.⁶⁶

⁶¹ For the purposes of the CFAA, computer is defined as

an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device.

18 U.S.C. § 1030(e)(1). Although this provision does not expressly include the term "network," in *United States v. Morris*, the Second Circuit found that releasing an Internet worm into the Internet—"a national computer network"—falls within the range of conduct regulated by section 1030(a)(5)(A). *United States v. Morris*, 928 F.2d 504, 505 (2d Cir. 1991); see also Dan Hunter, *Cyberspace as Place and the Tragedy of the Digital Anticommons*, 91 CAL. L. REV. 439, 475–76 (2003).

⁶² 18 U.S.C. §§ 1030(a)(2), 1030(a)(5)(A)(iii) (emphasis added). Section 1030(a)(2) differs moderately, attributing the intentional mens rea not only to access without authorization but also to access that "exceeds authorized access." § 1030(a)(2). The CFAA also requires particular mens rea with regard to damages. Sections 1030(a)(2), 1030(a)(5)(A)(ii), and 1030(a)(5)(A)(iii) all require a user to *intentionally* access a network. §§ 1030(a)(2), 1030(a)(5)(A)(ii), 1030(a)(5)(A)(iii) (emphasis added). Section 1030(a)(5)(A)(ii) further requires that the user *recklessly* cause damage. § 1030(a)(5)(A)(ii) (emphasis added). Section 1030(a)(5)(A)(i) requires that the user intentionally cause damage. § 1030(a)(5)(A)(i). Although Section 1030(a)(5)(A)(iii) contains a damage requirement, it applies with strict liability and has no requisite mens rea. § 1030(a)(5)(A)(iii).

⁶³ See *infra* notes 133–35 (discussing the mens rea requirement of the CFAA).

⁶⁴ *Id.*

⁶⁵ 18 U.S.C. §§ 1030(a)(2), 1030(a)(5)(A).

⁶⁶ It does define "exceeds authorized access," holding the term to mean "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter . . ." 18 U.S.C.

Courts have considered the meaning of unauthorized access in a variety of different ways: evaluating the means or purpose of access, looking for a violation of the terms of service governing access, or finding a violation of the express or presumptive terms of access to a website.⁶⁷

B. *Information Sharing and Damages*

In addition to intentional, unauthorized access, the CFAA requires a user to engage in information sharing and/or cause damage to be subject to liability.⁶⁸ Section 1030(a)(2)(C) requires that a user obtain “information from any protected computer if the conduct involved an interstate or foreign communication.”⁶⁹ The CFAA leaves “information” undefined.⁷⁰ While courts have not explicitly addressed what constitutes information, the issue has arisen in a variety of different contexts.⁷¹

While section 1030(a)(2)(C) focuses on information, section 1030(a)(5)(A) focuses on damage. Users must cause damage to be subject to liability under a section 1030(a)(5)(A) claim. Section 1030(a)(5)(A)(iii) specifically requires users to cause damage,⁷² defined as “any impairment to the integrity or availability of data, a program, a system, or information.”⁷³ The damage requirement set forth in this provision compels the court to make individual and aggregate assessments of the loss caused by the unauthorized access.⁷⁴

Section 1030(a)(5)(B) requires that the damage stemming from the unauthorized access cause loss in excess of a statutorily defined minimum.

§ 1030(e)(6); *see also* Orin S. Kerr, *Cybercrime’s Scope: Interpreting “Access” and “Authorization” in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596, 1632–37 (2003).

⁶⁷ *See infra* Part VI.A.1.

⁶⁸ *See* 18 U.S.C. §§ 1030(a)(2)(C), 1030(a)(5)(A).

⁶⁹ 18 U.S.C. § 1030(a)(2)(C). Also, in order to bring a civil claim, a plaintiff must additionally show loss or damage as a result of a violation of this provision. 18 U.S.C. § 1030(g); *see also In re Intuit Privacy Litigation*, 138 F. Supp. 2d 1272, 1280–81 (C.D. Cal. 2001) (addressing whether plaintiff must suffer economic damages under section 1030(g) in order to bring a civil claim).

⁷⁰ Looking at the legislative history, Congress stated that the “premise of 18 U.S.C. 1030(a)(2) will remain the protection, for privacy reasons, of computerized credit records and computerized information relating to customers’ relationship with financial institutions.” S. REP. 99-432, at 6 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2484. Congress later reiterated that the purpose of this section is “privacy protection.” *Id.*

⁷¹ *See infra* Part VI.A.1.

⁷² In contrast to sections 1030(a)(5)(A)(i) and (ii), which require users to intentionally or recklessly cause damage, subsection (iii) only requires that users cause damage, with no attached mens rea.

⁷³ 18 U.S.C. § 1030(e)(8).

⁷⁴ 18 U.S.C. § 1030(a)(5)(B)(i).

Although section 1030(a)(5)(B) sets forth five criteria, one or more of which must be met for the user's section 1030(a)(5)(A) conduct to be actionable, the monetary loss requirement is most germane to the WLAN context. The statute states that in addition to committing an act within the scope of section 1030(a)(5)(B), a user must have "caused . . . (i) loss to 1 or more persons during any 1-year period . . . aggregating at least \$5,000 in value."⁷⁵ The CFAA goes on to define "loss" as "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."⁷⁶ Courts have varied in interpreting loss, specifically with regard to whether the definition includes economic loss.⁷⁷

The CFAA constitutes but one means by which open wireless access may run afoul of the law. In addition to federal law, state laws could prove relevant to open Wi-Fi access.

IV. STATE STATUTORY LAW

All fifty states have enacted legislation that may impact users' access to open wireless networks.⁷⁸ These statutes vary widely in name, including:

⁷⁵ 18 U.S.C. § 1030(a)(5)(B). The statute goes on to list other prohibited effects of section 1030(a)(5)(A) conduct, including, among others, physical injury and a threat to public health or safety, but the monetary provision is most pertinent for the purposes of this Note.

⁷⁶ 18 U.S.C. § 1030(e)(11).

⁷⁷ See *infra* notes 155–63 and accompanying text.

⁷⁸ ALA. CODE § 13A-8-103 (LexisNexis 2004); ALASKA STAT. § 11.46.740 (2004); ARIZ. REV. STAT. ANN. § 13-2316 (2001); ARK. CODE ANN. §§ 5-41-104, 5-41-203 (2006); CAL. PENAL CODE § 502 (West 1999); COLO. REV. STAT. ANN. § 18-5.5-102 (West 2001); CONN. GEN. STAT. ANN. § 53a-251 (West 2001); DEL. CODE ANN. tit. 11, § 932 (2001); FLA. STAT. ANN. § 815.06 (West 2006); GA. CODE ANN. § 16-9-93 (2003); HAW. REV. STAT. § 708-895.7 (Supp. 2005); IDAHO CODE ANN. § 18-2202 (2004); 720 ILL. COMP. STAT. ANN. 5/16D-3 (West 2003); IND. CODE ANN. § 35-43-2-3 (West 2005); IOWA CODE ANN. § 716.6B (West Supp. 2006); KAN. STAT. ANN. § 21-3755 (Supp. 2005); KY. REV. STAT. ANN. §§ 434.850, 434.851, 434.853 (LexisNexis Supp. 2005); LA. REV. STAT. ANN. §§ 14:73.4 (1999), 14:73.7 (Supp. 2006); ME. REV. STAT. ANN. tit. 17-A, § 432 (2006); MD. CODE ANN., CRIM. LAW § 7-302 (LexisNexis 2002); MASS. ANN. LAWS ch. 266, § 120F (LexisNexis Supp. 2006); MICH. COMP. LAWS ANN. § 752.795 (West 2004); MINN. STAT. ANN. § 609.891 (West Supp. 2006); MISS. CODE ANN. § 97-45-5 (West 1999); MO. ANN. STAT. § 569.099 (West Supp. 2006); MONT. CODE ANN. § 45-6-311 (2005); NEB. REV. STAT. ANN. § 28-1344.01 (LexisNexis 2003); NEV. REV. STAT. ANN. § 205.4765 (LexisNexis 2006); N.H. REV. STAT. ANN. § 638:17 (Supp. 2005); N.J. STAT. ANN. § 2A:38A-3 (West 2000); N.M. Stat. Ann. § 30-45-5 (LexisNexis 2004); N.Y. PENAL LAW § 156.05 (McKinney 1999); N.C. GEN. STAT. § 14-454 (2005);

computer trespass, unauthorized use, computer tampering, computer crime, criminal use of a computer, offenses against computer users, and criminal invasion of computer privacy.⁷⁹ The content of these statutes reflects the diversity of their names. State statutes vary with regard to the mens rea and scope of the offense. States define access and authorization differently, or in some cases, not at all.⁸⁰ Additionally, some statutes require that an offender commit harm or cause damage while others provide affirmative defenses to the conduct engaged in by the accused.⁸¹ Sorting through the components of these statutes reveals differences that may impact the viability of an unauthorized access claim.

N.D. CENT. CODE § 12.1-06.1-08 (2005); OHIO REV. CODE ANN. § 2913.04 (West Supp. 2006); OKLA. STAT. ANN. tit. 21, § 1953 (West 2002); OR. REV. STAT. § 164.377 (2005); 18 PA. CONS. STAT. ANN. § 7611 (West Supp. 2006); R.I. GEN. LAWS § 11-52-3 (2002); S.C. CODE ANN. § 16-16-20 (Supp. 2005); S.D. CODIFIED LAWS § 43-43B-1 (2004); TENN. CODE ANN. § 39-14-602 (2003); TEX. PENAL CODE ANN. § 33.02 (Vernon 2001); UTAH CODE ANN. § 76-6-703 (Supp. 2006); VT. STAT. ANN. Tit. 13, § 4102 (Supp. 2005); VA. CODE ANN. § 18.2-152.6 (Supp. 2005); WASH. REV. CODE ANN. § 9A.52.120 (West 2000); W. VA. CODE ANN. § 61-3C-5 (LexisNexis 2005); WIS. STAT. ANN. § 943.70 (West 2005); WYO. STAT. ANN. § 6-3-504 (2005); *see also* Susan W. Brenner, *State Cybercrime Legislation in the United States of America: A Survey*, RICH. J.L. & TECH., ISSUE 3, WINTER 2001, at ¶¶ 8–9 (2001), <http://law.richmond.edu/jolt/v7i3/article2.html>. While this Part focuses on criminal liability, several states have expressly empowered victims of crimes of this nature to bring a civil action to recover damages. *See* CAL. PENAL CODE § 502(e)(1) (West 1999); FLA. STAT. ANN. § 815.06(4)(a) (West 2006); GA. CODE ANN. § 16-9-93(g) (2003); 720 ILL. COMP. STAT. 5/16D-3(b)(6) (2003); IOWA CODE ANN. § 716.6B(2) (West Supp. 2006); MO. ANN. STAT. § 537.525(1) (West 2000); N.J. STAT. ANN. § 2A:38A-3 (West 2000); N.D. CENT. CODE § 12.1-06.1-08(3) (2005); OKLA. STAT. ANN. tit. 21, § 1955 (West 2002); S.C. CODE ANN. § 16-16-25 (Supp. 2005); TENN. CODE ANN. § 39-14-604(a) (2003); VT. STAT. ANN. tit. 13, § 4106 (Supp. 2005); VA. CODE ANN. § 18.2-152.12(A) (Supp. 2005); W. VA. CODE ANN. § 61-3C-16(a) (LexisNexis 2005).

⁷⁹ *See supra* note 78. In addition to statutes that regulate unauthorized access, statutes that target theft of services may also prove relevant to the issue of open Wi-Fi access. While unauthorized access or computer trespass statutes focus more on the means of access, theft of services statutes typically mandate a purpose of obtaining unauthorized computer services. *See, e.g.*, N.H. REV. STAT. ANN. § 638:17(II) (Supp. 2005) (“A person is guilty of the computer crime of theft of computer services when he or she knowingly accesses or causes to be accessed or otherwise uses or causes to be used a computer or computer network with the purpose of obtaining unauthorized computer services.”).

⁸⁰ *See infra* Part IV.B.

⁸¹ *See infra* Part IV.C.

A. *Mens Rea*

State statutes make use of differing mens rea terminology and vary the terms to which the mens rea applies. Statutes use the terms knowingly,⁸² purposely,⁸³ willfully,⁸⁴ intentionally,⁸⁵ or a combination⁸⁶ to specify the

⁸² Examples include Colorado, COLO. REV. STAT. § 18-5.5-102 (2005) (“knowingly [a]ccesses”); New York, N.Y. PENAL LAW § 156.05 (McKinney 1999) (“knowingly uses”); and Ohio, OHIO REV. CODE ANN. § 2913.04(B) (West Supp. 2006) (“knowingly gain access to”). The majority of states make use of some variant of the “knowingly” mens rea. *See* ALASKA STAT. § 11.46.740 (2004); ARIZ. REV. STAT. ANN. § 13-2316 (2001); CAL. PENAL CODE § 502 (West 1999); COLO. REV. STAT. § 18-5.5-102; CONN. GEN. STAT. ANN. § 53a-251 (West 2001); DEL. CODE ANN. tit. 11, § 932 (2001); FLA. STAT. ANN. § 815.06 (West 2006); GA. CODE ANN. § 16-9-93 (2003); HAW. REV. STAT. § 708-895.7 (Supp. 2005); IDAHO CODE ANN. § 18-2202 (2004); 720 ILL. COMP. STAT. ANN. 5/16D-3 (West 2003); IND. CODE ANN. § 35-43-2-3 (West 2004); IOWA CODE ANN. § 716.6B (West Supp. 2006); KY. REV. STAT. ANN. §§ 434.850, 434.851, 434.853 (LexisNexis Supp. 2005); LA. REV. STAT. ANN. § 14:73.7 (Supp. 2006); ME. REV. STAT. ANN. tit. 17-A, § 433 (2006); MO. ANN. STAT. § 569.099 (West Supp. 2006); MONT. CODE ANN. § 45-6-311 (2005); NEB. REV. STAT. ANN. § 28-1344 (LexisNexis 2003); NEV. REV. STAT. ANN. § 205.4765 (LexisNexis 2006); N.H. REV. STAT. ANN. § 638:17 (Supp. 2005); N.J. STAT. ANN. § 2A:38A-3 (West 2000); N.M. Stat. Ann. § 30-45-5 (LexisNexis 2004); N.Y. PENAL LAW § 156.05; OHIO REV. CODE ANN. § 2913.04; OR. REV. STAT. § 164.377 (2005); S.C. CODE ANN. § 16-16-20 (Supp. 2005); S.D. CODIFIED LAWS § 43-43B-1 (2004); TEX. PENAL CODE ANN. § 33.02 (Vernon 2001); VT. STAT. ANN. tit. 13, § 4102 (Supp. 2005); W. VA. CODE ANN. § 61-3C-5 (LexisNexis 2005); WYO. STAT. ANN. § 6-3-504 (2005).

⁸³ Montana requires an offender to engage in conduct “knowingly or purposely.” MONT. CODE ANN. § 45-6-311 (1) (2005). New Jersey also states a mens rea of “purposeful or knowing.” N.J. STAT. ANN. § 2A:38A-3 (West 2000).

⁸⁴ North Carolina requires an offender to engage in access “willfully,” N.C. GEN. STAT. § 14-454 (2005), as do Alabama, ALA. CODE § 13A-8-103 (LexisNexis 2005), Oklahoma, OKLA. STAT. ANN. tit. 21, § 1953 (West 2002), and Virginia, VA. CODE ANN. § 18.2-152.6 (Supp. 2005).

⁸⁵ ARK. CODE ANN. § 5-41-104 (2006); KAN. STAT. ANN. § 21-3755(d) (Supp. 2005); MICH. COMP. LAWS ANN. § 752.795 (West 2004); MINN. STAT ANN. § 609.891 (West Supp. 2006), MISS. CODE ANN. § 97-45-5 (West 1999); NEB. REV. STAT. ANN. § 28-1344 (LexisNexis 2003); N.D. CENT. CODE § 12.1-06.1-08(2) (2005); 18 PA. CONS. STAT. ANN. § 7611(a)(2) (West Supp. 2006); R.I. GEN. LAWS § 11-52-3 (2002); TENN. CODE ANN. § 39-14-602(b) (2003); WASH. REV. CODE ANN. § 9A.52.120(1) (West 2000).

⁸⁶ Florida requires an offender to engage in accesses “willfully, knowingly, and without authorization.” FLA. STAT. ANN. § 815.06 (West 2006). Maryland states a mens rea of intentionally and willfully. MD. CODE ANN., CRIM. LAW § 7-302(c)(1) (LexisNexis 2002). Other states provide options, such as Indiana’s mens rea requirement of “knowingly or intentionally,” IND. CODE ANN. § 35-43-2-3(b) (West 2004), or New Jersey’s requirement of “purposeful or knowing.” N.J. STAT. ANN. § 2A:38A-3(c) (West 2000); *see also supra* note 84.

mens rea of the delineated offense. Additionally, the state of Utah appears to have eschewed a mens rea requirement and made unauthorized access a strict liability offense.⁸⁷ The differing mens rea in and of themselves are not particularly compelling; these terms encompass roughly the same category of conduct.⁸⁸ More importantly, states apply these mens rea in different ways.

States vary in how they apply the mens rea within a statute, most pertinently with regard to the terms access and authorization. Most states apply the mens rea to the access phrase with a lack of authorization being another element of the offense.⁸⁹ A typical statute in these jurisdictions

⁸⁷ Utah's statute penalizes "[a] person who without authorization gains or attempts to gain access to . . . any . . . computer network . . . and thereby . . . obtains . . . a benefit for any person without [a] legal right." UTAH CODE ANN. § 76-6-703(1) (Supp. 2006).

⁸⁸ While states provide specific definitions for culpable mental states within their codes, for the sake of expediency, consider the statutes' mens rea in light of the Model Penal Code. The Model Penal Code provides the following definitions:

(a) Purposely.

