Accessing the Internet through the Neighbor's Wireless Internet Connection: Physical Trespass in Virtual Reality

Ned Snow
University of South Carolina, snownt@law.sc.edu

Follow this and additional works at: https://digitalcommons.unl.edu/nlr

Recommended Citation
Available at: https://digitalcommons.unl.edu/nlr/vol84/iss4/5
Accessing the Internet Through the Neighbor's Wireless Internet Connection: Physical Trespass in Virtual Reality

TABLE OF CONTENTS

I. Introduction .................................................................................................................. 1227
II. Factual Background ...................................................................................................... 1231
III. The Elements of Trespass to Chattel Applied to Wi-Fi Joyriding .............................. 1234
    A. The Chattel ............................................................................................................. 1235
    B. The Trespass ......................................................................................................... 1238
       1. Physical Contact ................................................................................................. 1239
          a. Jurisprudence Dealing with Physical Contact in Cyberspace ...................... 1239
          b. Criticism of Physical Contact in Cyberspace .............................................. 1242
       2. Harm .................................................................................................................... 1244
          a. Two Actionable Harms .................................................................................. 1244
          b. Harmless Intermeddling with the Router .................................................... 1249
       3. Intent ..................................................................................................................... 1254
IV. Defenses of Trespass to Chattel Applied to Wi-Fi Joyriding ...................................... 1255
    A. The Wi-Fi Operator's Seeming Consent to Joyriding ........................................... 1255
    B. The Joyriding Neighbor's Seeming Abatement to a Wi-Fi Nuisance .................... 1260
V. Conclusion .................................................................................................................... 1263
I. INTRODUCTION

Wireless fidelity ("Wi-Fi") technology brings the Internet anywhere that a radio signal can reach.1 Transmitting radio signals beyond the confines of walls, fences, and property lines, Wi-Fi technology delivers newfound convenience to a person who operates a wireless computer network ("Wi-Fi operator").2 This convenience, however, has given rise to an unintended externality. Persons whom the Wi-Fi operator never intended to receive the transmission may realize full Internet access at the operator's expense.3 A Wi-Fi operator pays $29.95 each month for Internet service;4 the operator's next-door neighbor reaps that same service for free.5 In the lexicon of cyber speech, this phenomenon is appropriately referred to as "joyriding."6 Joyriding can cause substantial delays in data transmission,7 and it can facilitate the diffusion of harmful viruses to all computers within the wireless network.8 Yet despite these possible harms, Wi-Fi operators often do

---

3. Id. at 104.
5. See Kern, supra note 2, at 109.
6. Id. at 104.
8. See Henry Kumagai, Mobile Technology Security Considerations, TECHSOUP.ORG, June 16, 2004, http://www.techsoup.org/howto/articlepage.cfm?ArticleId=552&topicid=4 ("Two recently unleashed worms, Sasser and Korgo, infect one computer and then start looking for other networked computers close by to attack."). This Article contemplates only harms that usually occur unintentionally, such as the two described above. Nevertheless, other harms are possible. Those include accessing private information from a Wi-Fi operator's computer, such as credit-card or bank-account numbers. See Alex Leary, Wi-Fi Cloaks a New Breed of Intruder, ST. PETERSBURG TIMES, July 4, 2005, at 1A, available at http://www.sptimes.com/2005/07/04/news_pf/State/Wi-Fi_cloaks_a_new_br.shtml. Another harm could occur where a joyriding neighbor causes a Wi-Fi operator to suffer disrepute. If a joyriding neighbor commits criminal acts over the Internet, those acts are traced back to the Wi-Fi operator. Id. This is so because each online connection produces an Internet Protocol ("IP") address, which is a unique numerical combination that can be traced to the physical place where the Internet connection is set up. Id. Hence, a joyriding neighbor's activities on the Internet can be traced back to the Wi-Fi operator. Id. In one instance, an e-mail
not password protect their networks. Joyriding has thus become common practice. The law should intervene.

The question of whether the common law permits a neighbor to joyride on a wireless network presents novel and complex issues of tort and property law. At first glance, it seems that the joyriding neighbor does not invade any legally protected interest of the Wi-Fi operator, even though the Wi-Fi operator may suffer negative externalities. Tort law does not appear to protect a Wi-Fi operator's interest in the wireless network because a wireless network comprises radio signals. Radio signals are uncontrollable by nature, and thereby cannot be property. Absent property, trespass cannot lie.

containing death threats was sent to a school principal. The IP address lead investigators to a dumbfounded family that had been operating a wireless Internet connection. As it turned out, a neighborhood boy had tapped into their wireless network and sent the e-mail.

9. See Hale, supra note 7, at 547; Kern, supra note 2, at 104; Steve Hargreaves, Stealing Your Neighbor's Net, MONEY, Aug. 10, 2005, at 21, available at http://money.cnn.com/2005/08/08/technology/personaltech/internet_piracy/index.htm?cnn=yes (opining that Internet joyriding is becoming a common phenomenon); Leary, supra note 8, at 1A (commenting that experts believe that scores of joyriding incidents occur undetected, and that many people do not take the time to secure their wireless Internet connections).

10. See Hale, supra note 7, at 547 (reporting that sixty-seven percent of wireless users do not implement security measures); Kern, supra note 2, at 109 ("A roaming Wi-Fi user obtains broadband Internet access service, a valuable service, without paying compensation."); Leary, supra note 8, at 1A.

11. See discussion infra Parts III, IV. Other commentators have considered whether the conduct violates state and federal statutes specifically directed at prohibiting certain forms of computer activity. See Hale, supra note 7, at 544-52 (analyzing whether the conduct violates the Computer Fraud and Abuse Act of 1986 and the Electronic Communications Privacy Act); Kern, supra note 2, at 120-51 (analyzing whether the conduct violates the Computer Fraud and Abuse Act of 1986, the Electronic Communications Privacy Act, the Communications Act of 1934, and various state statutes prohibiting unauthorized access to computer systems). They have concluded that the conduct should not be viewed as violating these statutes. See Hale, supra note 7, at 544-52; Kern, supra note 2, at 120-51. This Article does not consider federal and state statutes that could arguably apply to the conduct. Rather, this Article considers only whether the common law applies.

12. See discussion infra Parts III, IV. An analogous example of a neighbor harming the adjacent landowner but not violating any legally protected interest might occur if the neighbor were to construct an unsightly edifice which had a negative effect on surrounding property values. 66 C.J.S. Nuisances § 32 (1998) ("[A] building or structure generally cannot be complained of as a nuisance merely because it interferes with the passage of light and air to adjoining premises, regardless of the impact on the injured party's property or person."); see also, e.g., Sher v. Leiderman, 226 Cal. Rptr. 698, 701-04 (Cal. Ct. App. 1986) (holding that landowners could not recover in tort against neighbor for harm caused to landowner's property in the form of sunlight blockage).

13. Energy that cannot be controlled cannot be possessed. See BLACK'S LAW DICTIONARY 1201 (8th ed. 2004) (defining "possession" to mean "[t]he right under which
Even if wireless networks were recognized as property, the neighbor's conduct is arguably permissible. Where the Wi-Fi operator has failed to set up a password, the operator seems to implicitly consent to sharing Internet access.\textsuperscript{17} The Wi-Fi operator seems to consent to joy-riding.\textsuperscript{18} Furthermore, the common law permits a neighbor to use property that crosses onto and interferes with the neighbor's airspace.\textsuperscript{19} The Wi-Fi radio signals cross over to the neighbor's land, potentially interfering with the neighbor's airspace, so the common law may protect the neighbor's conduct.\textsuperscript{20} Finally, social policy seems to support the position of the joyriding neighbor. The Internet is a public good, and the law should support any means of allowing as many persons to access it.\textsuperscript{21} To that end, it is arguable that Wi-Fi radio signals, which travel over government-regulated frequencies,\textsuperscript{22} should not be subject to private ownership. Wi-Fi signals should arguably be treated as part of a public commons available for anyone's use.\textsuperscript{23}

Despite these arguments against finding a trespass, recent caselaw dealing with the Internet suggests otherwise. Courts are quickly remolding the age-old trespass-to-chattel doctrine so that it fits the new medium of cyberspace.\textsuperscript{24} Albeit relatively young, Internet juris-
prudence has espoused the view that electronic signals sent through
cyberspace to a physical object may give rise to contact that is trespass-
sory in nature. Applying this new doctrine to the Wi-Fi context
reveals that a joyriding neighbor likely trespasses when the neighbor
sends electronic signals to the Wi-Fi operator's device that transmits
data through the Internet—a Wi-Fi router. Whereas Wi-Fi radio
signals are not property, the Wi-Fi router indisputably is. It is a phys-
ical object that remains in the possession and control of the Wi-Fi op-
erator. Under the reasoning of Internet caselaw, the joyriding
neighbor appears to "intermeddle" with the router when the neighbor
sends electronic signals through it. Because the router is the prop-
erty under consideration—rather than Wi-Fi radio signals—the fact
that a joyriding neighbor uses Wi-Fi radio signals which cross over to
the neighbor's land is of no consequence. Trespassory contact ap-
ppears to occur at the router.