A person acts purposely with respect to a material element of an offense when:

(i) if the element involves the nature of his conduct or a result thereof, it is *his conscious object* to engage in conduct of that nature or to cause such a result;

and

(ii) if the element involves the attendant circumstances, he is aware of the existence of such circumstances or he believes or hopes that they exist.

(b) Knowingly.

A person acts knowingly with respect to a material element of an offense when:

(i) if the element involves the nature of his conduct or the attendant circumstances, *he is aware* that his conduct is of that nature or that such circumstances exist;

and

(ii) if the element involves a result of his conduct, he is aware that it is practically certain that his conduct will cause such a result.

MODEL PENAL CODE § 2.02(2) (1962) (emphasis added). The distinction between these two mental states is functionally irrelevant because both states that make use of the "purposely" mens rea use it alternatively with knowingly. *See supra* note 84. The Model Penal Code goes on to state that "[a] requirement that an offense be committed wilfully [sic] is satisfied if a person acts knowingly with respect to the material elements of the offense, unless a purpose to impose further requirements appears." § 2.02(8). Thus, those states that employ a "willful" mens rea, *see supra* note 84, could be viewed as using a "knowing" mens rea. Lastly, the code provides that "'intentionally' or 'with intent' means purposely." § 1.13(12). So, the eleven states that use the "intentional" mens rea, *see supra* note 85, essentially are using a "purposeful" mens rea. Given the aforementioned, in a Model Penal Code world, the only practical difference in culpability would be between the eleven states that employ the "intentional" (i.e., purposeful) mens rea; the remaining thirty-nine states essentially all require a culpable mental state of "knowing."

⁸⁹ ALA. CODE § 13A-8-103 (LexisNexis 2005); ALASKA STAT. §11.46.740 (2005); ARIZ. REV. STAT. ANN. § 13-2316 (2001); ARK. CODE ANN. §§ 5-41-104, 5-41-203

would prohibit an offender from knowingly and without authorization accessing a computer network.⁹⁰ Other states take the opposite approach, applying the mens rea to authorization, with access constituting another element of the offense.⁹¹ In these states, statutes prohibit a person from accessing a network and provide that the person must know his or her access is not authorized.⁹² Lastly, some statutes apply the mens rea to both access and authorization,⁹³ with a representative statute requiring a person to both knowingly access a network and know that his or her access is not authorized.⁹⁴ These variances constitute more than semantic differences. A

(2006); CAL. PENAL CODE § 502 (West 1999); COLO. REV. STAT. § 18-5.5-102 (2005); FLA. STAT. ANN. § 815.06 (West 2006); HAW. REV. STAT. § 708-895.7 (Supp. 2005); IDAHO CODE ANN. § 18-2202 (2004); 720 ILL. COMP. STAT. ANN. 5/16D-3 (West 2003); IND. CODE ANN. § 35-43-2-3 (West 2004); IOWA CODE ANN. § 716.6B (West Supp. 2006); KAN. STAT. ANN. § 21-3755(d) (Supp. 2005); KY. REV. STAT. ANN. §§ 434.850, 434.851, 434.853 (LexisNexis Supp. 2005); LA. REV. STAT. ANN. §§ 14:73.4 (1999), 14:73.7 (Supp. 2006); MD. CODE ANN., CRIM. LAW § 7-302 (LexisNexis 2002); MASS. ANN. LAWS ch. 266, § 120F (LexisNexis Supp. 2006); MICH. COMP. LAWS ANN. § 752.795 (West 2004); MINN. STAT. ANN. § 609.891 (West Supp. 2006); MISS. CODE ANN. § 97-45-5 (West 1999); MO. ANN. STAT. § 569.099 (West Supp. 2006); MONT. CODE ANN. § 45-6-311 (2005); NEV. REV. STAT. ANN. § 205.4765 (LexisNexis 2006); N.J. STAT. ANN. § 2A:38A-3 (West 2000); N.M. Stat. Ann. § 30-45-5 (LexisNexis 2004); N.Y. PENAL LAW § 156.05 (McKinney 1999); N.C. GEN. STAT. § 14-454 (2005); N.D. CENT. CODE § 12.1-06.1-08(2) (2005); OHIO REV. CODE ANN. § 2913.04(B) (West Supp. 2006); OKLA. STAT. ANN. tit. 21, § 1953 (West 2002); OR. REV. STAT. § 164.377 (2005); 18 PA. CONS. STAT. ANN. § 7611 (West Supp. 2006); R.I. GEN. LAWS § 11-52-3 (2002); S.C. CODE ANN. § 16-16-20 (Supp. 2005); S.D. CODIFIED LAWS § 43-43B-1 (2004); TENN. CODE ANN. § 39-14-602(b) (2003); TEX. PENAL CODE ANN. § 33.02 (Vernon 2001); UTAH CODE ANN. § 76-6-703 (Supp. 2005); VT. STAT. ANN. tit. 13, § 4102 (Supp. 2005); VA. CODE ANN. § 18.2-152.6 (Supp. 2005); WASH. REV. CODE ANN. § 9A.52.120 (2000); W. VA. CODE ANN. § 61-3C-5 (LexisNexis 2005); WIS. STAT. ANN. § 943.70 (West 2005); WYO. STAT. ANN. § 6-3-504 (2005).

⁹⁰ See, e.g., Florida's statute delineating offenses against computer users, which states: "Whoever willfully, knowingly, and without authorization . . . accesses or causes to be accessed any . . . computer network . . ." FLA. STAT. ANN. § 815.06(1)(a) (West 2006).

⁹¹ CONN. GEN. STAT. ANN. § 53a-251(b) (West 2001); DEL. CODE ANN. tit. 11, § 932 (2001); GA. CODE ANN. § 16-9-93 (2003).

⁹² See, e.g., Delaware's statute, holding that a person is guilty of unauthorized access when, "knowing that the person is not authorized to do so, the person accesses . . . any computer system without authorization." DEL. CODE ANN. tit. 11, § 932 (2001).

⁹³ ME. REV. STAT. ANN. tit. 17-A, § 432 (2006); NEB. REV. STAT. ANN. § 28-1344 (LexisNexis 2003); N.H. REV. STAT. ANN. § 638:17 (Supp. 2005).

⁹⁴ See, e.g., New Hampshire's statute criminalizing conduct when, "knowing that the person is not authorized to do so, he or she knowingly accesses . . . any . . . computer network without authorization." N.H. REV. STAT. ANN. § 638:17(I) (Supp. 2005).

state's particular application of mens rea has implications for the viability of a claim of unauthorized access regarding open wireless networks.⁹⁵

B. Access and Authorization

The majority of states define the term “access” by statute,⁹⁶ typically referencing interaction with a computer network.⁹⁷ Although states define “access” similarly, courts’ interpretations are anything but—contradictory precedent exists regarding the scope of “access.”⁹⁸

⁹⁵ See *infra* Part VI.B.

⁹⁶ ALA. CODE § 13A-8-101(11) (LexisNexis 2005); ARIZ. REV. STAT. ANN. § 13-2301(E)(1) (2001); ARK. CODE ANN. § 5-41-102(1) (2006); CAL. PENAL CODE § 502(b)(1) (West 2005); COLO. REV. STAT. § 18-5.5-101(10) (2005) (defining “use”); CONN. GEN. STAT. ANN. § 53a-250(1) (West 2001); DEL. CODE ANN. tit. 11, § 931(1) (2001); FLA. STAT. § 815.02(1) (2005); GA. CODE ANN. § 16-9-92(16) (Supp. 2006) (defining “use”); HAW. REV. STAT. § 708-890 (Supp. 2005); IDAHO CODE ANN. § 18-2201(1) (2004); 720 ILL. COMP. STAT. ANN. 5/16D-2(e) (West 2003); IND. CODE ANN. § 35-43-2-3(a) (West 2004); KAN. STAT. ANN. § 21-3755(a)(1) (Supp. 2005); KY. REV. STAT. ANN. §§ 434.840(1) (LexisNexis Supp. 2005); LA. REV. STAT. ANN. § 14:73.1(1) (Supp. 2006); ME. REV. STAT. ANN. tit. 17-A, § 431(1) (2006); MD. CODE ANN., CRIM. LAW § 7-302(a)(2) (LexisNexis 2002); MICH. COMP. LAWS ANN. § 752.792 Sec. 2(1) (West 2004); MINN. STAT. ANN. § 609.87 Subd. 2 (West 2003); MISS. CODE ANN. § 97-45-1(a) (West 2005); MONT. CODE ANN. § 45-6-310 (2005) (defining “obtain the use of”); NEB. REV. STAT. ANN. § 28-1343(1) (LexisNexis 2003); NEV. REV. STAT. ANN. § 205.4732 (LexisNexis 2006); N.H. REV. STAT. ANN. § 638:16(I) (Supp. 2005); N.J. STAT. ANN. § 2C:20-23(a) (West 2005); N.M. Stat. Ann. § 30-45-2(A) (LexisNexis 2004); N.Y. PENAL LAW § 156.00(6) (McKinney 1999) (defining “uses a computer or computer service without authorization”); N.C. GEN. STAT. § 14-453(1) (2005); N.D. CENT. CODE § 12.1-06.1-01(3)(a) (2005); OHIO REV. CODE ANN. § 2913.01(T) (West Supp. 2006); OKLA. STAT. ANN. tit. 21, § 1952(1) (West 2002); OR. REV. STAT. § 164.377(1)(a) (2005); R.I. GEN. LAWS § 11-52-1(1) (2002); S.C. CODE ANN. § 16-16-10(i) (Supp. 2005); S.D. CODIFIED LAWS § 43-43B-2(1) (2004); TENN. CODE ANN. § 39-14-601(1) (2003); TEX. PENAL CODE ANN. § 33.01(1) (Vernon 2001); UTAH CODE ANN. § 76-6-702(1) (Supp. 2006); VT. STAT. ANN. tit. 13, § 4101(1) (Supp. 2005); VA. CODE ANN. § 18.2-152.2 (Supp. 2005) (defining “uses”); WASH. REV. CODE ANN. § 9A.52.010(6) (West Supp. 2006); W. VA. CODE ANN. § 61-3C-3(a) (LexisNexis 2005); WIS. STAT. ANN. § 943.70(1) (West 2005); WYO. STAT. ANN. § 6-3-501(a)(i) (2005).

⁹⁷ See, e.g., Florida, which defines access as “to approach, instruct, communicate with, store data in, retrieve data from, or otherwise make use of any resources of a computer, computer system, or computer network.” FLA. STAT. ANN. § 815.03(1) (West 2006).

⁹⁸ See *infra* Part VI.B.1.

In contrast to access, few states define what constitutes authorization.⁹⁹ The states that do provide definitions vary in the scope of conduct encompassed by the term. Some states define authorization as requiring the express consent of the owner.¹⁰⁰ Other states base the definition on a reasonableness standard¹⁰¹ or implied consent.¹⁰² Still other states define authorization generically in terms of consent or permission.¹⁰³ Unfortunately, state case law does little to illuminate the meaning of authorization. The few state cases that have addressed authorization have arisen primarily in the context of employee misconduct.¹⁰⁴ In some states, the determination of

⁹⁹ COLO. REV. STAT. § 18-5.5-101(1) (2005); GA. CODE ANN. § 16-9-92(18) (Supp. 2006); HAW. REV. STAT. § 708-890 (Supp. 2005); ME. REV. STAT. ANN. tit. 17-A, § 431(11) (2006); MINN. STAT. ANN. § 609.87 Subd. 2a (West 2003); N.H. REV. STAT. ANN. § 638:16(II) (Supp. 2005); N.J. STAT. ANN. § 2C:20-23(q) (2005); N.C. GEN. STAT. § 14-453(1a) (2005); R.I. GEN. LAWS § 11-52-1(15)(v) (2002); S.C. CODE ANN. § 16-16-10(1) (Supp. 2005); TENN. CODE ANN. § 39-14-601(2) (2003); UTAH CODE ANN. § 76-6-702(2) (2006); VA. CODE ANN. § 18.2-152.2 (Supp. 2005); W. VA. CODE ANN. § 61-3C-3(b) (LexisNexis 2005). In the absence of a definition, at least one court has turned to Black's Law Dictionary and Webster's Dictionary for guidance. *See Briggs v. State*, 704 A.2d 904, 909 (Md. 1998).

¹⁰⁰ *See, e.g.*, Colorado, which defines authorization as "the express consent of a person . . . to use said person's . . . computer network." COLO. REV. STAT. § 18-5.5-101(1) (2005).

¹⁰¹ While New Jersey defines authorization as permission, authority, or consent, the statute goes on to provide that "[a]n actor has authorization if a reasonable person would believe that the act was authorized." N.J. STAT. ANN. § 2C:20-23(q) (West 2005).

¹⁰² *See, e.g.*, South Carolina, which provides that "[u]nauthorized access" means access of a . . . computer network not explicitly or implicitly authorized by the appropriate principal." S.C. CODE ANN. § 16-16-10(1) (Supp. 2005). Tennessee provides perhaps the broadest definition, stating that "[a]uthorization" means any and all forms of consent, including both implicit and explicit consent." TENN. CODE ANN. § 39-14-601(2) (Supp. 2005).

¹⁰³ *See, e.g.*, Maine, which states that "unauthorized" mean[s] not having consent or permission of the owner." ME. REV. STAT. ANN. tit. 17-A, § 431(11) (2006). These definitions offer little clarity to the meaning of authorization, as they turn on the interpretations of permission and consent which are themselves undefined terms. Minnesota provides an exception to this vagary; while the statute defines authorization as permission, it goes on to state that "[a]uthorization may be limited by the owner by: (1) giving the user actual notice orally or in writing; (2) posting a written notice in a prominent location adjacent to the computer being used; or (3) using a notice displayed on or announced by the computer being used." MINN. STAT. ANN. § 609.87 Subd. 2a (West 2003). The last two options illustrate the conundrum presented by Wi-Fi: wireless networking changes the location dynamic such that posting or displaying a notice by a computer becomes impractical.

¹⁰⁴ *See Fugarino v. State*, 531 S.E.2d 187, 189 (Ga. Ct. App. 2000) (finding that Fugarino lacked the authority to delete portions of a company's computer program, as indicated by the testimony of the company's owner that no such permission was granted

unauthorized access ends the inquiry—liability attaches upon satisfaction of these terms. However, many states require damages for users to be culpable under state law.

C. Harm and Damages

In accord with the different statutory structures aforementioned, states vary in the manner in which they treat harm and damages. Some states predicate users' liability on whether some other harm occurs in addition to the unauthorized access. While the vast majority of states reject basing liability on an additional element, many states vary the offense level in connection with the amount of damage caused by the unauthorized access.

A handful of states criminalize unauthorized access *only if* accompanied by some harm being caused as a result of the access. For instance, Alaska requires that in addition to engaging in unauthorized access, an offender must, at a minimum, "obtain[] information concerning a person."¹⁰⁵ Under Georgia's computer trespass statute, an offender must not only use a computer without authority, but use the computer with the "intention of . . . [a]ltering, damaging, or in any way causing the malfunction of a . . . computer network."¹⁰⁶ The conduct criminalized by these statutes is comparable to higher level offenses in most other states,¹⁰⁷ but here

and by the "vindictive and retaliatory manner" of Fugarino's conduct); *State v. Olson*, 735 P.2d 1362, 1365–66 (Wash. Ct. App. 1987) (explaining that police officer's access of police database for personal use was not without authority; permission to use the database was not predicated on the uses made of the data, thus while against departmental policy, police officer still had authority to access); *Briggs v. State*, 704 A.2d 904, 909–10 (Md. 1998) (stating that system administrator had authority to access computer, thus while his conduct was inappropriate, he had the authority to engage in it because the Maryland statute prohibits only unauthorized access, not access outside the scope of authority); *see also Kerr, supra* note 66, at 1596, 1632–37.

¹⁰⁵ ALASKA STAT. § 11.46.740(a)(1) (2004).

¹⁰⁶ GA. CODE ANN. § 16-9-93(b) (2003). Although the statute requires the offender to engage in some form of harm, the harm may be only for a brief moment. *Id.* (stating that the requirement of alteration, damage, or malfunction applies "regardless of how long the alteration, damage, or malfunction persists"). It seems that momentary interference by a wireless user may be sufficient conduct to fall within the scope of the statute. North Carolina's statute addresses conduct in an even more vague manner. The statute prohibits unlawful access for purposes of fraud or obtaining property, but goes on to prohibit unauthorized access for any purpose as a lesser offense. N.C. GEN. STAT. § 14-454 (2005). This would appear to require a purpose behind the unauthorized access, but the extent of this purpose is unclear.

¹⁰⁷ For instance, in Hawaii, obtaining personal information, as per the Alaska statute, would raise the level of unauthorized access offense from a third degree misdemeanor to a class C felony. HAW. REV. STAT. §§ 708-895.6, 708-895.7 (Supp. 2005).

represents the minimum conduct required for an offender to face conviction for unauthorized access. While only a few states require a minimum level of additional harm, several tie the level of the offense to the monetary amount of damage caused.

Conviction for unauthorized access ranges from a misdemeanor to a felony offense, with some states varying the offense level in proportion to the amount of damage caused by the offender. For example, Delaware delineates five degrees of unauthorized access.¹⁰⁸ The highest level of offense is a class D felony and applies “when the damage to or the value of the property or computer services affected exceeds \$10,000.”¹⁰⁹ The lowest level offense, a class A misdemeanor, applies where the damage or value of the property at issue is \$500 or less.¹¹⁰ In some instances, no damage may be required and no unauthorized access need occur—fourteen states prohibit attempted unauthorized access.¹¹¹ In the event that users engage in unauthorized access in violation of state law, some states provide defenses or other means that may absolve users’ conduct.

D. Affirmative Conduct, Defenses, and Exceptions

Although nearly all states focus on the conduct of the offender in unauthorized access statutes, the State of New York imposes an affirmative conduct requirement on network operators. New York’s unauthorized use statute prohibits the knowing use of a computer service without authorization.¹¹² However, the statute only applies where the accessed computer “is 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.”¹¹³ Unless owners or operators protect their computer networks, the statute does not apply.¹¹⁴ New York represents the extreme by essentially imposing requirements on network operators, but a number of states offer avenues for users to avoid liability.