Policy also implies a trespass. The transaction costs of joyriding—
the possibility of computer viruses and transmission delays—ou-
weigh the benefit of permitting joyriding neighbors free access to the
Internet. In short, joyriding can impose costly consequences on the
unsuspecting Wi-Fi operator. Moreover, even if these transaction
costs did not exist, the joyriding neighbor strips Internet service prov-
iders ("ISPs") of economic returns. It is likely that some joyriding
neighbors value Internet access at a level sufficiently high such that
they would subscribe to ISP services were joyriding unavailable. To
realize a full return on their investment in Internet technology, ISPs
must receive payment for their services by anyone who uses it. Pro-

25. CompuServe, 962 F. Supp. at 1021 ("Electronic signals generated and sent by
computer have been held to be sufficiently physically tangible to support a tres-
pass cause of action." (relying on Thrifty-Tel, Inc. v. Bezenek, 54 Cal. Rptr. 2d
468, 473 n.6 (Cal. Ct. App. 1996) (holding that electronic signals that defendants
had generated to access a phone system were "sufficiently tangible to support a
trespass cause of action")).

26. See Bidder's Edge, 100 F. Supp. 2d at 1069 ("[I]t appears likely that the electronic
signals sent by [the defendant] to retrieve information from eBay's computer sys-

27. See How and Why of Wi-Fi, supra note 1.
28. See discussion infra subsection III.B.1.
29. See discussion infra subsection III.B.1.
30. See discussion infra subsection III.B.2.
31. See discussion infra subsection III.B.2.
32. See Kern, supra note 2, at 110 (discussing the detrimental effect that free-riding
users of a wireless network have on the capacity and infrastructure of an ISP).
33. See discussion infra subsection III.B.2.
tection of Internet investments favors viewing the neighbor's conduct as a trespass.34

This Article addresses the question of whether the joyriding neighbor commits an actionable trespass against the Wi-Fi operator. Part II explains how a wireless network functions, and how a neighbor is able to access that network. Part III examines whether the neighbor's conduct satisfies the elements of trespass to chattel, identifying the chattel at issue as the Wi-Fi router. Part III concludes that the neighbor's conduct satisfies the elements of trespass to chattel. Part IV examines the defenses to trespass to chattel, addressing whether joyriding is permissible when a Wi-Fi operator has not password protected the network or when the Wi-Fi operator's network interferes with the neighbor's ability to set up his or her own wireless network. Part IV concludes that neither the absence of password protection nor the presence of Wi-Fi interference should be a defense to the tortious conduct.

II. FACTUAL BACKGROUND

A wireless network allows computers within a local geographic area to share information without being connected by wires.35 Radio signals make Wi-Fi technology possible.36 Wi-Fi radio signals originate from a device called a Wi-Fi router.37 The Wi-Fi router transmits data between computers within the network, and between a modem that is connected to the Internet and a computer within the network.38 In effect, the Wi-Fi router serves as a hub for information exchange between computers within the network and between any network computer and the Internet.39

Wi-Fi routers operate on frequencies that the government has permitted consumers to use without licenses. Baby monitors, cordless phones, microwave ovens, Bluetooth devices,40 and other wireless de-

34. See discussion infra subsection III.B.2.
35. Kern, supra note 2, at 103.
36. See How and Why of Wi-Fi, supra note 1.
38. See sources cited supra note 37.
39. See sources cited supra note 37.
To prevent wireless devices from interfering with one another, the frequencies have multiple channels on which a single wireless device can operate. Most wireless devices will "listen" for a clear channel before becoming active. Thus, a wireless network can experience interference, but technological advances are decreasing instances of such interference.

The range of a Wi-Fi router's signal varies according to its strength in relation to physical obstructions. On average, routers can reliably transmit signals over a range of about 300 feet, approximately the size of a football field. Physical objects cannot usually impede Wi-Fi radio signals anywhere within this range. Hence, data transmission is possible between computers in separate rooms, or even in different buildings.

The strength of Wi-Fi radio signals allows a neighbor of a Wi-Fi operator to access the wireless network. The neighbor need merely install a wireless network adapter on a computer and place the computer within the range of the Wi-Fi operator's router. After the wireless network adapter is installed on the neighbor's computer, the computer can receive Wi-Fi radio signals. When the computer locates a Wi-Fi signal, it displays a prompt on its screen, querying the neighbor whether the computer should interface with the wireless net-


43. Id.

44. Id. at 6–7

45. Kern, supra note 2, at 103. It is noteworthy that the 300-foot range of home wireless networks does not reflect the limits of technology. Using the proper antenna, a person could receive Wi-Fi radio signals as far away as a mile from the transmitting router. Wi-Fi Alliance, Range & Environment Issues, http://wifi.org/OpenSection/range.asp?TID=2 (last visited May 15, 2006); accord Hines, supra note 7 (stating that with a special amplification device, a person could receive Wi-Fi radio signals as far away as seventy-two miles).


47. See Hale, supra note 7, at 543–44.

48. Kern, supra note 2, at 104.

49. See id. at 103; Linksys White Paper, supra note 42, at 6; Mitchell, supra note 37.

50. See Jim Harrington, Linksys: Antenna Basics, (Nov. 19, 2001), at 2–6 (on file with author) (explaining how computer antennas function); Mitchell, supra note 37.
work. Selecting “OK” connects the neighbor’s computer to the Internet through the wireless network. A neighbor might view websites, check e-mail, download files, file share, or media stream. Any of these practices constitutes “joyriding.” It is noteworthy that while joyriding, a neighbor may unintentionally transmit an electronic virus to computers within the wireless network. That is, a virus can pass from the neighbor’s computer, through the router, to the operator’s computer—even where the neighbor does not access the operator’s computer, but merely accesses the Internet through the Wi-Fi connection. In the absence of specialized software that many Wi-Fi operators are not likely aware of, viruses within a network can spread uninhibited from computer to computer.

A Wi-Fi operator often does not know when someone is joyriding on the wireless network. If a joyriding neighbor only surfs the web or checks e-mail, the Wi-Fi operator’s rate of data transmission to and from the Internet is not noticeably slower than if the neighbor were not using the wireless network. On the other hand, if the neighbor downloads large files from the Internet, or engages in file-sharing or media-streaming, the neighbor will tax the router’s resources. A Wi-Fi operator would notice a delay in the transmission speed. Nevertheless, even where there is such a delay, there is no immediate indication to the Wi-Fi operator that the neighbor has accessed the

51. See Hale, supra note 7, at 543.
52. See id.
53. See id. at 552–54.
54. Kern, supra note 2, at 104.
55. See Kumagai, supra note 8.
56. This type of virus transmission is possible through a process called “port scanning.” See Gary C. Kessler, Port Scanning: It’s Not Just an Offensive Tool Anymore (May 2001), www.garykessler.net/library/is_tools_scan.html. A computer connected to a network may contain a “port scanner” virus. A “port scanner” would probe the network, through the network’s unique IP address, to determine which other computers are connected to that network. See id. After probing the network, the port scanner would search for software on the network computers vulnerable to virus attacks. See id.
57. See Hines, supra note 7. It should be noted that a computer firewall that blocks virus transmission from sources on the Internet does not block viruses from sources within the network. See id. (advocating computer users purchase specialized firewalls for protection from virus dissemination within a network); Jeff Tyson, How Firewalls Work, http://computer.howstuffworks.com/firewall.htm/printable (last visited May 15, 2006) (“A firewall is simply a program or hardware device that filters the information coming through the Internet connection into your private network or computer system.”).
58. See Kern, supra note 2, at 104.
59. Hale, supra note 7, at 554.
60. Id. at 552–53.
61. Id.
wireless network. The Wi-Fi operator would experience a transmission delay, but would not know the source of that delay.

Wi-Fi operators can prevent joyriding by simply setting up a password that users must provide to access the wireless network. However, most Wi-Fi operators do not invoke such security measures. It is therefore likely that most instances of joyriding do not consist of "hacking" into a password-protected wireless network. For the purposes of this Article, "joyriding" refers to the unauthorized access of a wireless network, which is not password protected, for the sole purpose of engaging in Internet activity.

III. THE ELEMENTS OF TRESPASS TO CHATTEL APPLIED TO WI-FI JOYRIDING

This Part examines whether the joyriding neighbor's conduct gives rise to a claim of trespass to chattel. A trespass to chattel lies where

62. See Kern, supra note 2, at 104. It should be noted that software programs exist which would enable a Wi-Fi operator to be aware of another person accessing the network. See, e.g., IBM Tivoli Monitoring, http://www-306.ibm.com/software/tivoli/products/monitor/?CVM=no (last visited May 15, 2006) (describing network-monitoring software).
63. See Kern, supra note 2, at 104.
64. See Hale, supra note 7, at 546-47.
65. In 2003, an estimated sixty-seven percent of Wi-Fi operators did not enable security measures. Id. at 547. By 2007, it is estimated that nearly eighty percent of wireless networks will be unsecured. Id.
66. This Article does not consider whether joyriding gives rise to claims of trespass to land or nuisance. A brief analysis of these issues, however, reveals that neither tort applies. An argument that the joyriding neighbor commits a trespass to land relies on the premise that the Wi-Fi radio signals which the neighbor transmits to the Wi-Fi router constitute an actionable intrusion on the Wi-Fi operator's land. See RESTATEMENT OF TORTS § 158 cmt. i, at 278 (1958) (stating that an actor may trespass to land by throwing, propelling, or placing a thing in the air space above the land). This premise is untenable because the radio signals operate on bandwidth frequencies that the FCC has designated as "unlicensed." See supra note 22. A person has no right to exclude another from using one of the unlicensed frequencies, even where the frequency lies within the geographic boundary of the person's land. For instance, the interference that a baby monitor causes to an adjacent landowner's cordless phone does not result in a trespass to land.

With regard to the tort of nuisance, it is well established that federal law preempts a nuisance claim based on radio-signal interference. See Brody v. Gotham Tower, Inc., 13 F.3d 994, 997-98 (6th Cir. 1994) (holding that enforcement of a nuisance claim based on radio-signal interference would contravene the doctrine of preemption, frustrating the objectives of the Federal Communications Act); Goforth v. Smith, 991 S.W.2d 579, 584-85 (Ark. 1999) (ruling that the FCC has exclusive jurisdiction over disputes involving radio-interference nuisance claims); Still v. Michaels, 803 P.2d 124, 124-25 (Ariz. 1990) (same); Blackburn v. Doubleday Broad. Co., 353 N.W.2d 550, 555-57 (Minn. 1984) (same). Nuisance does not apply. With regard to the governing federal law, see supra note 12 and accompanying text.
an actor intentionally dispossesses another of a chattel, or alternatively, uses or intermeddles with a chattel in possession of another.\textsuperscript{67} Section III.A considers the possible chattel on which the joyriding neighbor allegedly trespasses. Section III.B analyzes whether the neighbor’s conduct is trespassory in nature. A discussion of the possible defenses to trespass to chattel follows in Part IV.

A. The Chattel

Trespass to chattel requires that a chattel exist.\textsuperscript{68} If the joyriding neighbor commits a trespass to chattel against the Wi-Fi operator, the Wi-Fi operator must own a “thing” on which a trespass can be committed.\textsuperscript{69} At first glance, the “thing” to be considered in the trespass analysis seems to be the wireless network.\textsuperscript{70} As discussed below, however, a wireless network does not possess characteristics of property which are necessary for ownership. Therefore the “thing” to be considered in the trespass analysis should not be the wireless network; instead, for reasons discussed below, the “thing” should be the Wi-Fi router.

The view that the wireless network is a chattel against which a trespass may be committed essentially posits that a Wi-Fi operator should be rewarded for laboring to create the network.\textsuperscript{71} It is the Wi-Fi operator who purchases and installs a router that makes the network even possible. On the basis that laborers should hold property rights in the fruits of their labors, the Wi-Fi operator arguably should own the radio signals that the Wi-Fi router transmits.\textsuperscript{72} The Wi-Fi operator is, in effect, the creator of the transmission. As the creator,
the Wi-Fi operator seems to hold property rights over the creation—the wireless network, or in other words, the Wi-Fi radio-signal transmission. The Wi-Fi operator seems to hold property rights over the creation—the wireless network, or in other words, the Wi-Fi radio-signal transmission.73

This argument is unpersuasive. Although a person may expend great labor to produce an outcome, that outcome does not necessarily produce a thing to which property rights may attach.74 Property requires exclusivity.75 Regardless of whether the subject of property is tangible or not, that subject must be capable of exclusive control and possession.76 The wireless network is not capable of being exclusively controlled or possessed because it includes radio signals.77 Radio signals cannot be contained within a geographic boundary.78 Their only boundary is their bandwidth frequencies, and those frequencies are unlicensed, meaning that the government has permitted any person to transmit signals over the frequencies.79 Coterminous use of the frequencies is therefore permissible, which could produce interference.

73. On three separate occasions, federal district courts have labeled a computer network as the subject of property. See Am. Online, Inc. v. LCGM, Inc., 46 F. Supp. 2d 444, 452 (E.D. Va. 1998) ("The transmission of electrical signals through a computer network is sufficiently 'physical' contact to constitute a trespass to property.") (emphasis added); Am. Online, Inc. v. IMS, 24 F. Supp. 2d 548, 550 (E.D. Va. 1998); Hotmail Corp. v. Van$ Money Pie, Inc., No. C-98 JW PVT ENE, C 98-20064 JW, 1998 WL 388389, at *7 (N.D. Cal. Apr. 16, 1998) (opining that "computer networks" comprising an e-mail system can be personal property). As one commentator has noted, however, where courts have found aspects of computer accessing to be property, their analysis appears to have been driven by a results-oriented outcome. See Orin S. Kerr, Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes, 78 N.Y.U. L. Rev. 1596, 1610–11 (2003).

74. See, e.g., Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., 499 U.S. 340, 349 (1991) ("The primary objective of copyright is not to reward the labor of authors . . . . ").

75. 73 C.J.S. Property § 7, at 9 (1998) ("It has been said that for a property right to exist in something, there must be an interest capable of a precise definition, it must be capable of exclusive possession or control, and the putative owner must have established a legitimate claim to exclusivity."); see also JOHN E. CRIBBET ET AL., PROPERTY 8 (David L. Shapiro et al. eds., The Foundation Press 1996) (1960) (commenting that exclusivity is a necessary criterion for an efficient system of property rights).

76. For instance, property rights exist in intangible domain names because registration of a domain name excludes others from using it on the Internet. See Kremen v. Cohen, 337 F.3d 1024, 1030 (9th Cir. 2003).

77. See How and Why of WiFi, supra note 1 (stating that wireless networks operate in the unlicensed 2.4 and 5 GHz bandwidths).