¹⁰⁸ DEL. CODE ANN. tit. 11, § 939 (2001).

¹⁰⁹ § 939(a).

¹¹⁰ § 939(e).

¹¹¹ *See, e.g.*, Ohio, which criminalizes an offender who “knowingly attempt[s] to gain access to . . . [a] computer network . . . without . . . consent.” OHIO REV. CODE ANN. § 2913.04(B) (West Supp. 2006).

¹¹² N.Y. PENAL LAW § 156.05 (McKinney 1999).

¹¹³ *Id.*

¹¹⁴ Similarly, Nebraska and Minnesota both have unauthorized access statutes that require that an offender “penetrate[] a computer security system.” NEB. REV. STAT. ANN. § 28-1343.01(1) (LexisNexis 2003); MINN. STAT. ANN. § 609.891 Subd. 1 (West Supp. 2006).

Several states provide other affirmative defenses and exceptions to unauthorized access offenses. Many of these are grounded in reasonableness. In some states, offenders may escape culpability for an offense by showing that they had reasonable grounds to believe that their access was authorized¹¹⁵ or could not have reasonably known that their access was unauthorized.¹¹⁶ Other states have provided affirmative defenses protecting employee conduct¹¹⁷ and acts that further computer security.¹¹⁸

While criminalizing unauthorized access, many of the previously mentioned federal and state laws provide for civil liability as well. But in the context of civil liability, the common law may prove a pertinent doctrine to addressing joyriding conduct.

V. COMMON LAW: TRESPASS TO CHATTELS

Courts may construe the common law doctrine of trespass to chattels in a manner that includes civil liability for users that connect to open Wi-Fi networks.¹¹⁹ The doctrine of trespass to chattels protects an individual's property from the use of others. The Restatement (Second) of Torts defines the doctrine, stating that "[a] trespass to a chattel may be committed by intentionally (a) dispossessing another of the chattel, or (b) using or intermeddling with a chattel in the possession of another."¹²⁰ An individual will only be liable to the possessor of the chattel if:

¹¹⁵ See, e.g., NEV. REV. STAT. ANN. § 205.477(4) (LexisNexis 2006) ("It is an affirmative defense . . . that at the time of the alleged offense the defendant reasonably believed that . . . [h]e was authorized to use or access the . . . network.").

¹¹⁶ See, e.g., CONN. GEN. STAT. § 53a-251(b)(2)(C) (2001) ("It shall be an affirmative defense to a prosecution for unauthorized access to a computer system that . . . the person reasonably could not have known that his access was unauthorized.").

¹¹⁷ See, e.g., FLA. STAT. § 815.06(6) (2006) ("This section does not apply to any person who accesses his or her employer's . . . computer network . . . when acting within the scope of his or her lawful employment.").

¹¹⁸ See, e.g., UTAH CODE ANN. § 76-6-703(5) (LexisNexis Supp. 2006) ("It is an affirmative defense . . . that a person obtained access . . . in response to, and for the purpose of protecting against or investigating, a prior attempted or successful breach of security.").

¹¹⁹ See Hale, *supra* note 35, at 552; Kern, *supra* note 41, at 152. The law of contracts provides another important dynamic to both the statutory and common law provisions. Internet service providers ("ISPs") contract with consumers to provide services. These contracts may impact the interpretation of authorization and in turn impact whether conduct comports with or violates the law. See Kerr, *supra* note 66, at 1637-40.

¹²⁰ RESTATEMENT (SECOND) OF TORTS § 217 (1965).

(a) he dispossesses the other of the chattel, or (b) the chattel is impaired as to its condition, quality, or value, or (c) the possessor is deprived of the use of the chattel for a substantial time, or (d) bodily harm is caused to the possessor, or harm is caused to some person or thing in which the possessor has a legally protected interest.¹²¹

Courts have interpreted these criteria in varying ways, and in some instances have found that open Wi-Fi access amounts to conduct contemplated by the Restatement.¹²²

Traditionally, trespass to chattels required physical touching or entry to constitute an actionable tort.¹²³ However, courts have applied the doctrine of trespass to chattels to electronic communications, creating what may be termed electronic or digital trespass.¹²⁴ Even if courts extend the doctrine to cover electronic conduct, damages remain a pressing concern. Damages considerations represent an important threshold issue in a court's application of trespass to chattels to Internet-related conduct. While courts may issue an injunction premised merely on the trespass, for the doctrine to be actionable, a plaintiff must demonstrate damage.¹²⁵

Several defenses to trespass to chattels exist, but most relevant is the doctrine of apparent consent, which may insulate users from liability for open wireless access. According to the Restatement, "[i]f words or conduct are reasonably understood by another to be intended as consent, they constitute apparent consent and are as effective as consent in fact."¹²⁶ In the context of wireless access, apparent consent could be inferred from leaving a wireless network unsecured.

¹²¹ *Id.* at § 218.

¹²² *See infra* Part VI.C.

¹²³ *See* *Thrifty-Tel, Inc. v. Bezenek*, 54 Cal. Rptr. 2d 468, 473 n.6 (Cal. Ct. App. 1996). This reflects the physical nature of a chattel, defined by Black's Law Dictionary as "[m]ovable or transferable property; personal property; esp., a physical object capable of manual delivery and not the subject matter of real property." BLACK'S LAW DICTIONARY 251 (8th ed. 2004).

¹²⁴ *Thrifty-Tel*, 54 Cal. Rptr. 2d at 473 n.6 ("In our view, the electronic signals generated by the Bezenek boys' activities were sufficiently tangible to support a trespass cause of action."); *see also* *White Buffalo Ventures L.L.C. v. Univ. of Texas*, 420 F.3d 366, 377 n.24 (5th Cir. 2005).

¹²⁵ *See infra* Part VI.C.

¹²⁶ RESTATEMENT (SECOND) OF TORTS § 892(2) (1965).

VI. THE APPLICABILITY OF STATUTORY AND COMMON LAW TO OPEN WIRELESS ACCESS

While prosecutors charged Benjamin Smith solely under Florida law, his case raises the bigger question pertinent to all Wi-Fi joyriders: is accessing an open wireless network legal? While a court can issue an injunction based on electronic trespass conduct, a plaintiff must demonstrate damage from the conduct in order to bring a colorable trespass to chattels action. In the federal context, if courts broadly construe the terms “access” and “authorization,” and liberally interpret the type and amount of damages permissible by statute, an individual may be liable for unauthorized access conduct. The same applies for state statutes constructed and interpreted similarly to the CFAA. However, differing state statutes lead to varying results. Liability attaches more easily in states with a minimal or no damage requirement. In contrast, liability is unlikely in states such as New York, which requires users to circumvent security for their conduct to be actionable.¹²⁷ Turning to the common law, user liability under the trespass to chattels doctrine depends on a court’s willingness to extend the doctrine to encompass unauthorized access conduct.

A. *The CFAA*

Distinguishing between intentional, unauthorized access and authorized access is paramount in the context of determining liability for users’ access to open Wi-Fi networks. The nature of Wi-Fi makes this determination a challenge. The CFAA originally addressed technology that significantly differs from Wi-Fi technology.¹²⁸ Given this difference, the language of the statute and precedent regarding authorization and access are unclear as applied to wireless networks.

¹²⁷ N.Y. PENAL LAW § 156.05 (McKinney 1999).

¹²⁸ The CFAA targeted technology that differs significantly from the wireless technology utilized today. Congress enacted the CFAA in 1984, significantly amending it in 1986 and 1994. In the mid-1980s, networks did not provide broad public access, but were instead private. *See* Kern, *supra* note 41, at 123. A user would need to physically enter a computing facility and access the network while on-site. As technology evolved, so did the means of access. In the late-1980s and through the 1990s, the Internet blossomed into a widely-used publicly accessible network. This development changed the access dynamic. Network access no longer required physical entry to a computing facility; a user could freely access the network from his or her home or business via dial-up, and later, broadband. Thus, while users were still tied to a physical location (the point of access created by the landline), the network, the Internet became widely available for public use. Wi-Fi networking represents the next evolution in the networking dynamic by allowing for less physically restricted access to the Internet.

1. *Case Interpretation*

Cases interpreting the CFAA reflect the difficulties brought on by the changing dynamic of network access. Some courts have examined the legislative history and text of the original CFAA to create a distinction between “insiders” and “outsiders.”¹²⁹ Under this distinction, provisions of the CFAA “‘are intended to apply to outsiders who access a computer,’ not to ‘insiders’ who access individuals’ computers with their permission to do so.”¹³⁰ However, other courts have cited the legislative history of the 1996 amendments to the CFAA to support the proposition that the insider/outsider distinction no longer exists.¹³¹ This initial distinction creates confusion about the exact scope and applicability of the act as a whole. Further complicating matters are the courts’ varying interpretations of the mens rea requirement, of what constitutes intentional unauthorized access, and the nature and measure of damages.

Courts have attempted to clarify the appropriate application of the “intentional” mens rea within the provisions of the CFAA. Both Section 1030(a)(2) and 1030(a)(5)(A)(ii) contain the intentional mens rea. In interpreting these statutes, courts faced the issue of whether this mens rea applied only to the term “access” or if it applied to the term “damages” as well. In evaluating section 1030(a)(5)(A), the Second Circuit indicated that the intentionality standard applies to the “accesses” phrase and not to damages:¹³²

Despite some isolated language in the legislative history that arguably suggests a scienter component for the “damages” phrase of section 1030(a)(5)(A), the wording, structure, and purpose of the subsection, examined in comparison with its departure from the format of its

¹²⁹ *Am. Online, Inc. v. Nat’l Health Care Disc., Inc.*, 121 F. Supp. 2d 1255, 1272, 1275 (N.D. Iowa 2000); *see also SecureInfo Corp. v. Telos Corp.*, 387 F. Supp. 2d 593, 609 (E.D. Va. 2005); *see also* S. Rep. No. 99-432, at 10–11 (1986) *reprinted in* 1986 U.S.C.C.A.N. 2479, 2488.

¹³⁰ *SecureInfo*, 387 F. Supp. 2d at 609, (citing *In re Am. Online, Inc.*, 168 F. Supp. 2d 1359, 1370–71 (S.D. Fla. 2001)). Congress’s willingness to draw a bright line distinction may be attributed to the physical access dynamic prevalent during the time period in which Congress enacted the original CFAA (as opposed to the current ubiquity of network and Internet usage). *See supra* note 128.

¹³¹ *Shurgard Storage Centers v. Safeguard Self Storage*, 119 F. Supp. 2d 1121, 1127 (W.D. Wash. 2000) (“Though the original scope of the CFAA was limited to [‘outsiders’ or ‘hackers,’ and not ‘insiders’ (employees)], its subsequent amendments have broadened the scope.”); *see also Am. Online*, 168 F. Supp. 2d at 1371 (specifically rejecting the insider/outsider distinction in the context of 18 U.S.C. § 1030(a)(5)(A) (2000 & Supp. III 2003)); Kern, *supra* note 41, at 122–23.

¹³² *United States v. Morris*, 928 F.2d 504, 509 (2d Cir. 1991).

predecessor provision persuade us that the “intentionally” standard applies only to the “accesses” phrase of section 1030(a)(5)(A), and not to its “damages” phrase.¹³³

Because the *Morris* court used the word “phrase,” as opposed to “term” or “word,” it appears to indicate that the intentional mens rea may extend to cover the whole of the “accesses a protected computer without authorization” phrase. Courts have not explicitly addressed this matter of statutory interpretation, but a few cases have indicated that the intentional mens rea applies only to the word “access.”¹³⁴ The bigger interpretive issue falls on the courts’ views of access and authorization.

Liability for an offense under the CFAA rests in part on an undefined term: unauthorized access.¹³⁵ In considering access, one court turned to the dictionary to define the act of accessing as “exercis[ing] the ‘freedom or

¹³³ *Morris*, 928 F.2d at 509 (emphasis added); see also *United States v. Sablan*, 92 F.3d 865, 868 (9th Cir. 1996); *Letscher v. Swiss Bank Corp.*, No. 94 Civ. 8277, 1997 WL 304895, at *5 (S.D.N.Y. June 5, 1997).

¹³⁴ The *Sablan* court expressly adopted the language of *Morris*. *Sablan*, 92 F.3d at 868. However, it is unclear whether the court intended to use *Morris* merely to disallow application of the “intentional” mens rea to the damages provision or to extend the intent mens rea to encompass the whole “accesses” phrase. At one point the court states that “*Sablan* must have had a wrongful intent in accessing the computer in order to be convicted under the statute.” *Sablan*, 92 F.3d at 869. This does not include the “without authorization” phrase, and may be indicative of the court’s desire to limit the wrongful intent requirement only to “access.” *Sablan*, 92 F.3d at 868 n.69; see also *Letscher*, 1997 WL 304895, at *5 (“As the Second Circuit has indicated, a claim under this section requires proof of intentional acts of unauthorized access—the statute is not designed to reach ‘mistaken, inadvertent, or careless acts of unauthorized access.’”) (quoting *Morris*, 928 F.2d at 507).

¹³⁵ 18 U.S.C. §§ 1030(a)(2), 1030(a)(5)(A) (2000 & Supp. III 2003); see *supra* note 66 and accompanying text. Relevant to Section 1030(a)(2), the statute defines computer as:

an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device.

18 U.S.C. § 1030(e)(1) (2000). Pertinent to section 1030(a)(5)(A), the CFAA definition for a protected computer includes a computer “which is used in interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States.” § 1030(e)(2)(B).

ability to . . . make use of” something.”¹³⁶ Once the *National Health Care Discount* court extrapolated that access under the CFAA, it encompassed a broad range of conduct, reaching so far as to include emails passing through a computer.¹³⁷ Beyond using the dictionary, courts have evaluated unauthorized access in different ways: referencing the means of access or the purpose of access, violating the provisions of a “terms of service” agreement, violating the terms of access to a website, or presumptively violating the terms of access to a website.¹³⁸

Courts have focused on the intended function (i.e., the means or purpose) of access to determine whether unauthorized access occurs. In *Morris*, the defendant was convicted under section 1030(a)(5)(A) for releasing a computer worm onto the Internet. The court focused on Morris’s use of a network’s email capabilities and the ability to learn information about the users of other computers on the network. In evaluating this conduct, the court noted that “Morris did not use either the [email or identification features] in

¹³⁶ *Am. Online, Inc. v. Nat’l Health Care Disc., Inc.*, 121 F. Supp. 2d 1255, 1273 (N.D. Iowa 2000).

¹³⁷ *Id.* (“For purposes of the CFAA, when someone sends an email 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.”).

¹³⁸ *See Hale, supra* note 35, at 545–46. Kern expands the notion of what qualifies as unauthorized access by proposing four tests for finding intentional unauthorized access. *See Kern, supra* note 41. These are (1) the express authorization test; (2) the subjective expectations test; (3) the reasonable expectations test; and (4) the express prohibition test. Kern, *supra* note 41, at 128–30. He bases the express authorization test on Congress’s statements during enactment of the CFAA noting that the CFAA provisions addressing unauthorized access apply to “outsiders,” while the provisions of the CFAA that apply to exceeding authorized access apply to insiders. *Id.* at 128–29. Based on this distinction, anyone who is not an insider (i.e., having a prior relationship with the network operator) would lack express authorization and be presumed unauthorized.

The subjective expectations test stems from the decision in *Morris*. Under the subjective expectations test, access is “unauthorized if the computer accessed was used in a way that is not in any way related to its ‘intended function.’” *Id.* at 129.

The reasonable expectations test is derived from the district court’s decision in *EF Cultural Travel v. Zefer Corp.*, 318 F.3d 58 (1st Cir. 2003), *see infra* note 146 and accompanying text, and by the implicit analysis under the CFAA. This test first examines “the reasonable expectations of a network operator in determining whether access is unauthorized,” before turning to an examination of “the reasonable expectations of a user in determining whether the user intend[ed] to engage in unauthorized access.” *Id.* at 129–30 (notably, the appellate court in *EF Cultural Travel* rejected the first component of this test).

The express prohibition test comes from common law interpretation of trespass to chattels and from the appellate court in *EF Cultural Travel*. Under this test, access is unauthorized only if “a network operator has indicated that access is prohibited, in website terms of use, by enabling password protection or otherwise.” *Id.* at 130.

any way related to their *intended function*. . . . [I]nstead he found holes in both programs that permitted him a special and unauthorized access route into other computers.”¹³⁹ Essentially, the purpose of Morris’s actions supported the court’s determination that he engaged in unauthorized access. In *Register.com, Inc. v. Verio, Inc.*,¹⁴⁰ the court found that Verio’s use of automated software process (“robots”) to access and collect information from Register.com’s database constituted unauthorized access.¹⁴¹ The court used Verio’s means of access to justify its finding.¹⁴²

Other courts have based the determination of unauthorized access on evidence of a violation of the terms of service or terms of use. In *America Online, Inc. v. LCGM, Inc.*,¹⁴³ the court found unauthorized use as a result of the defendant’s violation of AOL’s Terms of Service.¹⁴⁴ Defendant LCGM maintained an AOL membership and used this membership to harvest the email addresses of other AOL members by means of extractor software programs. The court succinctly held that “[d]efendants’ actions violated AOL’s Terms of Service, and as such was [sic] unauthorized.”¹⁴⁵ At issue in *EF Cultural Travel BV v. Zefer Corp.*¹⁴⁶ was defendant’s use of a “scraper tool” to skim pricing information from a competing student travel business’s website.¹⁴⁷ The court noted that “[a] lack of authorization could be established by an explicit statement on the website restricting access,”¹⁴⁸ thus giving rise to an unauthorized access cause of action where users of a website violate the specified terms of use.

¹³⁹ *United States v. Morris*, 928 F.2d 504, 510 (2d Cir. 1991) (emphasis added).

¹⁴⁰ *Register.com, Inc. v. Verio, Inc.*, 126 F. Supp. 2d 238 (S.D.N.Y. 2000), *aff’d in part, rev’d in part*, 356 F.3d 393 (2d Cir. 2004).