78. An argument could be made that Wi-Fi radio signals can be contained within a physical boundary. A company called Force Field Wireless has developed, and sells, paint that, according to the company, bars the passage of radio signals. See Force Field Wireless, http://www.forcefieldwireless.com/defendair.html (last visited May 15, 2006). Apparently the paint is laced with copper and aluminum, both of which form an electromagnetic shield. Hines, supra note 7. Unfortunately the paint comes in only one color—gray. Id.

79. See supra note 22.
between competing signals.\textsuperscript{80} A Wi-Fi operator cannot exclude another person from using a frequency, meaning that a Wi-Fi operator cannot exclude another person from interfering with Wi-Fi radio signals.\textsuperscript{81} In short, Wi-Fi radio signals do not admit exclusivity, so they should not be viewed as property.\textsuperscript{82}

It should be noted that the capability to password protect a wireless network does not satisfy the exclusivity requirement of property. Although a Wi-Fi operator can password protect the wireless network against unwanted use, the Wi-Fi operator cannot preclude another person from interfering with the Wi-Fi radio signals.\textsuperscript{83} The fact that interference is possible, and moreover permissible,\textsuperscript{84} demonstrates that a Wi-Fi operator is unable to exercise exclusive control and possession over the Wi-Fi radio signals. The password protects another person from interpreting Wi-Fi signals, but not from interfering with the signals. Password protection does not imply that the operator can exclude others from interfering with the Wi-Fi radio signals. They are not property.

Although the radio signals composing the network are not property, a physical piece of equipment that makes possible the network indisputably is. The router—the network component through which Wi-Fi radio signals are transmitted—is property.\textsuperscript{85} Unlike radio signals which are incapable of exclusive control and possession, the Wi-Fi router is continually in the control and possession of the Wi-Fi operator. Even during the neighbor's joyriding, the router remains physically with the Wi-Fi operator. The Wi-Fi operator therefore holds an undisputable property interest in the router. The question of trespass is thus whether the neighbor's use of the router constitutes a violation of the Wi-Fi operator's property rights in the router.

\textsuperscript{80} Linksys White Paper, \textit{supra} note 42, at 6.
\textsuperscript{81} The fact that a wireless-device user cannot prohibit radio interference on an unlicensed frequency is consistent with the fact that a wireless-device user can prohibit a person from employing the frequency as a means to harm the user's personal property. The former fact concerns interference on the frequency bandwidth; the latter fact concerns personal property rights, independent of frequency interference.
\textsuperscript{82} This fact is also manifested by Congress's express declaration with respect to licensed frequencies. \textit{See} 47 U.S.C. § 301 (2000). \textit{But see} Cribbet \textit{et al.}, \textit{supra} note 75, at 9–10 (arguing that property rights exist in broadcast frequencies in at least economic terms). If in fact licensed frequencies cannot be owned, it appears certain that property rights do not attach to unlicensed frequencies either.
\textsuperscript{83} \textit{See} Linksys White Paper, \textit{supra} note 42, at 6.
\textsuperscript{84} Interference is "permissible" to the extent that the unlicensed frequencies are not regulated by government. \textit{See} \textit{supra} note 22.
\textsuperscript{85} \textit{See} sources cited \textit{supra} note 37.
B. The Trespass

"The law hath not been dead, though it hath slept."86 The tort of trespass to chattel has lain dormant for years, having been employed in times past to remedy farmers for injuries that were intentionally inflicted on sheep and cattle.87 Recently, however, the tort has been revived to deal with troubles in cyberspace.88 Courts have resurrected the doctrine to prohibit the sending of unsolicited mass e-mails and the searching of websites by robotic software.89 Trespass to chattel has served as a legal means for controlling traffic in cyberspace. Still undetermined is the question of whether the tort's application to the ontology of cyberspace encompasses Wi-Fi joyriding.90

An actionable trespass to chattel occurs when an actor intentionally either dispossesses another of a chattel, or alternatively, uses or "intermeddles" with the chattel while it is in the possession of another.91 In the context of Wi-Fi joyriding, the neighbor does not physically dispossess the Wi-Fi operator of the router. The neighbor uses the router while it remains in the physical possession of the Wi-Fi operator. Accordingly, the question of whether the neighbor trespasses on the router involves an examination of whether the neighbor has intentionally used or "intermeddled" with the router.

To use or intermeddle with a chattel, an actor must bring about physical contact with the chattel.92 Physical contact may occur if the actor physically touches the chattel, or if the actor causes something else to touch the chattel.93 A touching results in intermeddling.94 Yet not all instances of intermeddling give rise to liability for trespass to chattel.95 Liability arises only if the intermeddling causes harm.96 Harm is manifest by an impairment of the chattel's condition, quality,
or value. In the absence of any of these conditions, the intermeddling is harmless, and thereby not actionable.

The following three subsections examine whether Wi-Fi joyriding satisfies these requirements for trespass to chattel. Subsection III.B.1 examines whether the neighbor's use of the Wi-Fi operator's router results in physical contact sufficient to constitute intermeddling. Subsection III.B.2 examines whether the alleged contact results in harm. Subsection III.B.3 examines whether the neighbor's use of the router is intentional.

1. Physical Contact

Perhaps most intriguing about the Wi-Fi trespass argument is the issue regarding whether a trespass is possible even though the neighbor never causes a material object to physically contact the Wi-Fi router. The argument for trespass relies on the premise that the neighbor causes physical contact with the router when the neighbor transmits electronic signals through the router in order to access the Internet. Although that premise has not yet been considered by any court, courts have considered whether electronic signals satisfy the physical-contact element in the context of Internet users sending e-mail and accessing information on websites. As discussed below, these e-mail and website cases suggest that Wi-Fi joyriding satisfies the physical-contact element of trespass to chattel.

a. Jurisprudence Dealing with Physical Contact in Cyberspace

Amidst public frustration with unsolicited mass e-mails, courts have held that transmitting such e-mails constitutes a trespass to chattel. The first instance occurred in CompuServe, Inc. v. Cyber Promotions, Inc. There, the defendants sent unsolicited mass e-
-mails to subscribers of an ISP, CompuServe. The federal district court held that the defendants had trespassed on CompuServe's computer equipment, finding that the defendants had "intermeddled" with the equipment. In so holding, the court specifically held that the electronic signals which the defendants had generated in order to send the e-mail through CompuServe's computer equipment resulted in physical contact.

Soon after CompuServe, trespass to chattel was routinely deployed to cease the practice of mass e-mailing. For instance, in America Online, Inc. v. IMS, a federal district court relied exclusively on CompuServe to find that the defendant had trespassed on an ISP's property. As in CompuServe, the IMS court held that the electronic signals that the defendants had sent as e-mails through the plaintiff's computer equipment were sufficient to constitute a "contact" for purposes of establishing trespassory intermeddling. Following IMS, the same federal district court faced the same issue in America Online, Inc. v. LCGM, Inc. Without hesitation, the LCGM court declared that "[t]he transmission of electrical signals through a computer network is sufficiently 'physical' contact to constitute a trespass to property." Thus, CompuServe's substantive alteration of an age-old tort principle was readily accepted by courts. Its rationale continues to be deployed against defendants who send unsolicited mass e-mails over the Internet.