¹⁴¹ *Id.* at 255. The court evaluated the nature of Verio’s access under a trespass to chattels perspective. *Id.* at 251. Although the court considered the nature of the robot’s conduct, ultimately the court resolved the question of unauthorized access based on notice; Register.com gave notice (in part by filing the lawsuit) that it objected to Verio’s use of the robots and because of this objection, the robots represent an unauthorized access. Still, the case illustrates that the means of access are subject to scrutiny in the court’s determination of access. Also of note, the Second Circuit overturned the preliminary injunction and found it unlikely that Register.com would be able to maintain its CFAA claim, based on lack of damages. *Register.com*, 356 F.3d at 439–40. However, the court upheld the trespass to chattels claim, the root of the district court’s unauthorized access analysis. *Id.* at 444.

¹⁴² *Id.* at 249–50.

¹⁴³ *Am. Online, Inc. v. LCGM, Inc.*, 46 F. Supp. 2d 444 (E.D. Va. 1998).

¹⁴⁴ *Id.* at 450.

¹⁴⁵ *Id.*

¹⁴⁶ *EF Cultural Travel BV v. Zefer Corp.*, 318 F.3d 58 (1st Cir. 2003).

¹⁴⁷ *Id.* at 60.

¹⁴⁸ *Id.* at 62. The court did register the concern that public policy might limit some of the restrictions placed on access. *Id.*

The *EF Cultural Travel* court raised the possibility that unauthorized access may be implicit. As previously stated, a website may restrict access by explicit statement. But the court went on to state that the “lack of authorization may be implicit, rather than explicit,” further stating that “[a]fter all, password protection itself normally limits authorization by implication (and technology), even without express terms.”¹⁴⁹ Just as courts interpret unauthorized access in a variety of ways, the scope of damage and loss vary between courts.

Courts have considered aspects of information sharing and damages in the context of the CFAA. Users must share information and/or cause damage to be liable under Sections 1030(a)(2) and/or 1030(a)(5)(A). Regarding information sharing, Congress noted that obtaining information in the context of the CFAA “includes mere observation of the data[.] [A]ctual asportation, in the sense of physically removing the dat[a] from its original location or transcribing the data, need not be proved in order to establish a violation of this subsection.”¹⁵⁰ Minimal case law addresses the specific meaning of the term “information,” but the issue has arisen, *inter alia*, in the context of medical information,¹⁵¹ Internet cookies,¹⁵² academic information,¹⁵³ and financial data.¹⁵⁴ Turning to damages, courts must make determinations of what exactly damage means and what constitutes loss.

In interpreting damage and loss, courts have interpreted the CFAA so as to accommodate a variety of network-related conduct. Courts have construed

¹⁴⁹ *Id.* at 63. The court discusses at length the “reasonable expectations” test used by the district court. Under this test, a lack of authorization can be inferred from the circumstances. The Second Circuit explicitly rejects this test, and in so doing states:

Our basis for this view is not, as some have urged, that there is a “presumption” of open access to Internet information. The CFAA, after all, is primarily a statute imposing limits on access and enhancing control by information providers. Instead, we think that the public website provider can easily spell out explicitly what is forbidden and, consonantly, that nothing justifies putting users at the mercy of a highly imprecise, litigation-spawning standard like “reasonable expectations.”

Id. at 63.

¹⁵⁰ S. REP. NO. 104-357, at 7 (1996) (citing S. REP. NO. 99-432, at 6–7 (1986)).

¹⁵¹ *Doe v. Datmouth-Hitchcock Med. Ctr.*, No. 00-100-M, 2001 U.S. Dist. LEXIS 10704, at *8–9 (D. N.H. July 19, 2001); *see also* *Physicians Interactive v. Lathian Sys. Inc.*, CA-03-1193-A, 2003 U.S. Dist. LEXIS 22868, at *15–20 (E.D. Va. Dec 5, 2003).

¹⁵² *In re DoubleClick, Inc. Privacy Litigation*, 154 F. Supp. 2d 497, 524–25 (S.D.N.Y. 2001).

¹⁵³ *Role Models Am., Inc. v. Jones*, 305 F. Supp. 2d 564, 566–68 (D. Md. 2004) (granting the motion to dismiss the CFAA claim based on lack of unauthorized access).

¹⁵⁴ *Charles Schwab & Co. v. Carter, et. al.*, No. 04 C 7071, 2005 U.S. Dist. LEXIS 21348, at *25–27 (N.D. Ill. Sept. 27, 2005).

the statutory definition of damages¹⁵⁵ broadly to encompass network slowdowns and diminished network capacity.¹⁵⁶ The CFAA also defines loss,¹⁵⁷ but courts vary in their interpretation of the scope of this definition. Generally, courts have found loss compensable only when it “result[s] from

¹⁵⁵ 18 U.S.C. § 1030(e)(8) (Supp. III 2003) (“any impairment to the integrity or availability of data, a program, a system, or information.”). The court in *America Online, Inc. v. Nat’l Health Care Disc. Inc.*, 121 F. Supp. 2d 1255 (N.D. Iowa 2000), looked to the dictionary to determine the meaning of the critical terms of the statutory definition, defining the terms as follows:

Impairment: something that damages or makes worse by diminishing in some material respect.

Integrity: Unimpaired, sound, complete, without corruption.

Availability: The state of being present or ready for immediate use; accessible.

Data: Information output that must be processed to be meaningful; information in numerical form that can be transmitted or processed digitally.

Program: A sequence of coded instructions that can be inserted into a computer, causing it to perform a particular function.

System: “[A] regularly interacting or interdependent group of items forming a unified whole . . . [such as] a group of devices or artificial objects . . . forming a network”

Information: Knowledge obtained from investigation, study, or instruction; facts, data; “a signal or character (as in a communication system or computer) representing data.”

Am. Online, Inc. v. Nat’l Health Care Disc., Inc., 121 F. Supp. 2d 1255, 1274 (N.D. Iowa 2000) (citations omitted). The court went on to construe the definition as encompassing slowdowns caused by email spam.

¹⁵⁶ *Id.* at 1274 n.18 (N.D. Iowa 2000) (“[P]hysical damage [is] not restricted to the physical destruction or harm of computer circuitry but includes loss of access, loss of use, and loss of functionality.”) (quoting *American Guarantee & Liab. Ins. Co. v. Ingram Micro, Inc.*, No. 99–185 TUC ACM, 2000 U.S. Dist. LEXIS 7299, at *6–8 (D. Ariz. Apr. 19, 2000)). The claim in *American Guarantee* did not arise under the CFAA, but the *National Health Care Discount* court still found the interpretation of damages noteworthy, specifically citing dicta that “[l]awmakers around the country have determined that when a computer’s data is unavailable, there is damage; when a computer’s services are interrupted, there is damage; and when a computer’s software or network is altered, there is damage.” *Id.*

¹⁵⁷ 18 U.S.C. § 1030(e)(11) (Supp. III 2003) (“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”).

damage to, or the inoperability of, the accessed computer system.”¹⁵⁸ Some courts have been unwilling to compensate for loss apart from the offending unauthorized access, such as lost profits, devaluation of database information, lost business opportunities, or money spent investigating the violation.¹⁵⁹ However, other courts have used the CFAA’s reference to economic damages¹⁶⁰ to construe damages more broadly.¹⁶¹ The *Creative Computing* court went so far as to allow recovery for lost profits and business goodwill.¹⁶² Regardless of how the term is defined, in considering loss, the CFAA expressly empowers the court to aggregate the loss a plaintiff suffers due to the conduct of the offending party to achieve the statutory minimum of \$5,000.¹⁶³

2. Unauthorized Access Under the CFAA

In light of the statute and precedent, liability for open wireless access under the CFAA depends on determinations of (1) intent, (2) access and authorization, and (3) information sharing or damages. If construed liberally,

¹⁵⁸ *Civic Ctr. Motors, Ltd. v. Mason St. Imp. Cars, Ltd.*, 387 F. Supp. 2d 378, 381 (S.D.N.Y. 2005) (referencing *Nexans Wires S.A. v. Sark-USA Inc.*, 319 F. Supp. 2d 468, 474 (S.D.N.Y. 2004)); *Register.com, Inc. v. Verio, Inc.* 126 F. Supp. 2d 238, 252 (S.D.N.Y. 2004); *see also* *Creative Computing v. Getloaded.com, L.L.C.* 386 F.3d 930, 936 (9th Cir. 2004) (“Damages are indeed limited to those caused by the impairment, which may not be the same thing as the expenses of the victim subsequent to the impairment.”).

¹⁵⁹ *Civic Ctr. Motors*, 387 F. Supp. 2d at 381–82; *see also* *Tyco Int’l (U.S.) Inc. v. Doe*, No. 01 Civ. 3856 (RCC) (DF), 2003 U.S. Dist. LEXIS 11800, at *4–5 (S.D.N.Y. July 11, 2003) (“While . . . the CFAA allows recovery for losses beyond mere physical damage to property, the additional types of damages awarded by courts under the Act have generally been limited to those costs necessary to assess the damage caused to the plaintiff’s computer system or to resecure the system in the wake of a hacking attack.”); *Nexans Wires*, 319 F. Supp. 2d at 477 (“[P]laintiffs’ lost revenue due to lost business opportunity does not constitute ‘loss’ under the statute.”).

¹⁶⁰ The economic damages language applies in the civil context. In a civil action, damages for a violation involving Section 1030(a)(5)(B)(i) are limited to economic damages. 18 U.S.C. § 1030(g) (Supp. III 2003).

¹⁶¹ *E.g.*, *Creative Computing v. Getloaded.com, L.L.C.*, 386 F.3d 930, 936 (9th Cir. 2004).

¹⁶² *Id.* at 935. The court went on to state that “[w]hen an individual or firm’s money or property are impaired in value, or money or property is lost, or money must be spent to restore or maintain some aspect of a business affected by a violation, those are ‘economic damages.’” *Id.* In making this statement, the court turned to the Black’s Law Dictionary definition of consequential economic losses, which included lost profits and the loss of goodwill or reputation. *Id.* at 935 n.19 (citing BLACK’S LAW DICTIONARY 552 (8th ed. 2004)).

¹⁶³ 18 U.S.C. § 1030(a)(5)(B)(i) (Supp. III 2003).

these provisions may encompass open wireless access. However, given the high damage threshold and ambiguity surrounding authorization, open wireless access likely escapes the CFAA's reach.¹⁶⁴

a. *Favoring Liability Under the CFAA*

For users to be liable for unauthorized access, they must have the requisite criminal intent under the statute. The CFAA requires intentional conduct on the part of the user.¹⁶⁵ Under *Morris*, the intentional mens rea applies to the “‘accesses’ phrase” of the statute, and not to the “‘damages’” phrase.¹⁶⁶ Although the term “access” is undefined, some courts have broadly construed it in a manner that could encompass conduct such as a computer communicating to another computer via a wireless network.¹⁶⁷ After clearing the intent and access hurdles, users’ open wireless conduct must be without authorization for liability to attach.

Unauthorized access under the CFAA may be established by a terms of service violation or implicitly. Most ISPs restrict their subscribers from redistributing networking/Internet services.¹⁶⁸ Although these terms of service expressly apply to the subscriber, they may impact other users as well. Users engaging in open Wi-Fi access participate in conduct that

¹⁶⁴ *But see* Kerr, *supra* note 66, at 1598–99. Kerr notes a trend in civil cases interpreting the CFAA that leads him to posit that “any computer use that violates an implicit or explicit contract with the computer’s owner exceeds the authorization that the owner has granted the user, and therefore violates the federal unauthorized access statute.” *Id.*

¹⁶⁵ 18 U.S.C. §§ 1030(a)(2), 1030(a)(5)(A)(ii) (2000 & Supp. III 2003).

¹⁶⁶ *United States v. Morris*, 928 F.2d 504, 509 (2d Cir. 1991). *But see, supra* notes 132–34 and accompanying text, discussing whether the intentional mens rea applies solely to “access” or to “unauthorized access” and the implications thereof.

¹⁶⁷ *See Am. Online, Inc. v. Nat’l Health Care Disc., Inc.*, 121 F. Supp. 2d 1255, 1272–73 (N.D. Iowa 2000); *see also* Hunter, *supra* note 61, at 477 (“[B]ecause of the technical requirements of the Internet’s fundamental transmission protocol, TCP/IP, which relays messages through many computers before they reach their final destination, the person initiating the transmission actually accesses each computer in the transmission chain.”).

¹⁶⁸ *See* Time Warner Cable Residential Services Subscriber Agreement, at § 4(b), http://help.twcable.com/html/twc_sub_agreement2.html (last visited Aug. 16, 2006) (“I will not resell or redistribute (whether for a fee or otherwise) the Services, or any portion thereof, or charge others to use the Services, or any portion thereof.”); SBC Yahoo! Terms of Service, at § 14, <http://sbc.yahoo.com/terms/> (last visited Aug. 16, 2006) (“You agree that the Service is not to be used to trunk or facilitate public internet access (‘Hotspots’) or any other Public Use of the Service, except for FreedomLink.”). However, not all ISPs share this view; Speakeasy explicitly allows for wireless sharing. *See* Speakeasy WiFi NetShare Service, <http://www.speakeasy.net/netshare/terms/#Wi-Fipolicy> (last visited Aug. 16, 2006).

violates the terms of service. This violation may be sufficient to establish that the users' access is without authorization.¹⁶⁹ Unauthorized access may also be found implicitly by extending the court's reasoning in *EF Cultural Travel*.¹⁷⁰ The *EF Cultural Travel* court noted that the "lack of authorization may be implicit, rather than explicit" and rejected "that there is a 'presumption' of open access to Internet information."¹⁷¹ Taken together, one may argue for a presumption of unauthorized access, rendering users' access to an open wireless network unauthorized without express or implicit authorization.¹⁷² Once unauthorized access is established, the analysis shifts to obtaining information and damages.

Damages present a significant challenge to liability for open Wi-Fi access under the CFAA. The CFAA requires users who gain unauthorized access to obtain information¹⁷³ and/or have their conduct result in damage that causes at least a \$5,000 loss.¹⁷⁴ The broad language of section 1030(a)(2) likely encompasses standard communications that occur between computers on a network (i.e., routing information, IP addresses, trading data packets, etc.).¹⁷⁵ Damages may include harm to the functionality of a

¹⁶⁹ *Am. Online, Inc. v. LCGM, Inc.*, 46 F. Supp. 2d 444, 450–51 (E.D. Va. 1998); see also Kerr, *supra* note 66, at 1637–41. Kerr notes that precedent established in civil cases that addresses authorization in the breach of contract context have provided prosecutors with a "broad and powerful tool" to attack unauthorized access conduct. *Id.* at 1640; see also Hale, *supra* note 35, at 548 ("With regard to finding unauthorized access through a 'Terms of Service' violation, the AOL cases . . . provide precedent for enforcing such terms on third parties with no privity of contract and no notice of the terms.").

¹⁷⁰ *EF Cultural Travel BV v. Zefer Corp.*, 318 F.3d 58, 63 (1st Cir. 2003).

¹⁷¹ *Id.* at 63.

¹⁷² See Hale, *supra* note 35, at 548 ("The line of reasoning in [*EF Cultural Travel BV v.*] Zefer further supports this view to the extent that the end user remains 'unauthorized' by default, absent some explicit or implicit agreement."); see also *Physicians Interactive v. Lathian Sys. Inc.*, CA-03-1193-A, 2003 U.S. Dist LEXIS 22868, at *20 (E.D. Va. Dec. 5, 2003) (calling defendant's argument that a website with no posted limits on access is open to Internet users for all purposes 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.").

¹⁷³ 18 U.S.C. § 1030(a)(2) (2000).

¹⁷⁴ 18 U.S.C. § 1030(a)(5)(B)(i) (Supp. III 2003).

¹⁷⁵ See Hale, *supra* note 35, at 548 ("[A]ccess to any WLAN involves some exchange of information that typically passes between computers (IP addresses, data packets, etc.) as a means of gaining access to the Internet."); Kern, *supra* note 41, at 135 ("The language of Section 1030(A)(2) [sic] is broad enough to suggest that, by accessing routing and addressing information, a roaming Wi-Fi user 'obtains information' for purposes of the statute.").

network, such as slowdowns or diminished capacity.¹⁷⁶ Users who access an open wireless network are likely to cause a slowdown (albeit a small one) of the network, causing “damage.” This damage must cause aggregate loss of at least \$5,000.¹⁷⁷ Admittedly, users who access open wireless networks for the purpose of email or web browsing are unlikely to meet the statutory amount because their activity uses so little bandwidth.¹⁷⁸ However, users who repeatedly engage in heavy bandwidth network activity over a long period of time, such as downloading movies or other large files, may cause sufficient loss to rise to the level of liability under the statute.¹⁷⁹ This may be particularly likely in circumstances where the WLAN provider incurs expenses investigating and securing access.¹⁸⁰ Further, if the WLAN provider makes use of the network in a business context, aggregate loss may include economic losses caused by network slowdowns and push the amount past the statutory threshold.¹⁸¹

In theory, users who engage in open wireless access violate the CFAA. They engage in intentional access. This access is unauthorized because it may violate the terms of service governing the WAP or violate the presumption that uninvited access is unauthorized. Standard network communications between computers establish information sharing sufficient for liability under Section 1030(a)(2). The damage caused by users’ slowdown and capacity diminishing conduct could potentially create an aggregate loss in excess of \$5,000, establishing liability under Section 1030(a)(5)(A)(iii). However, this outlook broadly construes the terms of the CFAA; under a narrower construction, the CFAA will likely not apply to open wireless access.

¹⁷⁶ *Am. Online, Inc. v. Nat’l Health Care Disc., Inc.*, 121 F. Supp. 2d 1255, 1274 n.18 (N.D. Iowa 2000).

¹⁷⁷ 18 U.S.C. § 1030(B)(i) (Supp. III 2003).

¹⁷⁸ Bandwidth usage is difficult to quantify. A fairly common measure for the cost to an ISP of delivering email is \$.001 per email. *Earthlink, Inc. v. Carmack*, No. 1:02-CV-3041-TWT, 2003 U.S. Dist. LEXIS 9963, at *15 (N.D. Ga. May 7, 2003). By analogy, the cost to WLAN operators of email traffic would seem low.

¹⁷⁹ One article estimates that downloading a complete ninety to one hundred twenty minute movie can consume bandwidth equivalent to sending more than one hundred fifty thousand emails. Freshnews.com, *Websense Helps Organizations Cool Down Bandwidth Loss and Illegal File Sharing*, Aug 16, 2004, http://www.freshnews.com/news/computers-internet/article_18971.html?Websense (last visited Aug. 16, 2004).

¹⁸⁰ See 18 U.S.C. § 1030(e)(11) (Supp. III 2003); *Civic Ctr. Motors, Ltd. v. Mason St. Imp. Cars, Ltd.*, 387 F. Supp. 2d 378, 381–82 (S.D.N.Y. 2005).

¹⁸¹ See *Creative Computing v. Getloaded.com, L.L.C.*, 386 F.3d 930, 935 (9th Cir. 2004). The court permits loss of goodwill and loss of business amongst the aggregate economic damage.

b. *Against Liability Under the CFAA*

The intent requirement of the CFAA may be construed in a manner that makes liability for open wireless access more difficult to achieve. As stated in *Morris*, the intent mens rea applies to the “‘accesses’ phrase.”¹⁸² By using the word “phrase,” the *Morris* court’s interpretation of the mens rea requirement could apply to “access a protected computer without authorization.” If the intent requirement applies to the whole “access” phrase, the prosecutor or plaintiff must prove that a defendant not only intended to access, but also intended to access without authorization. This heightened mens rea requirement could limit the applicability of the CFAA to open wireless access due to the difficulty of proving intent to engage in unauthorized conduct.¹⁸³ Even assuming that intent is established, unauthorized access presents problems in the context of wireless networking.

Taking an intended function (i.e., means or purpose) approach to unauthorized access may preclude liability under the CFAA. Critical to the *Morris* court’s determination of unauthorized access was the fact that the defendant did not use email capabilities “in any way related to their intended function.”¹⁸⁴ Applied to wireless, users who access an open wireless network are using the network for its intended function, and thus, their access would be authorized. Additionally, open wireless access may be authorized unless it is expressly prohibited by the network operator.¹⁸⁵ Both these perspectives support the contention that open wireless access may be conduct allowed by the CFAA. In the event that unauthorized access is found, users are not likely to have obtained information or caused sufficient loss to trigger the statute.

Simply accessing a wireless network should not subject a user to liability. The legislative history of the 1996 amendment to the CFAA indicates that “the term ‘obtaining information’ includes merely reading it.”¹⁸⁶ This indicates that the lower threshold of “information” under the CFAA is defined as something readable, with the implication of being readable to a person (not a computer). Unless users view content from

¹⁸² *United States v. Morris*, 928 F.2d 504, 509 (2d Cir. 1991).

¹⁸³ This issue obviously hinges significantly on the interpretation of unauthorized access. In the case of Wi-Fi, if merely accessing a Wi-Fi network is considered unauthorized, then the intent requirement’s application to “without authorization” is effectively irrelevant, as simple access would meet the requisite level of intent. However, if authorization depends on more than mere access, then the breadth of the intent mens rea takes on greater importance.

¹⁸⁴ *Morris*, 928 F.2d at 510.

¹⁸⁵ *EF Cultural Travel BV v. Zefer Corp.*, 318 F.3d 58, 63 (1st Cir. 2003) (“[W]e think that the public website provider can easily spell out explicitly what is forbidden . . .”).

¹⁸⁶ S. REP. NO. 104-357, at 7 (1996).

another computer, they do not obtain information as contemplated by Congress. Further, the exchange of networking protocols inherent to access does not rise to the level of obtaining information because it involves no “readable” information—users do not “read” the information exchanged.

Users accessing an open wireless network will not likely cause sufficient loss to satisfy the terms of the CFAA. Although damages may include network slowdowns, the aggregated loss from these slowdowns probably would not amount to a figure approaching the \$5,000 required by statute. Even in the case of heavy bandwidth users, evidentiary problems would likely be prohibitive; wireless providers, particularly non-business providers, would have difficulty establishing the loss caused by diminished network capacity.

Users who engage in open wireless access are unlikely to be liable under the CFAA.¹⁸⁷ The primary difficulties lie with authorization, obtaining information, and/or loss. Courts must take a narrow view of authorization to deem access of an open network unauthorized. Even if unauthorized, users who access open wireless networks for “typical” internet conduct (email, web browsing, etc.) would be hard pressed to satisfy the requirement for obtaining information or meet the \$5,000 threshold for loss caused by their damaging access. Despite the CFAA, liability may still arise under state law.

¹⁸⁷ It does not appear that CFAA claims are common in instances of unauthorized access. One exception is the case of Stefan Puffer. Puffer worked as a computer security analyst for the Central Technology Department of Harris County (Houston), Texas. Rosanna Ruiz, *Computer Expert Indicted in Alleged Hacking*, HOUSTON CHRON., July 25, 2002, at 26A. Puffer provided a demonstration to a county official and newspaper reporter about the ease of access to the county district clerk’s wireless network. *Id.* Prosecutors indicted Puffer on a charge that he violated the CFAA, alleging that the \$5,000 damage requirement of the statute was met by the financial costs of staffing changes implemented to determine the nature of the intrusion and prevent future wireless break-ins. Rosanna Ruiz, *Federal Trial Starts for Man Who Hacked County Computer*, HOUSTON CHRON., Feb. 19, 2003, at 16A. The jury acquitted Puffer in fifteen minutes, with one juror stating “[w]e didn’t feel he intentionally wanted to do damage, but just to embarrass [the county].” Rosanna Ruiz, *Jurors Acquit Man of Hacking System at District Clerk’s Office*, HOUSTON CHRON., Feb. 21, 2003, at 26A. Despite the lack of conviction, federal officials remained adamant about the viability of a CFAA claim, with the U.S. Attorney on the case stating that “[t]he allegation is that this man intentionally invaded a cyberspace that did not belong to him” and that “[w]e should not allow that intrusion in our homes, and we can’t allow it to systems so critical to (daily) operations.” *Id.*

B. State Statutory Law

The varying terms of state statutes addressing open wireless access make determining whether this conduct gives rise to liability challenging.¹⁸⁸ Some statutes evidence language that would clearly encompass open wireless access whereas others would prohibit extending liability to this conduct. In between is a gray area where the exact application of the statute is unclear. Unfortunately, case law has done little to illuminate the proper application of these statutes.

1. Case Interpretation

In contrast to the CFAA, courts have rarely had the occasion to consider state statutory law in the area of unauthorized access.¹⁸⁹ The cases that have

¹⁸⁸ States may further complicate matters by pursuing a conviction for open wireless access conduct based on traditional theft or trespass statutes. In the state of Washington, police arrested a man for repeatedly using a coffee shop's wireless Internet service. Stephanie Rice, *Accused Wi-Fi Thief Pleads to Trespass*, COLUMBIAN, Aug. 16, 2006, at A1. Alexander Smith would park outside the coffee shop, then access the Internet via his laptop. *Id.* The coffee shop provided the Internet service for customers, but Mr. Smith did not make a purchase and refused the shop's repeated requests that he leave the area. *Id.* Although Washington has a computer trespass statute, Mr. Smith ultimately pled guilty to criminal trespass, a different statute within the criminal code. *Id.*; see WASH. REV. CODE § 9A.52.120 (2006) (Washington's computer trespass statute); WASH. REV. CODE § 9A.52.080 (2006) (Washington's criminal trespass statute). Commenting on the case, the Clark County Deputy Prosecutor noted that "[t]he law hasn't caught up with the idea of stealing Internet service." *Id.*

¹⁸⁹ The weight of a state statute depends heavily on the interpretation and application of these terms. Unfortunately, this is largely a theoretical exercise as only a minimum of cases have explored these statutes and have not necessarily done so in a manner that provides much guidance. See *People v. Lawton*, 56 Cal. Rptr. 2d 521, 523 (Cal. App. Dep't Super. Ct. 1996) (interpreting the unauthorized access provision of California's computer crime statute); *Wesley Coll. v. Pitts*, 974 F. Supp. 375, 391–92 (D. Del. 1997) (construing Delaware's unauthorized access statute); *Gallagher v. State*, 618 So.2d 757, 757 n.58 (Ct. App. Fla. 1993) (Glickstein, C.J., dissenting) (discussing unauthorized access under Florida law delineating offenses against computer users); *Fugarino v. State*, 531 S.E.2d 187, 187–89 (Ga. Ct. App. 2000) (construing Georgia's computer trespass statute); *State v. Hargrove*, 67 P.3d 111, 114 (Idaho Ct. App. 2003) (overturning conviction under Idaho unauthorized access law); *State v. Rupnick*, 125 P.3d 541, 556 (Kan. 2005) (upholding validity of Kansas computer trespass statute); *State v. Allen*, 917 P.2d 848 (Kan. 1996) (*discussed infra* notes 190–98 and accompanying text); *Commonwealth v. Cocke*, 58 S.W.3d 891, 894 (Ky. Ct. App. 2001) (declaring first degree unlawful access void for vagueness); *Commonwealth v. Farley*, No. 95-934, 1996 Mass. Super. LEXIS 410, at *13–14 (Super. Ct. Mass. Oct. 18, 1996) (upholding constitutionality of unauthorized access statute); *People v. Schilke*, No. 253117, 2005 Mich. App. LEXIS 1079, at *8–9 (Mich. Ct. App. May 3, 2005) (affirming conviction

considered these laws have done so mostly in the context of defining the scope of access.

In *State v. Allen*,¹⁹⁰ the Kansas Supreme Court set forth the notion that access means interaction with a computer beyond merely potentially logging in. Allen used his computer to dial Southwestern Bell computer modems; the company believed this act would lead to Allen acquiring the ability to make free long distance telephone calls.¹⁹¹ Upon dial-up, Allen faced a prompt requiring him to enter a username and password. However, the evidence indicated that Allen never attempted to respond to the prompt.¹⁹² Considering this evidence, the court held that Allen never accessed the Southwestern Bell computers.¹⁹³

The *Allen* Court interpreted access to mean something more than making contact with a computer. The State argued that Allen's conduct fell within the meaning of "to approach," which was part of the statutory definition of "access."¹⁹⁴ In considering the competing arguments, the court first turned to a National Institute of Justice manual containing the comment that "[t]he use of the word 'approach' in the definition of 'access,' if taken literally, could mean that any unauthorized physical proximity to a computer could

under Michigan unauthorized access statute); *People v. Helleman*, No. 217190, 1999 Mich. App. LEXIS 2325 (Mich. Ct. App. Sept. 10, 1999) (discussing intentional unauthorized access); *State v. Gaikwad*, 793 A.2d 39 (N.J. Super. Ct. App. Div. 2002) (discussing intentional unauthorized access); *People v. Angeles*, 180 Misc. 2d 146, 149 (N.Y. Crim. Ct. 1999) (granting defendant's motion to dismiss for failure of the prosecution to state in the charge that the computer was protected, an element of the offense); *People v. Johnson*, 148 Misc. 2d 103, 112 (N.Y. Crim. Ct. 1990) (denying defendant's motion to dismiss unauthorized use charge); *State v. Burrell*, No. 76890, 2000 Ohio App. LEXIS 4169, at *20–21 (Ohio Ct. App. Sept. 14, 2000) (evidence insufficient to support unauthorized access conviction); *State v. Washington*, 710 N.E.2d 307, 320 (Ohio Ct. App. 1998) (upholding conviction under unauthorized use statute); *State v. Lebron*, 646 N.E.2d 481, 484–85 (Ohio Ct. App. 1994) (upholding conviction under unauthorized use statute); *State v. Schwartz*, 21 P.3d 1128, 1138 (Or. Ct. App. 2001) (affirming conviction for unauthorized access under state computer crime law); *Commonwealth v. McFadden*, 850 A.2d 1290, 1294 (Pa. Super. Ct. 2004) (upholding sentence imposed for violation of unauthorized use statute); *Superior Court Chain Store Maint. v. Nat'l Glass & Gate Serv., Inc.*, No. PB 01-3522, 2004 R.I. Super. LEXIS 81, at *31–36 (R.I. Super. Ct. Apr. 21, 2004) (discussing authorization); *see also Kerr, supra* note 66, at 1617 n.86 and surrounding text.

¹⁹⁰ *State v. Allen*, 917 P.2d 848 (Kan. 1996).

¹⁹¹ *Id.* at 850.

¹⁹² *Id.*

¹⁹³ *Id.* at 853. The *Allen* Court evaluated unauthorized access in the context of a felony, thus requiring damage done to the system. However, Kansas provides for misdemeanor unauthorized access, an offense that does not contain damage as an element.

¹⁹⁴ *Id.* at 852.

constitute a crime.”¹⁹⁵ Next, the court looked to Webster’s Dictionary, which defined “access” as the “freedom or ability to obtain or make use of.”¹⁹⁶ Minding the words of the National Institute of Justice and the dictionary, the *Allen* court found that because Allen did not “proceed[] beyond the initial banner and enter[] appropriate passwords, he could not be said to have had the ability to make use of Southwestern Bell’s computers.”¹⁹⁷ While the *Allen* Court was unwilling to allow the definition of access to encompass approach,¹⁹⁸ another state court did not feel so constrained.

In *State v. Riley*,¹⁹⁹ the Washington Supreme Court found that approach represents a viable form of access. The *Riley* Court faced similar facts as in *Allen*; the defendant used a computer to repeatedly dial the general access number of a telephone company and input a random six digit number in attempt to acquire long distance telephone services.²⁰⁰ The Washington computer trespass statute defined access as “to approach . . . or otherwise make use of any resources of a computer, directly or by electronic means.”²⁰¹ The court held that *Riley*’s conduct satisfied the statutory definition; *Riley*’s approach and entry of the random number constituted approach, and thus, access.²⁰²

In contrast to access, few courts have addressed what constitutes authorization. This lack of clarity is further compounded by the fact that few states define what constitutes authorization.²⁰³ The states that do provide a

¹⁹⁵ *Allen*, 917 P.2d at 852 (quoting DONN B. PARKER, NATIONAL INSTITUTE OF JUSTICE, COMPUTER CRIME: CRIMINAL JUSTICE RESOURCE MANUAL 84 (2d ed. 1989)).

¹⁹⁶ *Allen*, 917 P.2d at 853 (quoting WEBSTER’S NEW COLLEGIATE DICTIONARY 7 (1977)).

¹⁹⁷ *Allen*, 917 P. 2d at 853.

¹⁹⁸ See Kerr, *supra* note 66, at 1624–26. Kerr describes the *Allen* Court as adopting a “virtual reality” approach, whereby Allen must have gotten inside the computer for his conduct to be considered access. *Id.*

¹⁹⁹ *State v. Riley*, 846 P.2d 1365 (Wash. 1993) (en banc).

²⁰⁰ *Id.* at 1367–68. It is unclear on the facts whether *Riley* in fact obtained valid access codes that would have enabled him to procure free long distance services.

²⁰¹ *Id.* at 1373 (quoting WASH. REV. CODE § 9A.52.010(6) (West Supp. 2006)).

²⁰² *Riley*, 846 P.2d at 1373.

²⁰³ COLO. REV. STAT. § 18-5.5-101(1) (2005); GA. CODE ANN. § 16-9-92(18) (Lexis Supp. 2006); HAW. REV. STAT. §§ 708-890 (Supp. 2005); ME. REV. STAT. ANN. tit. 17-A, § 431(11) (2006); MINN. STAT. § 609.87 Subd. 2a (2003); N.H. REV. STAT. ANN. § 638:16(II) (West Supp. 2005); N.J. STAT. ANN. § 2C:20-23(q) (2005); N.C. GEN. STAT. § 14-453(1a) (2005); R.I. GEN. LAWS § 11-52-1(15)(v) (2002); S.C. CODE ANN. § 16-16-10(l) (West Supp. 2005); TENN. CODE ANN. § 39-14-601(2) (2003); UTAH CODE ANN. § 76-6-702(2) (Lexis Supp. 2006); VA. CODE ANN. § 18.2-152.2 (Lexis Supp. 2005); W. VA. CODE § 61-3C-3(b) (2005). In the absence of a definition, at least one court has turned to Black’s Law Dictionary and Webster’s Dictionary for guidance. See *Briggs v. State*, 704 A.2d 904, 909 (Md. 1998).

statutory definition vary regarding the conduct encompassed by the term. At one extreme, authorization requires the express consent of the owner.²⁰⁴ At the other extreme are statutes that define authorization under a reasonableness standard²⁰⁵ or based on implied consent.²⁰⁶ Somewhere in the middle are statutes that define authorization generically in terms of consent or permission.²⁰⁷ Unfortunately, state case law does little to clarify the meaning of authorization. The small number of state cases that have addressed authorization have arisen primarily in the context of employee misconduct.²⁰⁸

²⁰⁴ See, e.g., Colorado, which defines authorization as “the express consent of a person . . . to use said person’s . . . computer network.” COLO. REV. STAT. § 18-5.5-101(1) (2005).

²⁰⁵ While New Jersey defines authorization as permission, authority or consent, the statute goes on to provide that “[a]n actor has authorization if a reasonable person would believe that the act was authorized.” N.J. STAT. ANN. § 2C:20-23(q) (2005).

²⁰⁶ See, e.g., South Carolina, which provides that “[u]nauthorized access’ means access of a . . . computer network not explicitly or implicitly authorized by the appropriate principal.” S.C. CODE ANN. § 16-16-10(1) (West Supp. 2005). Tennessee provides perhaps the broadest definition, stating that “[a]uthorization’ means any and all forms of consent, including both implicit and explicit consent.” TENN. CODE ANN. § 39-14-601(2) (2003).