Following the lead of these trespass-by-e-mail cases, courts applied the doctrine of trespass to chattel as a means for precluding Internet users from engaging automated software to collect data from web-

104. Id. at 1017.
105. Id. at 1027.
106. Id. at 1021. The CompuServe court relied on the reasoning of one case for this finding—a California State Court decision, Thrifty-Tel, Inc. v. Bezenek, 54 Cal. Rptr. 2d 468 (Cal. Ct. App. 1996). In Thrifty-Tel, children used software to conduct high-speed automated searches of possible access codes for a company's telephone system. Id. at 471–72. The court held that the children had committed a trespass to chattel. Id. at 473 n.6. According to the court, the electronic signals composing the access codes were "sufficiently tangible to support a trespass cause of action." Id. The court reached this conclusion by relying on cases holding that microscopic particles, such as dust and smoke, can constitute a trespass. Id. As one commentator has pointed out, however, those cases on which Thrifty-Tel relied dealt with trespass to land, not trespass to chattel. Dan L. Burk, The Trouble with Trespass, 4 J. SMALL & EMERGING BUS. L. 27, 33 (2000).
107. See, e.g., cases cited supra note 102.
109. Id. at 550.
111. Id. at 452.
112. See cases cited supra note 102.
sites. In eBay, Inc. v. Bidder's Edge, Inc., the defendant, Bidder's Edge, executed a computer program, otherwise known as a "bot," to search and retrieve data from the website of the plaintiff, eBay. The court held that the electronic signals sent by Bidder's Edge through the bot to eBay's server were "sufficiently tangible to support a trespass cause of action." Electronic signals satisfied the physical-contact requirement. Subsequently, in Register.com, Inc. v. Verio, Inc., another federal district court ruled that searching websites by using an automated software bot constituted a trespass to chattel. The court did not even offer an explanation for the fact that physical contact had occurred. The court's failure to address this point suggests that it was so well established that it did not merit discussion.

These cases adopt a rationale that electronic signals which interact with physical components of computer equipment satisfy the physical-contact requirement for trespass. Notable is the fact that physical contact has been found in situations where the computer equipment facilitates Internet communication. It appears that the intangible nature of the Internet affects the physical-contact requirement of trespass: where the alleged trespass occurs on the Internet, the contact need not be with a physical object, but rather can be with an electronic wave. Also notable is the fact that in cases where courts have held that a trespass to chattel did not occur on the Internet, the courts have not taken issue with the principle that electronic signals satisfy the physical-contact requirement. Cyberspace jurisprudence thus appears to establish that electronic signals that contact a computer component which facilitates Internet communication is sufficient to satisfy the physical-contact requirement of trespass to chattel.

115. 100 F. Supp. 2d 1058 (N.D. Cal. 2000).
116. Id. at 1060, 1062.
117. Id. at 1069.
118. See id.
120. See id. at 245–50.
121. See id.
124. See cases cited supra note 123.
Applying this principle to the Wi-Fi context reveals that the joyriding neighbor who sends electronic signals through the Wi-Fi router is causing physical contact with the router. A Wi-Fi router is a physical component of computer equipment that facilitates Internet communication. The reasoning of the cases described above implies that the electronic signals that contact the router constitute physical contact sufficient to support a finding of intermeddling.

b. Criticism of Physical Contact in Cyberspace

The view that physical contact occurs when an electronic signal contacts a physical object is not without criticism. The evident flaw with the view is that a Wi-Fi electronic signal is not a material object. It is a wave that travels through air. If an electromagnetic wave is capable of causing physical contact with a chattel, then other forms of waves would be capable of causing physical contact. For example, physical contact would result when a person directs an air fan to blow air onto another’s flag, yet this does not seem to be a tenable example of trespassory physical contact. Consequently, the view that Wi-Fi signals satisfy the physical-contact element of trespass to chattel opens the door to situations where it would seem ridiculous to find trespassory intermeddling.

One commentator has raised a similar criticism of the physical-contact element in the context of Internet trespass cases. Trespassory physical contact over the Internet, according to the commentator, gives rise to ridiculous implications. Unwanted telephone callers send electronic signals to another’s telephone, so they would commit a trespass to chattel; the same could be said of people who transmit facsimiles or television broadcasts. Electronic signals from baby monitors which interfere with the operation of cordless telephones would also result in trespass. Such bizarre results would seem to preclude the conclusion that an electronic signal satisfies the physical-contact requirement of trespass to chattel.

These criticisms would be well grounded if intermeddling were the only element of an actionable trespass to chattel. Indeed, nearly every device capable of producing airwaves or electronic signals would constitute a means for committing a trespass to chattel. Such an outcome cannot be. And it is not. As discussed above, trespassory intermed-

125. See Hewlett Packard, supra note 37 (describing function of wireless router).
126. See Burk, supra note 106, at 32–34.
127. See Harrington, supra note 50, at 2.
128. See id.
130. Id. at 34.
131. Id.
132. Id.
dling requires that the physical contact cause actionable harm, and that the intermeddling be intentional. With respect to harm, the seemingly "ridiculous" examples of airwaves and electronic signals causing physical contact lack this necessary element. The lack of harm in the airwave example is obvious: blowing airwaves onto a flag does not damage the flag. However, if a person directed a powerful air fan toward a lightweight vase that was precariously standing upright, and in so doing caused the vase to blow over and break, then the airwaves would be the means of committing actionable physical contact. The same is true of electronic signals. A telephone caller causes electronic signals to contact another's telephone, but the signals do not result in any damage to the telephone that is contacted. By contrast, if a person were to cause a power surge to short a cordless telephone so that it was no longer operable, then the contact by the electronic signals would have resulted in a trespass. An action for trespass lies only if physical touching—by physical object, by airwave, or by electronic signal—results in harm to the chattel.

Intentionality must also exist for an intermeddling to be tortious. According to the Restatement, trespass to chattel does not lie unless the actor acts "for the purpose of using or otherwise intermeddling with a chattel or with knowledge that such an intermeddling will, to a substantial certainty, result from the act." In other words, an actor must intend to contact the chattel at issue for trespass to lie. Most instances where an electronic device interferes with the performance of another electronic device are not likely intended. For instance, parents do not usually intend for their baby monitors to interfere with nearby cordless phones. An action for trespass would

133. See Restatement of Torts §§ 217, at 417, 218 cmt. e, at 421–22 (1958); see also discussion supra section III.B.
134. See Chair King, Inc. v. GTE Mobilnet of Houston, Inc., 135 S.W.3d 365, 395 (Tex. App. 2004) (refusing to recognize that an unsolicited fax resulted in a trespass to chattel because the fax recipient sustained no actual damages). It is noteworthy that even an obscenely offensive telephone call would not satisfy the harm requirement for trespass to chattel. See Intel Corp. v. Hamidi, 71 P.3d 296, 308–09 (Cal. 1996) (rejecting argument that electrical signal can harm recipient based on the content of the message sent via the signal).
135. See Restatement of Torts § 218 cmt. e, at 421–22; W. Page Keeton et al., supra note 87, § 14, at 87. It should be noted that in circumstances where an actor touches but does not harm a chattel, the chattel owner may use reasonable force to halt the touching. Restatement of Torts § 218 cmt. e, at 421–22. For example, a car owner may remove a person who refuses to move from the owner's car. W. Page Keeton et al., supra note 87, § 14, at 87. In the context of electronic signals, then, a telephone owner may use reasonable force to protect her phone from the electronic signals of an unwanted telephone call—she may hang up on the caller.
137. Id. cmt. c, at 418.
138. See id.
On the other hand, if a person intentionally employed a radio jammer to interfere with the signal of a cordless phone so that it was inoperable, then a trespass would lie. Whereas the concerned parent would never face liability for trespassing by baby monitor, the radio jammer would. Wireless radio interference is usually unintentional, preventing otherwise ridiculous instances of trespass.

In sum, the view that electronic signals and airwaves can be the means of committing actionable physical contact appears sound. The ridiculous examples that the above criticisms raise would never result in liability for trespass. Just as patting another's horse or accidentally tripping on another's cat does not result in actionable trespass, neither does blowing air on a flag, placing a telephone call, or interfering with a baby monitor. Trespassory liability requires harm and intentional conduct. In conjunction with those elements, electronic signals and airwaves can constitute means for trespassing on a chattel.

2. Harm
   a. Two Actionable Harms

As most wireless electronic signals do not result in actionable harm, an issue arises as to whether the neighbor who joyrides on the wireless network causes harm to the router of the Wi-Fi operator. To satisfy the harm requirement, the physical contact must impair the chattel's condition, quality, or value, or alternatively, the contact must result in the owner being deprived of the chattel's use for a substantial time period. Impairment must be actual rather than merely possible. In the Wi-Fi context, two harms are possible: (i) decreasing router performance for the Wi-Fi operator; and (ii) transmitting computer viruses through the router to the Wi-Fi operator's computer.