²⁰⁷ See, e.g., Maine, which states that “[u]nauthorized’ mean[s] not having consent or permission of the owner.” ME. REV. STAT. ANN. tit. 17-A, § 431(11) (2006). These definitions offer little clarity to the meaning of authorization, as they turn on the interpretations of permission and consent, which are themselves undefined terms. Minnesota provides an exception to this vagary; while the statute defines authorization as permission, it goes on to state that “[a]uthorization may be limited by the owner by: (1) giving the user actual notice orally or in writing; (2) posting a written notice in a prominent location adjacent to the computer being used; or (3) using a notice displayed on or announced by the computer being used.” MINN. STAT. § 609.87 Subd. 2a (2003). The last two options illustrate the conundrum presented by Wi-Fi; wireless networking changes the location dynamic such that posting or displaying notice by a computer becomes impractical.

²⁰⁸ See *Fugarino v. State*, 531 S.E.2d 187, 189 (Ga. Ct. App. 2000) (holding that Fugarino lacked the authority to delete portions of a company’s computer program, as indicated by the testimony of the company’s owner that no such permission was granted and by the “vindictive and retaliatory manner” of Fugarino’s conduct); *State v. Olson*, 735 P.2d 1362, 1365–66 (Wash. Ct. App. 1987) (holding that police officer’s access of police database for personal use was not without authority; permission to use the database was not predicated on the uses made of the data; thus while against departmental policy, police officer still had authority to access); *Briggs v. State*, 704 A.2d 904, 909–10 (Md. 1998) (holding that a system administrator had authority to access computer; thus, while his conduct was inappropriate, he had the authority to engage in it) (noting also that Briggs likely exceeded the scope of his authority, but the Maryland statute prohibits only unauthorized access, not access outside the scope of authority); see also Kerr, *supra* note 66, at 1632–37.

2. Statutes Supporting Liability for Open Wireless Access

The statutes that provide the clearest indication of liability for open wireless access premise authorization on express consent. Colorado's statute prohibits the knowing access of any computer network without authorization.²⁰⁹ The statute goes on to define "authorization" solely in terms of "express consent."²¹⁰ California's computer crimes statute targets the knowing access of a computer network without permission.²¹¹ One commentator has indicated that the California Attorney General's Office would consider access to be "without permission" if absent express permission.²¹²

These statutes could give rise to liability for open wireless access. Users of an open wireless network do not obtain the express consent of the networks' operators. Absent express consent, the users do not have the authorization to use the wireless networks. Their lack of authorization or permission makes the users liable for their open wireless access.

3. Statutes Limiting Liability for Open Wireless Access

In contrast to Colorado and California, some state statutes indicate that open wireless access is permissible absent particular conduct by network operators. New York provides the strongest example of limiting the liability of open wireless access. New York's unauthorized use statute prohibits the knowing use of a computer without authorization, but additionally requires that "the computer utilized is 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."²¹³ Thus, open wireless access would only be

²⁰⁹ COLO. REV. STAT. § 18-5.5-102 (2005).

²¹⁰ COLO. REV. STAT. § 18-5.5-101(1) (West Supp. 2006). Other statutes use the "express consent" language, but typically provide for the option of implied consent as well.

²¹¹ CAL. PENAL CODE § 502(c)(7) (West Supp. 2006).

²¹² Kern, *supra* note 41, at 151 n.156 and accompanying text (citing a June 2004 telephone interview with the California Deputy Attorney General).

²¹³ N.Y. PENAL LAW § 156.05 (1999). The force of the statute was reaffirmed in *People v. Angeles*, 180 Misc. 2d 146, 148-49 (N.Y. Crim. Ct. 1999), where the court stated:

The statute, however, on its face does not make criminal the mere use or accessing of a computer system without permission or authority. The Legislature has imposed the additional requirement that the computer be "*equipped or programmed with any device or coding system, a function of which is to prevent the unauthorized use of [the] computer or computer system.*" The legislative history of the statute makes clear that this requirement was included on the ground that "[s]uch protective devices

actionable under this statute if the network operator has enabled encryption or password protection on the network, and users usurped this protection.

While New York explicitly requires security protection, other states imply a connection between authorization and password protection or notice. In prohibiting knowing access without authorization, Massachusetts also states that “[t]he requirement of a password or other authentication to gain access shall constitute notice that access is limited to authorized users.”²¹⁴ Minnesota defines authorization to include options whereby the owner of a computer network can limit authorization by: “(1) giving the user actual notice orally or in writing; (2) posting a written notice in a prominent location adjacent to the computer being used; or (3) using a notice displayed on or announced by the computer being used.”²¹⁵ By creating a presumption that a use is unauthorized if security or notice is provided, these statutes also create an implication that silence does not necessarily constitute a lack of authorization.²¹⁶ An open wireless network by definition is not protected by security measures. Thus, users accessing an open wireless network may be considered authorized in the absence of security or notice. While construction of these statutes requires interpreting the silence of the statute, other states provide less guidance regarding open access conduct.

4. *Statutes Inconclusive on Liability for Open Wireless Access*

It is unclear how a number of state statutes apply to open wireless access, mostly because of questions of what constitutes unauthorized access. Some states provide a reasonableness standard, others speak of implicit consent, and still more provide no guidance at all regarding authorization.

Some states permit access if users reasonably believed their access was authorized. For example, New Hampshire provides an affirmative defense to an unauthorized access prosecution whereby the accused may show that “[t]he person reasonably believed that the owner of the . . . computer network . . . had authorized him or her to access; or . . . [t]he person reasonably could not have known that his or her access was unauthorized.”²¹⁷

provide the first line of defense against unauthorized intrusion into a computer system.”

Id. at 148–49 (emphasis original) (citations omitted).

²¹⁴ MASS. GEN. LAWS Ch. 266, § 120F (2002).

²¹⁵ MINN. STAT. 609.87 subd. 2a (2003).

²¹⁶ Kern, *supra* note 41, at 144–45 (“These statutes do not have an equivalent 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.”).

²¹⁷ N.H. REV. STAT. ANN. § 638:17(I)(a)–(c) (West Supp. 2005); *See* OHIO REV. CODE ANN. § 2913.04(D) citing § 2913.03(C)(1) (West 2006) (providing an affirmative defense to unauthorized access, as empowered by Section 2913.04, where “[a]t the time

This standard cuts both ways in terms of liability. On one hand, users may not be able to ascertain information regarding the open wireless network they are accessing, and thus, could not reasonably know whether their access is authorized. On the other hand, if users are outside the range of any familiar networks, the logical assumption is that the network is under another operator's control, and the inquiry turns to whether it is reasonable that the operator would authorize access to the network by design or mistake.

Other states provide an equally ambiguous standard by allowing for implied consent. South Carolina defines "unauthorized access" as access of a computer network "not explicitly or implicitly authorized" by the network operator.²¹⁸ Permitting implied consent may limit the applicability of state statutes to open wireless access. This depends on the presumption of whether a network left unsecured is impliedly open. If this presumption is valid, an open network indicates implied consent on behalf of the network operator for users to access his or her network. If this presumption is invalid, liability may still attach for access conduct.

Even more states are silent as to what represents unauthorized access. The majority of state statutes merely prohibit unauthorized access; they do not specify what the term "unauthorized access" means.²¹⁹ The lack of statutory guidance and the lack of case law addressing the authorization issue leaves users to their own devices to try and determine whether accessing an open wireless network constitutes criminal conduct under state law.

While the aforementioned sections focus on the statutory construction of unauthorized access, damages also factor heavily into the liability equation. Several states do not require that users who commit unauthorized access cause any damage.²²⁰ In essence, these states criminalize the mere act of unauthorized access, which broadens the scope of liability under these states' laws.²²¹ Other states provide different tiers of damages tied to offense levels. Any statute that introduces a monetary damage component raises problems of proof because of the difficulty associated with demonstrating (1) the

of the alleged offense, the actor, though mistaken, reasonably believed that the actor was authorized to use or operate the property").

²¹⁸ S.C. CODE ANN. § 16-16-10(l) (West Supp. 2005); *see also* W. VA. CODE § 61-3C-3(b)(2005) ("Authorization" means the express or implied consent given by a person to another to access that person's computer network.).

²¹⁹ *See supra* note 99, identifying the states that define "authorization."

²²⁰ Of the states that do require the unauthorized access to cause damage, the threshold amount of loss is relatively low. Thus, in general, the inquiry into damages is less germane to the question of liability for unauthorized access under state law as opposed to liability under the CFAA.

²²¹ By strictly criminalizing the act of unauthorized access, these statutes extend liability beyond the scope of the CFAA and many state statutes, all of which require damage.

damage caused by the unauthorized access, and (2) the loss caused by the damage. Liability under state law varies greatly based on the differing state statutes. Liability under the common law suffers a similar fate based on the scope that courts choose to give the doctrine of trespass to chattels.

C. The Doctrine of Trespass to Chattels

The scope and applicability of this common law doctrine depends largely on matters of judicial interpretation. Courts have varied the scope of the trespass to chattels doctrine. In some jurisdictions, the doctrine expansively applies to a variety of Internet related conduct. Other jurisdictions limit the scope of trespass to chattels to tangible items. Courts' construction of the trespass to chattels doctrine may be determinative of liability for open wireless access.

1. Case Interpretation

Courts have interpreted the trespass to chattels doctrine in a manner that accommodates a variety of Internet related issues. In *Register.com v. Verio*, the court upheld a preliminary injunction premised on a trespass to chattels claim regarding Verio's use of search robots.²²² Other courts have found that trespass to chattels in "computer space" may exist where defendants caused misdirected emails to be sent—conduct that was outside the scope of the terms and conditions that bound the defendants.²²³ Several cases have arisen in the context of email spam²²⁴ and spyware (or similar information gathering software).²²⁵ One court has even specified the exact elements of a claim in this area. The court held that to maintain a trespass claim premised

²²² *Register.com, Inc. v. Verio*, 356 F.3d 393, 404–05 (2d Cir. 2004).

²²³ *Hotmail Corp. v. Van \$ Money Pie, Inc.*, No. C98-20064, 1998 U.S. Dist. LEXIS 10729, at *19–20 (N.D. Cal. Apr. 16, 1998) (using the language "trespassed on Hotmail's computer space," one of the first acknowledgements that the trespass doctrine may be construed to encompass electronic conduct).

²²⁴ *CompuServe, Inc. v. Cyber Promotions, Inc.*, 962 F. Supp. 1015, 1027 (S.D. Ohio 1997) ("Defendants' intentional use of plaintiff's proprietary computer equipment . . . is an actionable trespass to plaintiff's chattel."); *Am. Online v. IMS*, 24 F. Supp. 2d 548, 550–51 (E.D. Va. 1998) (granting summary judgment to AOL on trespass to chattels claim); *Am. Online, Inc. v. LCGM*, 46 F. Supp. 2d 444, 451–52 (E.D. Va. 1998) ("Courts have recognized that the transmission of unsolicited bulk e-mails can constitute a trespass to chattels."); *Am. Online, Inc. v. National Health Care Disc., Inc.*, 121 F. Supp. 2d 1255, 1277 (N.D. Iowa 2000).

²²⁵ *Sotelo v. DirectRevenue, L.L.C.*, 384 F. Supp. 2d 1219, 1229–33 (N.D. Ill. 2005); *Southwest Airlines v. Farechase, Co.*, 318 F. Supp. 2d 435, 442 (N.D. Tex. 2004); *eBay, Inc. v. Bidder's Edge*, 100 F. Supp. 2d 1058 (N.D. Cal. 2000); *Register.com*, 356 F.3d at 404.

on unauthorized access to a computer system, “the plaintiff must establish: (1) defendant intentionally and without authorization interfered with plaintiff’s possessory interest in the computer system; and (2) defendant’s unauthorized use proximately resulted in damage to plaintiff.”²²⁶ In contrast, some courts have expressly rejected the application of trespass to chattels to Internet issues.

State and federal courts have noted limits on the application of the doctrine of trespass to chattels to electronic communication. In *Intel v. Hamidi*, the court found that “under California law [trespass to chattels] does not encompass, and should not be extended to encompass, an electronic communication that neither damages the recipient computer system nor impairs its functioning.”²²⁷ Hamidi sent emails critical of Intel’s employment practices to other employees via the company’s email system.²²⁸ The California Supreme Court noted that the emails “caused neither physical damage nor functional disruption” but rather “caused discussion among employees and managers.”²²⁹ Intel asserted damages in the form of the loss of productivity as a result of the employee discussions. The court rejected these consequential economic damages as an actionable injury to the company’s interest in its computers. Notably, the court explicitly stated that email is not necessarily exempt from ordinary tort liability, referencing the harmful effects of large quantities of spam on a computer system’s functioning.²³⁰

A federal district court in Tennessee construing Florida law further limited the doctrine of trespass to chattels to movable personal property.²³¹ In *Partsbases*, the court considered allegations that the defendant trespassed by hacking into Partsbases’s database and accessing customer information. While the court noted that other jurisdictions have allowed actions for trespass to electronic resources under a trespass to chattels theory, Florida does not allow the doctrine to be characterized in such a manner. Citing a Florida appellate court case rejecting classifying a bank account as a chattel, the *Partsbases* court noted that in Florida, “an action for trespass to chattels must involve movable personal property.”²³² The database at issue in the case did not constitute movable property, and because Florida “does not recognize a

²²⁶ *Bidder’s Edge*, 100 F. Supp. 2d at 1069–70.

²²⁷ *Intel Corp. v. Hamidi*, 71 P.3d 296, 300 (Cal. 2003).

²²⁸ *Id.* at 299.

²²⁹ *Id.*

²³⁰ *Id.* at 300.

²³¹ *Inventory Locator Serv., L.L.C. v. Partsbases, Inc.*, No. 02-2695, 2005 U.S. Dist. LEXIS 32680, at *34–37 (W.D. Tenn. Sept. 6, 2005).

²³² *Id.* at *35.

cause of action for trespass to chattels in cyberspace[,]" the court dismissed the common law trespass count in the case.²³³

Damages present a difficult issue in a court's application of trespass to chattels to Internet related conduct. While courts may issue an injunction premised merely on the trespass,²³⁴ for the doctrine to be actionable, a plaintiff must demonstrate damage. In *CompuServe v. Cyberpromotions*, the court discussed the nature of actionable damages, focusing on the harm to the personal property or diminution of its quality, condition, or value as a result of defendant's use as a predicate for liability.²³⁵ *CompuServe* involved spam, and the court found that spam diminished the value of CompuServe's equipment by occupying disk space and draining processing power. The *Bidder's Edge* court used similar reasoning, finding the potential for damage in the defendant's admittedly small use of plaintiff eBay's computer system.²³⁶ In upholding the preliminary injunction against Bidder's Edge, the Court stated that

it is undisputed that eBay's server and its capacity are personal property, and that BE's searches use a portion of this property. Even if, as BE argues, its searches use only a small amount of eBay's computer system capacity, BE has nonetheless deprived eBay of the ability to use that portion of its personal property for its own purposes. The law recognizes no such right to use another's personal property.²³⁷

²³³ *Id.* at *36.

²³⁴ See *Register.com, Inc. v. Verio, Inc.*, 356 F.3d 393, 404-5 (2d Cir. 2004); *Physicians Interactive v. Lathian Systems, Inc.*, No. CA-03-1193-A, 2003 U.S. Dist. LEXIS 22868, at *26-27 (E.D. Va. Dec. 5, 2003).

²³⁵ *CompuServe, Inc. v. Cyber Promotions, Inc.*, 962 F. Supp. 1015, 1022 (S.D. Ohio 1997) (citing RESTATEMENT (SECOND) OF TORTS § 218(b) (1965)). The court went on to quote the comments to section 218, stating:

An unprivileged use or other intermeddling with a chattel which results in actual impairment of its physical condition, quality or value to the possessor makes the actor liable for the loss thus caused. In the great majority of cases, the actor's intermeddling with the chattel impairs the value of it to the possessor, as distinguished from the mere affront to his dignity as possessor, only by some impairment of the physical condition of the chattel. There may, however, be situations in which the value to the owner of a particular type of chattel may be impaired by dealing with it in a manner that does not affect its physical condition In such a case, the intermeddling is actionable even though the physical condition of the chattel is not impaired.

RESTATEMENT (SECOND) OF TORTS § 218 cmt. h (1965).

²³⁶ *eBay, Inc. v. Bidder's Edge, Inc.*, 100 F. Supp. 2d 1058, 1071 (N.D. Cal. 2000).

²³⁷ *Id.* at 1072; see also *Oyster Software, Inc. v. Forms Processing, Inc.*, No. C-00-0724, 2001 U.S. Dist. LEXIS 22520, at *35-41 (N.D. Cal. Dec. 6, 2001).

In contrast to *CompuServe* and *Bidder's Edge*, other courts have found that a negligible amount of computer use does not constitute sufficient damage to render a trespass claim actionable. In *Ticketmaster v. Tickets.com*, the court rejected a preliminary injunction barring defendant's use of a robot web crawler (similar to that used by the defendant in *Bidder's Edge*) because the defendant's use of plaintiff's system was "very small" and did not "interfere[] to any extent with the regular business" of plaintiff.²³⁸

2. Liability Under the Doctrine of Trespass to Chattels

Liability under a trespass to chattels theory depends on how liberally the doctrine is applied. Some courts have shown a willingness to extend the doctrine to encompass Internet conduct, while others have been reluctant to permit that far a reach. Even amongst those courts that have extended the doctrine, questions still arise regarding what constitutes sufficient damage to render a trespass to chattels claim actionable.

The doctrine of trespass to chattels may apply to Internet conduct. One court delineated the elements for an unauthorized access based trespass to chattels claim, stating that a plaintiff must establish that "(1) defendant intentionally and without authorization interfered with plaintiff's possessory interest in the computer system; and (2) defendant's unauthorized use proximately resulted in damage to plaintiff."²³⁹ Applied to open wireless access, users' access without authorization²⁴⁰ may interfere with the plaintiff network operator's wireless network in a manner sufficient to satisfy the first element. Turning to damages, courts have found that draining processing power or diminishing system capacity, even in small amounts, may satisfy the damage requirement under a trespass to chattels claim.²⁴¹ This view of damages seems to encompass the potentially minimal amount of bandwidth loss and system strain caused by the typical users of open wireless networks.

In contrast, different courts' interpretations of the doctrine support the contention that trespass to chattels does not apply to open wireless access. A Tennessee court limited the doctrine of trespass to chattels to movable property.²⁴² Under this view, unauthorized access of a network does not

²³⁸ *Ticketmaster Corp. v. Tickets.com, Inc.*, No. CV99-7654-HLH, 2000 U.S. Dist. LEXIS 12987, at *17 (C.D. Cal. Aug. 10, 2000).

²³⁹ *Bidder's Edge*, 100 F. Supp. 2d at 1069-70.

²⁴⁰ The issue of unauthorized access is discussed at length in the previous two sections. For the sake of brevity, the debate will not be rehashed in this Section.

²⁴¹ *CompuServe, Inc., v. Cyber Promotions, Inc.*, 962 F. Supp. 1015, 1023 (S.D. Ohio 1997); *see also Bidder's Edge*, 100 F. Supp. 2d at 1071.

²⁴² *Inventory Locator Serv., L.L.C. v. Partsbase, Inc.*, No. 02-2695, 2005 U.S. Dist. LEXIS 32680, at *34-37 (W.D. Tenn. Sept. 6, 2005).

involve movable property, thus precluding the applicability of the doctrine. Even if the doctrine does apply, damages present an additional, potentially insurmountable, hurdle. Some courts have been unwilling to apply trespass to chattels where the conduct at issue causes no damage or impairment to the system.²⁴³ Users of open wireless networks may cause only negligible impairment to the system, and thus not meet the required level of damages to sustain a trespass to chattels claim.

Even in the event the doctrine does apply, users may be able to escape liability by asserting apparent consent. Users may argue that the lack of encryption, password protection, or other security measures on a wireless network grants them the apparent consent to access the open network. Apparent consent operates under a reasonableness standard.²⁴⁴ It seems reasonable that if users' laptops detect wireless signals that allow them to connect, the network operator consents to their access.²⁴⁵

Federal law, state law, and the common law provide a myriad of relevant legal regimes. Unfortunately, the variances between the substance and application of these laws confuse the issue of the legality of open Wi-Fi access and leave results unpredictable. How the law treats open wireless networks has far-reaching policy and societal implications and deserves measured consideration.

VII. A WAY OF MAKING SENSE OF OPEN WI-FI ACCESS

Examining the case of Benjamin Smith, the most compelling question is not whether his conduct violates the law, but whether it *should* violate the law—should the law prohibit casual users from accessing open Wi-Fi networks? This Part addresses the policy behind unauthorized access law and makes a proposal for the construction of a statute regulating unauthorized access.

²⁴³ Intel Corp. v. Hamidi, 71 P.3d 296, 300 (Cal. 2003); *see also Ticketmaster*, 2000 U.S. Dist. LEXIS 12987, at *17.

²⁴⁴ RESTATEMENT (SECOND) OF TORTS § 892 cmt. c (1979).

²⁴⁵ Of course, one can reasonably argue the other side: just because network operators leave their WLANs unsecured does not mean they consent to users accessing their networks.

A. The Wi-Fi Policy Debate: Property, Radio, or Somewhere in Between

Behind the legal debate over the legality of accessing open wireless networks are competing conceptualizations of the nature of the technology at issue. Wi-Fi networks allow widespread public access to the Internet with minimal physical limitations. Wireless networking technology continually evolves; now consumers can use simple add-ons to expand the range of wireless networks to upward of fifty miles.²⁴⁶ Access to a wireless network may be provided by any number of sources, from residential consumers to businesses. This free availability mirrors the public availability of websites on the Internet.²⁴⁷ However, consumers who deploy Wi-Fi networks may still intend for some aspects of the network to remain private. This represents the conundrum of Wi-Fi authorization and access: consumers make Wi-Fi networks publicly available, but do not necessarily want other users to have unfettered access to the network.

Open wireless technology can be conceptualized by the use of two competing analogies: property rights and radio signals. Wireless networks may be viewed as an extension of the network operator's property, with unauthorized access of the network concomitantly viewed as theft or trespass.²⁴⁸ Alternatively, an open wireless network may be viewed as a radio signal, where access of the network is implicitly authorized (and therefore legal) by the public broadcast of the signal. Each of these conceptualizations reflects differing views regarding rights of use and access and has important economic and public policy implications.²⁴⁹

²⁴⁶ See Hines, *supra* note 43 (“A signal enhancer available at your local RadioShack can give someone access from as far as 50 miles away.”).

²⁴⁷ See Kern, *supra* note 41, at 124.

²⁴⁸ “This is very similar to you walking down the street where a store has apples and oranges, and you grab one and keep going.” Jay Lyman, *Floridian Faces Wireless Trespassing Charges*, TECH NEWS WORLD, July 8, 2005, <http://www.technewsworld.com/story/44501.html>. (quoting Roger Entner, Vice President of Wireless Telecom at Ovum. Mr. Entner goes on to note the proliferation of unauthorized wireless access (and how it may result in the increased cost of bandwidth for all network users) before concluding that “[j]ust because it’s happening, and I think it’s happening frequently, doesn’t make it right.”) *Id.*

²⁴⁹ There is a robust debate in the literature regarding cyberproperty and spectrum regulation. See *infra* notes 250–57. This Section endeavors only to briefly explain these competing conceptualizations and their policy and economic impact; a thorough analysis or comprehensive theory of the Internet is outside the scope of this Note.

The root of the “cyberspace as place”²⁵⁰ concept lies in metaphor and user experience—popular culture refers to the Internet in spatial terms and users often engage in conduct online (such as online shopping) that creates the sensation of entering or using a physical space.²⁵¹ Existing solely as a theoretical notion, the idea of cyberspace as a place has little practical impact, but in many cases courts have seized this concept and in a sense transformed the place metaphor from a descriptive tool to a guiding rule.²⁵² Using the place metaphor, courts may evaluate cyberspace claims in a manner analogous to property²⁵³—a potentially harmful approach in the area of Wi-Fi.

Defining open wireless networks in terms of property rights may lead to a policy of closed access and result in economic inefficiencies. If courts conceive of cyberspace as a place, their logical response would be to construct a regulatory structure analogous to that which regulates real property.²⁵⁴ This would in essence confer a proprietary right to the owners of

²⁵⁰ The concept of “cyberspace as place” has been addressed by a number of commentators. See Hunter, *supra* note 61; Mark A. Lemley, *Place and Cyberspace*, 91 CAL. L. REV. 521 (2003); Patricia L. Bellia, *Defending Cyberproperty*, 79 N.Y.U. L. REV. 2164 (2004); LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 63–84 (1999) [hereinafter CODE AND OTHER LAWS OF CYBERSPACE]; David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367 (1996); Lawrence Lessig, *The Zones of Cyberspace*, 48 STAN. L. REV. 1403 (1996) [hereinafter *The Zones of Cyberspace*]; James Boyle, *A Theory of Law and Information: Copyright, Spleens, Blackmail, and Insider Trading*, 80 CAL. L. REV. 1413 (1992). Interestingly, the term “cyberspace” borrows from the world of fiction, with the term first espoused by William Gibson in his 1984 novel NEUROMANCER. See VINCENT MOSCO, THE DIGITAL SUBLIME: MYTH, POWER, AND CYBERSPACE 11 (2004).

²⁵¹ See Lemley, *supra* note 250, at 523; Hunter, *supra* note 61, at 446; Lessig, *supra* note 250, at 1403 (“Cyberspace is a place. People live there. They experience all the sorts of things that they experience in real space, there.”).

²⁵² See Hunter, *supra* note 61, at 472–500; Lemley, *supra* note 250, at 527–29. Certainly, courts must apply physical-world laws to the Internet, however, problems may arise when courts extend the property conception of the Internet without limitation. See *id.* at 542.

²⁵³ *Id.*

²⁵⁴ See Hunter, *supra* note 61, at 503:

If we think of cyberspace as a place, then the legal response would be to impose a real-property-based regulatory structure on the place. Moreover, because our physical world property system is based on private land tenure, the legal reaction is to use real-property mechanisms to delineate and fence off these new property entitlements in cyberspace.

For insight into the Department of Justice’s perspective, see Richard W. Downing, *Shoring Up the Weakest Link: What Lawmakers Around the World Need to Consider in Developing Comprehensive Laws to Combat Cybercrime*, 43 COLUM. J. TRANSNAT’L L. 705, 711–12 (2005) (discussing an approach to legislating cybercrime, including

wireless networks; accessing such networks, even if open, would be the equivalent of walking on to that particular owner's lawn. As the law discourages such conduct in the real world, open access would be discouraged in the cyberspace world. The fragmentation of wireless networks caused by conferring property rights on network operators leads to economic inefficiency. Free and open access of the Internet enhances the Internet's value.²⁵⁵

At its onset, the Internet embodied several attributes characteristically associated with commons.²⁵⁶ However, propertization that allows network operators to limit access may act as an enclosure on the Internet commons. Granting propriety rights in wireless networks may create a tragedy of the anticommons, thereby excluding users from access of the Internet and preventing users from realizing the benefits that the Internet brings to society.²⁵⁷ In contrast, the radio signal conceptualization of wireless networks mitigates the economically inefficient splintering caused by courts' adopting the property-based conceptualization.

The radio conceptualization of Wi-Fi supports the notion of free access for open wireless networks. WLAN operators must set up a WAP, essentially a small radio tower, with which they broadcast the wireless signal over a publicly available radio spectrum.²⁵⁸ Wi-Fi's use of unlicensed radio

unauthorized access, that involves creating consistency between conduct criminalized in the physical world and conduct criminalized in the virtual world).

²⁵⁵ See LAWRENCE LESSIG, *THE FUTURE OF IDEAS* 171 (2001) [hereinafter *THE FUTURE OF IDEAS*] ("It is this general feature [free and open access] 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.").

²⁵⁶ Hunter, *supra* note 61, at 503.

²⁵⁷ See *id.* at 509 ("Anticommons property exists where multiple owners have a right to exclude others from a scarce resource, and no one has an effective privilege of use."). Not all commentators agree about the viability of rejecting a property-based regime for regulating access on the Internet, with one commentator noting the gaps in the position taken by critics of the property rule approach. See Bellia, *supra* note 250, at 2209–10 ("[A]rguments based on 'overpropertization' of informational goods or of the Internet fail to explain why the law nonetheless should protect against uses that cause physical harm to a computer system; [or] why, if the law does protect against such physical harm, it should not also protect against economic harms.").

²⁵⁸ See *supra* Part II. A rich scholarly debate exists over the proper regulation of spectrum, typically positioning a property based regime against a commons approach. See Stuart Minor Benjamin, *Spectrum Abundance and the Choice Between Private and Public Control*, 78 N.Y.U. L. REV. 2007 (2003); Kevin Werbach, *Supercommons: Toward a Unified Theory of Wireless Communication*, 82 TEX. L. REV. 863 (2004); Yochai Benkler, *Some Economics of Wireless Communications*, 16 HARV. J.L. & TECH. 25 (2002); Patrick S. Ryan, *Wireless Communications and Computing at a Crossroads: New Paradigms and Their Impact on Theories Governing the Public's Right to Spectrum*

frequencies provides the impetus for the radio conceptualization of wireless networking. This notion of Wi-Fi functions as a foil to the property conceptualization. Rather than distributing private rights in networking that would restrict public access, publicly broadcasted (and hence publicly available) networks presumptively grant open access to all. This open access paradigm embodies a commons approach to wireless networking that better reflects the characteristics of the Internet and may help realize higher network optimization and generate other positive economic outcomes.

A commons policy for WLANs increases network productivity and produces positive externalities. Commons may be defined as a “situation in which a resource is openly accessible to all users regardless of the users’ identity or intended use of the resource.”²⁵⁹ Applied to Wi-Fi, open wireless networks would be available for unfettered public access. For networking, open access correlates with increased network productivity. Metcalfe’s law holds that the value of a network increases exponentially with the incorporation of additional interconnections to the network.²⁶⁰ Allocating WLANs as a common resource would introduce more interconnections into the Internet network and correspondingly the value of the network would increase exponentially.²⁶¹ Further, maintaining open access reflects a policy toward favoring technological innovation.²⁶² Cumulatively, these benefits illustrate the positive economic effects of a commons approach to Wi-Fi.

Wireless networking presents the opportunity for a comedy of the commons, whereby open access correlates to greater social value. The comedy of the commons functions as the opposite of the tragedy of the commons,²⁶³ and “arises where open access to a resource leads to scale

Access, 3 J. TELECOMM. & HIGH TECH. L. 239 (2005); Thomas W. Hazlett, *Spectrum Tragedies*, 22 YALE J. ON REG. 242 (2005). Given that Wi-Fi uses radio frequencies that are unlicensed by the FCC, this Note avoids entering the debate over the proper regulation of radio spectrum and instead focuses on the commons-like attributes of unlicensed radio frequencies.

²⁵⁹ Brett M. Frischmann, *An Economic Theory of Infrastructure and Commons Management*, 89 MINN. L. REV. 917, 933 (2005) (citing THE FUTURE OF IDEAS, *supra* note 255, at 19–20).

²⁶⁰ See GILDER, *supra* note 25, at 73.

²⁶¹ Aside from social value, a technological gain may also be realized due to the nature of computer networks. Networking protocols enable interconnection, interoperability, and data transfer, all of which may be made more efficient by an increased number of participating computers in a network. Frischmann, *supra* note 259, at 928.

²⁶² THE FUTURE OF IDEAS, *supra* note 255, at 264–68.

²⁶³ The tragedy of the commons, popularly introduced by Garrett Hardin, holds that open access to a common resource ultimately leads to degradation of the resource because the resource users’ individual gains in using the resource will always exceed the distributed cost to all of the deprivation of the resource. Garrett Hardin, *The Tragedy of*

returns—greater social value with greater use of the resource.”²⁶⁴ As mentioned above, adding users to a network enhances the social and technological value of the network. These positive externalities serve as the foundation for the comedy of the commons and illustrate the potential positive economic effects of open access under a radio conceptualization of Wi-Fi.²⁶⁵

Reconciling the potential economic benefits of open access with the individual right to enjoy one’s property requires consideration not only of the conceptualization of Wi-Fi technology, but the stakeholders involved in wireless networking. The property and radio conceptualizations serve as useful tools in evaluating the nature of Wi-Fi technology, but do not fully capture the range of interests that come to bear on the issue. Owners and operators of WAPs typically must contract with ISPs in order to obtain service. In turn, ISPs often set terms and conditions governing the end-users’ Internet usage—a contractual relationship indicative of ISPs’ stake in Wi-Fi policy. Hardware manufacturers have a stake by providing the equipment necessary to enable wireless networking. At an even broader level, telecommunications companies provide the foundation for Internet usage by providing the broadband pipes used by computers to communicate.²⁶⁶ The

the Commons, SCIENCE, Dec. 13, 1968, at 1243–48, available at <http://www.sciencemag.org/cgi/reprint/162/3859/1243.pdf>.

²⁶⁴ Frischmann, *supra* note 259, at 928 (citing Carol M. Rose, *The Comedy of the Commons: Custom, Commerce, and Inherently Public Property*, 53 U. CHI. L. REV. 711 (1986)).

²⁶⁵ Countervailing opinions exist over whether open access in fact leads to a tragedy of the commons as opposed to a comedy of the commons. Generally, these commentators assert that increased usage decreases the availability of bandwidth, which negatively impacts the experience of all network users. See Brett Frischmann, *Privitization and Commercialization of the Internet Infrastructure: Rethinking Market Intervention into Government and Government Intervention into the Market*, 2 COLUM. SCI. & TECH. L. REV. 1, 27 (2000/2001) (“Internet infrastructure consumption is often nonrivalrous; for example, during off-peak hours. . . . At some threshold, determined in terms of aggregate capacity being used, however, nonrivalrous consumption turns rivalrous and congestion problems arise.”); see also Benjamin, *supra* note 258, at 2015.

²⁶⁶ The dynamic between broadband carriers and content providers may shift in a manner impacting end-users of the Internet. In an interview with *BusinessWeek*, SBC CEO Edward Whitacre fired a shot across the bow to content providers, stating:

How do you think they're going to get to customers? Through a broadband pipe. Cable companies have them. We have them. Now what they would like to do is use my pipes free, but I ain't going to let them do that because we have spent this capital and we have to have a return on it. So there's going to have to be some mechanism for these people who use these pipes to pay for the portion they're using. Why should they be allowed to use my pipes? The Internet can't be free in that sense, because we and the cable companies have made an investment and for a

nature of Wi-Fi technology and the number of stakeholders relevant to Wi-Fi policy raise challenges to legislation addressing the legality of open wireless access.

Sensible Wi-Fi policy requires balancing individual and societal benefits while considering the range of interested parties. The property and radio conceptualizations serve as the ends to a continuum of conduct; the critical question is at what point on this continuum does open wireless access fall? The stronger argument lies on the side of open access akin to the radio conceptualization. Open access results in greater economic and social benefits. However, access cannot be completely unfettered. Under the right circumstances, stakeholders in WLANs should be able to assert property-like control over their network. One way to reconcile the competing interests and players in the Wi-Fi policy arena is to establish a regime of presumptive open access, a method illustrated by the following proposed statute.

B. A Model Unauthorized Access Statute and Analysis

The proposed statute is intended as a model rule regarding unauthorized access. As with the Model Penal Code, the aim of the statute is adoption by the states (though the principles embodied in the statute could perhaps be incorporated into federal law).²⁶⁷ The argument for statutory uniformity cuts

Google or Yahoo! or Vonage or anybody to expect to use these pipes for free is nuts!

Patricia O'Connell, ed., *At SBC, It's All About "Scale and Scope,"* BUS.WK. ONLINE, Nov. 7, 2005, http://www.businessweek.com/@n34h*IUQu7KtOwgA/magazine/content/05_45/b3958092.htm.