139. See id. at 417.
140. See W. PAGE KEETON ET AL., supra note 87, § 14, at 87 (noting that patting a horse does not result in trespass to chattel).
142. Id. § 218, at 420; see also W. PAGE KEETON ET AL., supra note 87, § 14, at 87 (observing that harmless interference will not result in a trespass to chattel).
143. RESTATEMENT OF TORTS § 218 cmt. e, at 421–22.
144. It is arguable that the neighbor unintentionally commits other harms against the Wi-Fi operator. The Wi-Fi operator could be liable to an ISP for permitting a third party to access the ISP's services without authorization. See Kerr, supra note 73, at 1599–1600, 1637–39 (observing that courts have interpreted "unauthorized access" as occurring when a computer user accesses another's computer network in violation of a contract between that other person and a third party). In most contractual agreements with ISPs, Wi-Fi operators agree to restrict their use of the ISP's services. Hale, supra note 7, at 555. For instance, one ISP service agreement states that that user agrees "not to permit anyone else to use [the] Member Account." See SBC Yahoo! Terms of Service, http://sbc.yahoo.com/terms/ (last visited May 15, 2006). By failing to password protect the wireless network,
As discussed below, these consequences of joyriding should demonstrate sufficient harm to impose liability for trespass.

The first harm occurs where the Wi-Fi operator experiences a delay while accessing the Internet through the router. When the neighbor accesses the Internet through the Wi-Fi operator's router, the neighbor consumes resources of the Wi-Fi router. For example, if the neighbor were to download large media files from the Internet, the neighbor would decrease the speed at which the router transfers data to the Wi-Fi operator. Similarly, if the neighbor were to engage in peer-to-peer file sharing over the Internet, the neighbor would compromise router performance. Hence, when the neighbor intermediates with the Wi-Fi operator's router, the neighbor could harm the Wi-Fi operator's ability to optimally use the router. A router that transmits data slower than it otherwise could is less valuable to the Wi-Fi operator. The first harm appears to result in an impairment of the router's value.

The second harm occurs where the Wi-Fi operator receives a computer virus from the neighbor's computer. By joyriding, a neighbor

the Wi-Fi operator who fails to institute security measures is arguably permitting anyone within the physical range of the network's range to access the ISP's services. The Wi-Fi operator could therefore be breaching the ISP agreement if that agreement specifically restricts the usage of ISP services to the Wi-Fi operator. Such a breach would likely impair the value of the router: the router would be the means by which the Wi-Fi operator becomes liable to the ISP, so its value would decrease in proportion to the amount of liability. A harm arguably results.

Despite the presence of this harm, it is not likely actionable under trespass to chattel because it is economic in nature. Courts have refused to recognize economic harm as a basis for supporting liability under a claim of trespass to chattel. See Intel Corp. v. Hamidi, 71 P.3d 296, 300 (Cal. 2003) (refusing to recognize "consequential economic damages" as satisfying the requirement for harm under trespass to chattel).

Another harm could occur based on the fact that every website that a joyriding neighbor visits will register the Wi-Fi operator's unique IP address. See Hines, supra note 7. Tracing which Internet users visited particular websites could potentially harm the reputation of the Wi-Fi operator, especially given that downloading child pornography through another person's Wi-Fi connection has become a reality. See id.; Seth Schiesel, Growth of Wireless Internet Opens New Path for Thieves, N.Y. Times, Mar. 19, 2005, at A1. It is possible, then, that a Wi-Fi operator could suffer reputational harm due to the neighbor's joyriding.

145. See Hines, supra note 7 (reporting that joyriding can result in a decrease in Internet performance for a Wi-Fi operator).
146. Hale, supra note 7, at 552; Hines, supra note 7.
147. Hale, supra note 7, at 553.
148. Id. at 552–53; Hines, supra note 7. Admittedly, not all instances of joyriding result in this first harm. Checking e-mail or viewing websites would not noticeably slow down the rate of data transmission. See Hale, supra note 7, at 554.
149. See Klaus, supra note 41 ("Next generation virus and worms have become a multi-vector attack programs [sic] that self-propagate through any TCP/IP interface including wireless. If one computer on a wireless network is infected with a hybrid threat, this threat can easily spread to other wireless computers and po-
can unknowingly subject all other computers within the wireless network to a virus. This is possible because all computers within the same wireless local area network indiscriminately share data through the Wi-Fi router. Consequently, the router becomes a device for disseminating viruses from the neighbor's computer to the Wi-Fi operator's computer. The neighbor's conduct transforms the router from a valuable conduit for Internet access to a noxious chamber of virus diffusion. When the neighbor transmits electronic signals containing a virus through the Wi-Fi operator's router, the value of the router decreases. The second harm thus results in an impairment of the router's value.

It could be argued that trespass to chattel does not lie because neither of these alleged harms actually impair the physical condition of the router. The Restatement provides that in most instances, actionable impairment of a chattel must result from some impairment of the physical condition of the chattel. With respect to the first harm, the delay that the Wi-Fi operator may notice while the neighbor is joyriding does not imply that the router is physically dysfunctional. On the contrary, the router functions exactly as it should: it splits its resources between the computers connected to the wireless network.

The opposite situation—where the joyriding neighbor receives a virus from the Wi-Fi operator—would not give rise to a tort action against the Wi-Fi operator. Presumably the joyriding neighbor would bring a negligence suit against the Wi-Fi operator for breaching a duty of care to operate the network without any harmful computer viruses. See W. Page Keeton et al., supra note 87, § 30, at 164–65 (outlining the elements of a negligence cause of action). The Wi-Fi operator would likely be viewed as having assumed the risk of harm by logging onto the wireless network. See id. § 68, at 484–85 (explaining the considerations in finding an implied assumption of risk). Likely the situation would be analogous to a property owner who allows his bumble bees to fly onto land where the bees consume poison. See Jeanes v. Holtz, 211 P.2d 925, 927 (Cal. Dist. Ct. App. 1949) (ruling that defendant was not negligent where neighbor's bees came onto defendant's land and consumed poisonous fertilizer). Just as the landowner would not be liable for negligently killing the bees, so also would the Wi-Fi operator not be liable for negligently spreading a computer virus. See id.

150. See Klaus, supra note 41; see generally discussion supra note 56.
151. See Klaus, supra note 41; Kumagai, supra note 8; Linksys White Paper, supra note 42.
152. Protecting a computer from receiving a virus through a local network requires a unique type of computer firewall that is unlike a firewall designed to protect against viruses received through the Internet. See Hines, supra note 7 (encouraging Wi-Fi users to institute firewalls specifically designed for protecting viruses from spreading among network users); Tyson, supra note 57 ("A firewall is simply a program or hardware device that filters the information coming through the Internet connection into your private network or computer system.").
154. Id. § 218 cmt. h, at 422.
work.\textsuperscript{155} A delay in data transmission may result from the neighbor’s use of the router, but that router is performing as optimally efficient as it is capable of performing.\textsuperscript{156} There is no physical impairment. With respect to the second harm, disseminating computer viruses through a router does not damage the physical condition of the router.\textsuperscript{157} The viruses pass through the router, but they do not actually harm the functionality of the router.\textsuperscript{158} During and after the transmission of a computer virus through a router, the router performs just as it did prior to the virus transmission. It continues to send and receive data in an efficient manner. Thus, neither delaying a Wi-Fi operator’s data transmission nor transmitting a virus through the router results in physical impairment of the router.

Admittedly, the neighbor’s conduct does not physically impair the router. This fact, however, does not imply that the neighbor has not committed a trespass.\textsuperscript{159} A harmful trespass to chattel may occur when an actor temporarily deprives another of the ability to use a chattel, even where the chattel is not physically impaired or where the actor does not physically dispossess the chattel from the owner.\textsuperscript{160} For example, locking a car owner’s keys in the car deprives the owner of the car’s use, although the car owner is not physically dispossessed of the car. Liability for such deprivation of use requires that the time period of deprivation be so substantial that it is possible to estimate


\textsuperscript{156} See id.