²⁶⁷ Although the CFAA may regulate open wireless access conduct, states may be better positioned to address this conduct than the federal government. Regulating unauthorized access via state law more adequately reflects the distribution of power between the federal and state government—specifically, the Constitution's grant to the states of the police power. *See* ERWIN CHERMERINSKY, CONSTITUTIONAL LAW: PRINCIPLES AND POLICIES 230 (2d ed. 2002) (“[A] key difference between federal and state governments is that only the latter possess the police power.”).

Certainly one can make the argument that the vast expanse of the Internet better comports with federal regulation via the Commerce Clause. However, state regulation seems more apt to particular instances of unauthorized access contained wholly within a particular state's jurisdiction. Further, joyriding seems outside the purpose of the CFAA. *See Doe v. Dartmouth-Hitchcock Med. Ctr.*, No. 00-100-M, 2001 U.S. Dist. LEXIS 10704, at *13 (D.N.H. July 19, 2001) (“[T]he CFAA's unequivocal purpose is to deter and punish those who intentionally access computer files and systems without authority and cause harm.”) (citations omitted).

However, the FBI has at least hinted at the possibility that the CFAA may be interpreted otherwise. In a widely circulated email, an FBI agent from Pittsburgh stated that: “Identifying the presence of a wireless network may not be a criminal violation,

against trespass to chattels as a viable means for asserting liability for open wireless access. Providing uniform statutes would give a clear indication of permissible conduct, in contrast to trespass to chattels, a doctrine that courts may apply in an inconsistent, confusing, and potentially outcome determinative fashion.²⁶⁸ Uniform statutes mitigate user confusion and focus liability on the conduct at issue rather than the jurisdiction in which it takes place.

The model statute covers a range of conduct, with a primary focus on the character of authorization. The most notable feature of the statute is what it *does not* regulate—under the model statute, users may engage in open wireless access without fear of legal repercussions.

1. *The Model Statute*

§ 100.1 Definitions

(1) “Access” means to gain entry to, instruct, intercept, store data in, retrieve data from, communicate with or otherwise make use of, any resources of a computer, computer network, or computer system.

(2) “Authorization” means the express or implied consent of the principal. Consent may be expressly granted or denied by giving verbal or written notice, including posting or displaying notice electronically. In the context of computer networking, the implementation of security measures indicates a denial of consent, unless the principal otherwise grants express consent, and in the absence of security measures, there exists a rebuttable presumption of implied consent regardless of whether express consent has been granted. This presumption may be overcome by clear and convincing evidence that shows no reasonable user would believe he or she would have authorization.

(3) “Computer” means an electronic, magnetic, optical, electromagnetic, or other data processing device, which performs logical, arithmetic, memory, or storage functions by the manipulations of electronic, magnetic, radio

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 Abuse Statute[.]” *War, Peace, or Stalemate*, *supra* note 32, at *44 (emphasis removed); *see also* Michael J. Madison, *Rights of Access and the Shape of the Internet*, 44 B.C. L. REV. 433, 480 (2003) (“Despite its anti-hacking origins, the CFAA, and subsections 1030(a)(2) and 1030(a)(5) in particular, appears on its face to justify interpreting the statute as an access-control regime . . .”).

²⁶⁸ Additionally, accepting trespass to chattels as applicable to WLANs has serious implications for the conception of wireless networking. Subjecting Wi-Fi to trespass to chattels implies a notion of cyberspace as property, a potentially dangerous and inaccurate conception with legal implications beyond the area of open wireless access.

wave, or light wave impulses, and includes all input, output, processing, storage, software, or communication facilities which are connected or related to or operating in conjunction with such a device.

(4) "Computer network" means the interconnection of communication lines (including microwave, radio wave, or other means of electronic communication) with a computer through remote terminals, or a complex consisting of two or more interconnected computers, or any system that provides communications between one or more computers or computer systems.

(5) "Computer system" means a set of interconnected computer equipment intended to operate as a cohesive system.

(6) "Damage" means any impairment to the integrity or availability of a computer, computer network, or computer system.

(7) "Loss" means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the computer, computer network, or computer system to its condition prior to the offenses, and any revenue lost, cost incurred, or other economic loss or consequential damage incurred because of the unauthorized access.

(8) "Person" means any individual, firm, corporation, educational institution, financial institution, governmental entity, or any legal or other entity.

(9) "Principal" means any person who is the owner, operator, manager, or otherwise responsible for a computer, computer network, or computer system.

(10) "Security measures" mean any device, coding system, encryption, password protection, or other means utilized to prevent a person from gaining access to a principal's computer, computer network, or computer system.

§ 100.2 Unauthorized Access

A person commits the crime of unauthorized access when he or she knowingly accesses a computer, computer network or computer system without the authorization of the principal of the computer, computer network or computer system.

§ 100.3 Offense Level and Civil Action

A person convicted of the crime of unauthorized access commits a felony offense. The offense level may be adjusted upward based on damage and/or loss caused by the unauthorized access. An individual subject to harm by the unauthorized access may bring a civil action under the laws of this state to compensate for the damage and/or loss caused by the unauthorized access.

§ 100.4 Conflict of Law

This section is in no way intended to abrogate an Internet Service Provider's rights under principles of state contract law.

2. Analysis

The operative provision of the statute, Section 100.2, contains standard language prohibiting unauthorized access. Most state statutes in some way, shape, or form, prohibit intentional, knowing, purposeful, and/or willful . . . access without authorization.²⁶⁹ This statute varies slightly from the language used by most states. For instance, it does not include the language “in excess of authorization,” found in many state statutes. Ultimately, this language is redundant; a principal's express consent would likely specify the terms of access, thus any access beyond those terms would inherently be “without authorization,” which is conduct already addressed by the statute. Additionally, because the model statute focuses on authorization and circumventing security, it does not criminalize attempted unauthorized access, as do some states. Lastly, the structure of the statute separates the “accesses” phrase and the “without authorization” phrase, which indicates that the mens rea applies only to the word “accesses” and not to “without authorization.”

The choice of a “knowing” mens rea reflects a decision to encompass a broad range of conduct. States effectively make a choice between an intentional/purposeful mens rea and a knowing mens rea.²⁷⁰ Under a purposeful mens rea, it must be the conscious object of a person to commit unauthorized access of the specific network in question. In contrast, with a knowing mens rea, a person need only be aware that the unauthorized access may result in the access of the specific network in question. This distinction is particularly significant in the wireless world, where multiple wireless networks may be available to a person at a given time. The intentional mens rea could limit a person's culpability to instances where he or she had the conscious object of accessing one specific wireless network among the many potentially available networks. This seems unduly limiting and could lead to an unjust result for network operators. The knowing mens rea leads to a more sensible result, whereby a person is still culpable if he or she is aware of the possibility of accessing one network among many. The choice of mens rea reflects a broader decision to encompass a broader range of conduct, with the true determining factor resting on authorization.

The definitions contained in Section 100.1 cover a range of access conduct and subject matter by diverse users. The defined terms of the statute

²⁶⁹ See *supra* Part IV.A.

²⁷⁰ See *supra* note 83.

borrow heavily from a variety of state statutes as well as the CFAA.²⁷¹ The terms “computer,” “computer network,” and “computer system,” encompass a range of electronic medium. Relevant to wireless, the term “computer network” includes “any system that provides communications between one or more computer or computer systems,” indicating that wireless networking falls within the scope of the statute. “Person” is liberally defined to include a range of users from individuals to corporate entities. The use of “principal” is intended to reflect the complexities of network administration. Many statutes define unauthorized access in terms of the “owner.” Although the owner can be easily discerned in the context of a residential network, corporate or small business networks present an additional problem. In these situations, the owner may have little or nothing to do with the actual network administration. The definition of “principal” allows for the possibility that other persons may be the appropriate source for consent to access. Just as the players (“person” and “principal”) and the parts (“computer,” “computer network,” and “computer system”) are broadly defined, so is the term that brings them together: “access.”

The term “access” includes an array of conduct while at the same time avoiding the pitfalls illuminated by a handful of state cases. The definition of “access” is intended to include any sort of communication or interaction with a computer. For wireless networking, the radio signal emitted by a WAP would constitute the resource of a computer network (if not an aspect of the network itself) and any interaction with that signal would constitute access. Notably, the definition does not include the term “to approach.” Including this term would create the same confusion dealt with by the courts in *State v. Allen* and *State v. Riley*.²⁷² Conduct that likely constitutes “to approach” would fall under “interaction.” But eliminating the term “to approach” from the definition shifts the interpretive focus from access to its rightful place: authorization.

Authorization is the key operative term of the statute; culpability only attaches in instances where a person does not have consent to access the

²⁷¹ The term “access” is a mix of language common to most statutes. *See* CAL. PENAL CODE § 502(b)(1) (West 1999); COLO. REV. STAT. § 18-5.5-101(10) (2004). “Computer” is provided as defined by Colorado (though other statutes contain similar language). *See* COLO. REV. STAT. § 18-5.5-101(2) (2004). The term “computer network” combines aspects of the language from Colorado and Florida. *See* COLO. REV. STAT. § 18-5.5-101(3) (2004); FLA. STAT. ANN. § 815.03(4) (West 2006). The definition of “computer system” is common to many states. *See* N.J. STAT. ANN. § 2C:20-23(g) (West 2005). The concept of a “principal” borrows from South Carolina, although that state’s code does not technically define the term. *See* S.C. CODE ANN. § 16-16-10(l) (West Supp. 2005). The CFAA also informs several terms, including “damage,” “loss,” and “person.” *See* 18 U.S.C. § 1030(e) (Supp. III 2003).

²⁷² *See supra* Part VI.B.1.

network.²⁷³ The definition provides for express or implied consent. Express consent can be given verbally (i.e., a principal informing a person he or she can use the principal's network) or by written notice. Express consent plays less of a role in the context of computer networking. This is designed to insulate against the potentially absurd results the use of notice might create in the wireless networking environment. For example, posting a sign prohibiting access seems impractical and ineffectual given that the range provided by a WAP would likely extend well past the immediate location where the sign is visible.²⁷⁴

Security measures play a critical role in determining liability in the computer networking environment. A principal's implementation of security measures functions as the principal's denial of consent. Specifically, if the principal makes use of any reasonable means²⁷⁵ to prevent a person from gaining access, the principal in essence establishes that such a person lacks authorization. This lack of authorization may of course be overcome by the express consent of the principal (i.e., the principal giving the person a password or network key to log on to a wireless network), but absent express consent, a person would lack authorization. Not only do security measures impact authorization when they are put in place, but they also have an effect when omitted as well.

The absence of security measures gives rise to implied consent, and hence, authorization. The definition of authorization provides that where a principal does not implement security measures, a person has implied consent that gives him or her authorization to access a computer network.²⁷⁶ Implied consent exists regardless of whether express consent has been granted. This implied consent is not absolute. Rather, the lack of security measures creates a rebuttable presumption that the principal has granted

²⁷³ In many ways this is a practical implementation of Kerr's views on unauthorized access statutes. *See* Kerr, *supra* note 66, at 1648 ("The functional effect of this broad construction [of access] is to eliminate access as a limit on the scope of unauthorized access statutes, and to place major weight on the meaning of authorization . . .").

²⁷⁴ The range of a wireless network can easily be extended to several miles beyond the exact location of the WAP. *See* Hines, *supra* note 43.

²⁷⁵ The reasonable means language is designed to include as of yet undeveloped security technologies that may apply in the future, while precluding individuals from claiming suspect security measures (for example, sitting on a porch chair with a bullhorn yelling at others to stay off your network).

²⁷⁶ The construction of this provision reflects the stance taken by New York. *See* N.Y. PENAL LAW § 156.05 (McKinney Supp. 2006). The model statute differs from New York in that it allows the principal to rebut (subject to a high evidentiary standard) the presumption created by a lack of security measures. This accommodates unique factual situations. Suppose a hack opened a normally secure state government network (the state treasury); the government would be allowed to present clear and convincing evidence that a person knew that he or she did not have authorization to be on the website.

implied consent. The principal may present clear and convincing evidence that shows no reasonable person would believe he or she had authorization to access. This approach contrasts with the handful of states that allow an affirmative defense whereby defendants may show that they reasonably believed they had authorization.²⁷⁷ The model statute changes two things: it (1) shifts the burden from the defendant to the plaintiff, and (2) heightens the evidentiary standard to clear and convincing evidence. These changes are indicative of a policy favoring open access in the absence of conduct to the contrary by the principal, and of encouraging network operators to implement security measures lest they face overcoming the high bar set by the clear and convincing standard.

The expansive definitions of parts, players, and access, in conjunction with the comprehensive definition of authorization, indicate an important policy decision: culpability should rest on whether the conduct at issue is authorized and not on the exact nature of the conduct itself. People, technology, and access conduct are defined broadly to avoid interpretive problems regarding whether the model statute covers a particular form of access. Instead, the model statute focuses on authorization: whether a principal consents to a person's access conduct. The question of authorization is narrower than that of access—a distinction reflected in how the model statute defines the level of the offense.

The severity of the model statute's punishment derives from the statute's focus on authorization and security. The model statute establishes unauthorized access as a felony offense.²⁷⁸ In several states unauthorized access is only a misdemeanor offense. This difference can be attributed to the importance of authorization and security measures. The model statute is constructed in such a manner that if a person is culpable under the statute, he or she must have violated the express edict of the principal or circumvented the principal's security measures. In contrast, the states that classify unauthorized access as a misdemeanor typically criminalize less severe conduct, such as accessing an open wireless network where the principal is silent on consent and no security measures are in place. The model statute criminalizes more severe conduct, and thus the corresponding punishment should be more severe as well.

The model statute also differs with regard to its consideration of damages. In contrast to several states that tie the level of offense to the level

²⁷⁷ For example, in Ohio, the defendants may assert the affirmative defense that they reasonably believed their access was authorized. *See* OHIO REV. CODE ANN. § 2913.03(C)(1) (West 1997).

²⁷⁸ The phrase "felony offense" is intended to mean a mid-level felony. However, given that states have differing felony standards, providing a specific grade of felony here is impractical.

of damage or loss, the model statute grants the prosecutor discretion to adjust the level of the offense based on the damage and/or loss caused by a person's unauthorized access. This reflects a policy choice to eliminate the potential for "one dollar inequity"²⁷⁹ and acknowledges the difficulties in determining damage and loss in these situations. The statute further contemplates damages and loss by empowering a principal to bring a civil suit to recover for the harm that the unauthorized access caused. The impact of damage and loss again reflects the model statute's focus on more severe conduct. Damage and loss are difficult to determine and inappropriate solely for the purpose of determining liability in and of itself. However, under the model statute, damage and loss do not determine liability, but are instead ancillary factors. Because damage and loss do not come to bear on liability itself, the statute mitigates the impact of these difficult determinations.

The last provision of the model statute, Section 100.3, addresses the potential for conflict with state contract law. Most ISPs limit the ability of their subscribers to make their wireless network freely available to the public. The potential exists for a person to engage in permissible access of an open wireless network (i.e., the principal expressly or impliedly consents to access, taking the person's access outside the scope of the model statute), while at the same time causing subscribers to violate the terms of their agreement with the ISPs. Section 100.3 disallows subscribers from asserting that they are absolved from liability to the ISP because the third party's access is permissible under state law. This provision specifically maintains the ISPs' right to bring a suit based on the terms of their agreement with subscribers.

Given this Note's focus, the application of the model statute to open wireless access is of obvious interest. The definitions provided by the statute cover all the components of an open wireless access event: "computer network" encompasses wireless networks, "person" encompasses potential wireless network users, and "principal" covers wireless network operators. Users who then log on to the wireless network engage in "access" as defined by the statute. The analysis hinges on authorization. If the principal has implemented security measures (typically encryption or password protection) and users circumvent these measures, they are liable under the statute. If the principal has expressly prohibited access by notice, users who then access are in violation of the statute. If the principal has not provided express prohibition nor implemented security measures, users' access of the principal's wireless network is presumptively valid. Unless the principal satisfies the high evidentiary threshold set by the statute and shows that users

²⁷⁹ When a statute defines an offense as a felony (that would otherwise be a misdemeanor) if the loss caused is \$1,000 or greater, \$1 may mean the difference between a felony and a misdemeanor—a potentially arbitrary and inequitable result.

did not have his or her implied consents, users' open wireless access will not violate the statute. Assuming that users do in fact engage in unauthorized access, they will be liable for a felony offense with the prosecutor to determine the grade of felony in light of the damage and loss caused by the unauthorized access. Additionally, the principal may bring a civil suit to recover from the offending users.

The proposed model statute provides a measured legal response to the issue of open wireless access. Wi-Fi networks raise important policy questions regarding free access and individual rights. The law must be sensitive to this tension and endeavor to provide an appropriate balance between these sometimes competing interests.

VIII. CONCLUSION

So what becomes of Benjamin Smith? The answer remains unclear. Regardless of his fate, his case has raised important questions of Wi-Fi policy. How should the law apply to those casual users who happen across a wireless network and browse the Web? More importantly, how should society provide for the growth and development of the Internet—do we follow a path of propretization or chart a course for the Internet commons?

Technology continually affects the lives of nearly all Americans. The growth of the Internet has changed the way people receive information, shop, communicate, and countless other aspects of daily life. Wireless technology represents the next evolution of Internet growth, taking users away from their home and incorporating the Internet into a more diverse range of everyday activities. Widespread wireless access may help to break down socioeconomic barriers by allowing users to access the Internet who might otherwise be unable to connect in their homes. Preserving free access allows the Internet to continue to grow and society to benefit.

It is imperative that the law sensibly accommodate Internet growth. Implementing law that legalizes access of open wireless networks does just that. Allowing access while protecting the right to secure one's network represents a sensible balance that furthers the development of the Internet and guards the social value created by the Internet commons. By enacting law that embodies a respect for open access to the Internet, society protects the wireless evolution of today and ensures the continued benefits from the Internet evolution of tomorrow.