\textsuperscript{158} See id.

\textsuperscript{159} See \textsc{Restatement of Torts} § 218(c) & cmt. i, at 420, 423 (stating that harmful contact may occur where the chattel owner is deprived of the chattel’s use).

\textsuperscript{160} Id. The argument against finding a trespass because no physical impairment is present is also flawed for another reason. Physical impairment is not absolutely required for an intermeddling to be actionable. According to the \textit{Restatement}, it is possible that “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.” \textit{Id.} § 218 cmt. h, at 422. For instance, a person who wears another’s lingerie, or who brushes the person’s own teeth with another’s toothbrush, commits a trespass to chattel even though the chattel remains physically unimpaired. \textit{Id.} The lingerie and toothbrush owner could sell their respective chattels for the same price as they could before the actor intermeddled with the chattels, yet from their standpoint, the their chattels have decreased in value. Value arises from the fact that no one else makes use of them, even though the chattels function properly. Although the router is not the same sort of chattel as lingerie or a toothbrush, it seems that value lies in the fact that the neighbor does not joyride on the router. Under the lingerie–toothbrush rationale, a court could find that the neighbor’s intermeddling is trespassory without finding that physical contact occurred. See \textit{id.}
the loss caused by that deprivation. In the car example, if the car owner were deprived of using the car for a mere hour, trespass to chattel would lie according to the Restatement.

The two harms that could result from the neighbor's intermeddling with the router appear to deprive the Wi-Fi operator of the router's use in a manner sufficient to impose trespassory liability. The delay that the Wi-Fi operator experiences because of the neighbor's joyriding demonstrates that the Wi-Fi operator is unable to use the full capacity of the router. Assuming that this delay occurs for a sufficient time period, e.g., an hour, the deprivation of use would give rise to a trespass. Similarly, a computer virus that the Wi-Fi operator receives through the router demonstrates that the Wi-Fi operator is unable to use the router without inhibition, i.e., connecting to the Internet without receiving viruses from other computers within the wireless network. The Wi-Fi operator is deprived of realizing full use of the router. As infinitesimally short as the time period is in which the virus passes through a router, the time period would nevertheless be of a sufficient duration to be actionable because the harm would be calculable. Thus, the Wi-Fi operator cannot make full use of the router where the two harms occur.

That the Wi-Fi operator can still make a partial use of the router while the neighbor is joyriding should not affect the conclusion that actionable harm occurs. In effect, the two possible harms represent trespasses on two "sticks" within the Wi-Fi operator's "bundle of sticks." Although the Wi-Fi operator can exercise other property uses in the router, the Wi-Fi operator cannot exercise every use. Disabling a chattel owner's ability to exercise only some uses over the chattel—rather than all uses—results in a trespass to chattel, whereas disabling a chattel owner's ability to exercise all rights results in conversion. It is this distinction between disabling a portion of property rights in a chattel and disabling all property rights in a chattel that gives rise to the two different causes of action. As one com-

---

161. See id. § 218 cmt. i, at 423.
162. Id. illus. 4.
163. See id.
164. Id. § 218 cmt. i, at 423 ("The deprivation of use, not amounting to a dispossession, necessary to render the actor liable for his use or other intermeddling with the chattel of another without the other's consent must be for a time so substantial that it is possible to estimate the loss caused thereby.").
165. See Cribbet et al., supra note 75, at 2 ("It appears, then, that 'ownership' consists of many disparate claims [with respect to one chattel] sanctioned by law against many persons—a 'bundle of sticks,' as legal scholars sometimes have put it.").
166. See W. Page Keeton et al., supra note 87, § 14, at 85–86 (describing trespass to chattel as interferences "which are not sufficiently important to be classed as conversion").
167. See id.
mentator notes, trespass to chattel is the little brother to conversion. Hence, the fact that the Wi-Fi operator is still able to exercise some property rights in the router does not detract from the argument that a trespass lies. The fact is consistent with the doctrine of trespass to chattel.

b. Harmless Intermeddling with the Router

The two harms described above—delay in data transmission and dissemination of viruses—appear to satisfy the requirement for harm under the tort of trespass to chattel. But a neighbor can joyride without either of these harms occurring. The Wi-Fi operator would not notice any delay in the speed of data transmission if the neighbor uses the Wi-Fi router merely to view websites or to check e-mail. Nor would the router be a means for transmitting viruses if the neighbor's computer is not infected with one. Seemingly harmless intermeddling could therefore result from joyriding.

Despite the doctrine that harmless intermeddling does not produce an actionable trespass to chattel, a strong argument can be made that an exception to this general doctrine should exist where the intermeddling occurs in cyberspace. Support for such an exception arises in caselaw. In the context of cyberspace, courts have not always

168. Id.
169. See id.; eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058, 1071 (N.D. Cal. 2000) (finding harm based on the fact that defendant had deprived plaintiff "of the ability to use [a] portion of its personal property for its own purposes") (emphasis added).
170. The point that not every use must be disabled for a trespass to occur is illustrated by the following example. Consider someone who intentionally disengages a spark plug from another's car so that the car performs poorly. The car is not permanently damaged by disengaging the spark plug. The car owner can still speed on a highway, open the sunroof, listen to its radio, stop at a light, and perform nearly every other use of the car. Nevertheless, the car owner cannot run the engine at its most efficient level in the absence of the spark plug. That is, the car owner cannot realize one possible use of the car—driving the car with all spark plugs. During the time that the spark plug is disengaged, the car owner is deprived of making full use of the car. The value temporarily decreases. Trespass to chattel lies.
171. See discussion supra subsection III.B.2.a.
172. Hale, supra note 7, at 554.
173. Id.
adhered to the requirement that there must be actual harm for an actionable trespass to chattel to lie.\textsuperscript{176} Bidder's Edge is a good example.\textsuperscript{177} There, the bot device that Bidder's Edge used to search eBay's website consumed approximately one percent of eBay's server capacity.\textsuperscript{178} Consequently, the bot did not detract from eBay's ability to meet the needs of all other Internet users who accessed its website.\textsuperscript{179} The court, however, held that Bidder's Edge caused eBay harm because the bot "consume[d] at least a portion of [eBay's] bandwidth and server capacity."\textsuperscript{180} Recognizing that the level of bandwidth that Bidder's Edge consumed did not actually pose any harm to eBay, the court reasoned that if that activity were permissible, then the activity could increase, and in the aggregate, the activity could harm eBay.\textsuperscript{181} While admitting that there was no actual harm, the court found the harm requirement of trespass to chattel to be satisfied.\textsuperscript{182}

Bidder's Edge does not stand alone in judicial softening of the harm requirement. In Register.com the court contemplated the same facts as those present in Bidder's Edge.\textsuperscript{183} As in Bidder's Edge, the Register.com court found an actionable harm based on the defendant's use of automated software that searched a website.\textsuperscript{184} The court opined that the "possibility" of harm to the plaintiff's server capacity was sufficient to satisfy the harm requirement under trespass to chattel.\textsuperscript{185} Similarly, in CompuServe, the court held that the mass e-mail that the defendants had sent through the ISP produced actionable harm because the e-mail placed a "demand" on disk space and processing power, which resources could have otherwise been available for

\begin{thebibliography}{99}
\bibitem{176} See cases cited supra note 175; cf. Restatement of Torts § 218 cmt. e, at 421–22 (requiring harm for trespass to chattel to lie).
\bibitem{177} Bidder's Edge, 100 F. Supp. 2d at 1071.
\bibitem{178} Id. at 1064.
\bibitem{179} See id. at 1071 (discounting defendant's argument that website searches represented "a negligible load on plaintiff's computer systems" because the searches deprived plaintiff of an ability to use a portion of personal property).
\bibitem{180} Id. (emphasis added).
\bibitem{181} Id. at 1066, 1071. The court attempted to portray its discourse on harm as consistent with trespass jurisprudence. See id. at 1071. The flaw in its reasoning is apparent, however. Initially, the court relied on the true premise that the law does not recognize a right to commit a harmless intermeddling. Id. From that premise, the court faultily concluded that harmless intermeddling is actionable. Id. The fact that the law does not recognize a right to commit harmless intermeddling does not imply that the law condemns harmless intermeddling. Despite the court's ostensible attempt to cram its holding into the well established jurisprudence of tort law, it failed. The court introduced an exception to the rule—not a consistency.
\bibitem{182} Id. at 1066, 1071.
\bibitem{184} Id. at 249–50.
\bibitem{185} Id. at 250.
\end{thebibliography}
ISP customers.\textsuperscript{186} That demand, however, did not detract from the capability of the ISP's computer equipment to function properly.\textsuperscript{187} Indeed, any single e-mail results in a demand of disk space and processing power.\textsuperscript{188} The mass e-mails did not deter the ISP's ability to facilitate Internet traffic; instead, the e-mails merely invoked that ability.\textsuperscript{189}

These cases suggest that in the context of determining whether electronic trespass exists on the Internet, the harm necessary for an actionable trespass need only be minimal in nature. Courts have looked to the potential for harm, rather than actual harm, in deciding whether the harm element is satisfied in cyberspace.\textsuperscript{190} An electronic signal is harmful when it could affect the performance of the physical object at issue if the signal were duplicated in the aggregate.\textsuperscript{191}

One case that implicitly supports this interpretation of these cases is \textit{Intel Corp. v. Hamidi}.\textsuperscript{192} There, the California Supreme Court considered whether a trespass to chattel occurred when the defendant sent e-mails critical of his former employer, Intel, to current Intel employees.\textsuperscript{193} The court held that the tort did not lie because the alleged harm stemmed from the content of the e-mails, rather than an injury to the functionality of Intel's computer system.\textsuperscript{194} In its analysis, the court distinguished \textit{Bidder's Edge, Register.com,} and \textit{CompuServe} on the grounds that those cases dealt with either actual or "threatened" harm, whereas the defendant's e-mails neither actually harmed nor threatened to harm his employer's computer system.\textsuperscript{195} The \textit{Hamidi} decision therefore implicitly endorses the potential-for-harm rationale set forth in the above cases.\textsuperscript{196}

Also notable in \textit{Hamidi} is the fact that Intel argued that the e-mails caused harm in the form of economic damage.\textsuperscript{197} The Intel employees, Intel alleged, were distracted by the content of the e-mails,

\begin{flushright}
\textsuperscript{187} See id. at 1022.
\textsuperscript{189} See \textit{CompuServe}, 962 F. Supp. at 1022.
\textsuperscript{190} See cases cited supra note 175.
\textsuperscript{191} See eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058, 1066 (N.D. Cal. 2000) ("If [defendant's] activity is allowed to continue unchecked, it would encourage other auction aggregators to engage in similar recursive searching of the eBay system such that eBay would suffer irreparable harm from reduced system performance, system unavailability, or data losses.").
\textsuperscript{192} 71 P.3d 296 (Cal. 2003).
\textsuperscript{193} Id. at 299–300.
\textsuperscript{194} Id. at 303–04.
\textsuperscript{195} Id. at 304–06.
\textsuperscript{196} See id.
\textsuperscript{197} Id. at 307–08.
\end{flushright}
causing Intel to incur loss of productivity. The Hamidi court rejected this argument, holding that economic damages did not satisfy the harm requirement of trespass to chattel. The tort required the harm to be directly to the chattel. Thus, consequential business-related damages appear to be neither sufficient nor necessary for trespass to chattel to lie in the context of sending electronic signals over the Internet.

According to this recent Internet jurisprudence, the radio signals that a joyriding neighbor sends to a Wi-Fi operator's router appear to constitute trespassory harm. As Bidder's Edge, Register.com, and CompuServe suggest, the potential for physical harm that an electronic signal poses to computer equipment appears sufficient to satisfy the harm requirement. The fact that the harm does not cause consequential economic damage to the owner of the computer equipment should not, according to Hamidi, affect the trespassory analysis. These general principles imply that the electronic signal which the neighbor causes to contact the Wi-Fi operator's router is sufficient to constitute trespassory harm. Although the neighbor's signal may not drain the router's capacity, if duplicated in the aggregate the signals would.

Tellingly, courts have remained silent as to why they have softened the harm requirement for a trespass to chattel arising in cyber-space. Their silence suggests that policy concerns outweigh the value of an antiquated tort doctrine. At the outset of the Internet, uncertainty as to how the law would treat the new electronic medium threatened to hamper its commercial viability. Faced with a promising new medium of exchange, and likely noting its relatively infantile stage, courts delivered the needed certainty. Courts provided market participants certainty that their Internet investments were

198. Id. at 299–300.
199. Id. at 300.
200. See id.
201. See id.
202. See cases cited supra note 175.
203. See Hamidi, 71 P.3d at 300.
204. Hale, supra note 7, at 547.
205. See cases cited supra note 175.
206. See Quilter, supra note 88, at 435–36 (arguing that courts have incorrectly applied trespass to chattel to deal with public annoyances on the Internet).
207. See Daniel Dern, Meeting the Challenges of Business and End-User Communities on the Internet: What They Want, What They Need, What They're Doing, in PUBLIC ACCESS TO THE INTERNET 212–13 (Brian Kahin & James Keller eds., 1996) (explaining, at the time that the Internet was initially becoming commercial, that commercial Internet users seek “[a]ccountability and clear problem-resolution paths”).
well protected, and they did so even before any harm occurred.\footnote{See, e.g., eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058, 1066–72 (N.D. Cal. 2000).} Confidence in the new intangible, commercial medium could not be sacrificed at the expense of upholding a doctrine that was crafted for problems arising in the disparate realm of the physical. The policy of promoting and protecting valuable benefits of the Internet prevailed over a principle established for a wholly distinct ontology.

This policy of liberally protecting Internet investors strengthens the argument that a joyriding neighbor has acted tortiously. Because the neighbor can access a wireless network at no cost, the neighbor is neither likely to purchase a Wi-Fi router nor likely to purchase the services of an ISP. It seems likely that at least some joyriding neighbors value the Wi-Fi connection at a level equal to or greater than the cost of ISP services or of a Wi-Fi router.\footnote{This conclusion seems likely given that the neighbor must purchase a wireless network adapter to interface with the wireless network. \textit{See} discussion supra Part II. A wireless network adapter costs approximately seventy dollars. \textit{See} Best Buy, http://www.bestbuy.com/site/olspage.jsp?navLevel=4&type=category&navHistory=cat00000%2Bcat01000%2Bcat01024&id=cat01032 (last visited Jan. 6, 2006) (displaying retail of price of 802.11g Wireless Notebook Card to be $70.99).} Assuming that this is true, these joyriding neighbors would purchase ISP services and Wi-Fi routers if they were not provided the opportunity to access the Internet through Wi-Fi operators' networks. ISPs and manufacturers of Wi-Fi routers are therefore not realizing a complete economic return on their investment in Internet technology.\footnote{Kern, \textit{supra} note 2, at 110 (discussing the detrimental effect that free-riding users of a wireless network have on the capacity and infrastructure of an ISP).} Prohibiting joyriding would ensure that they are rewarded for their investment.

The upshot of this discussion about the seemingly harmless nature of Wi-Fi joyriding is that the joyriding does result in a harm, but on a macro level. Judicial holdings dealing with equipment that facilitates Internet activity seem to indicate that if the conduct at issue would produce harm were it duplicated in the aggregate, then the harm requirement is satisfied.\footnote{See \textit{Bidder's Edge}, 100 F. Supp. 2d at 1066 ("If [defendant's] activity is allowed to continue unchecked, it would encourage other auction aggregators to engage in similar recursive searching of the eBay system such that eBay would suffer irreparable harm from reduced system performance, system unavailability, or data losses.").} Those holdings also implicitly indicate that protecting participants of Internet-based technology is sufficient reason to find actionable harm where a single instance of intermeddling could produce harm if duplicated en masse.\footnote{See cases cited \textit{supra} note 175.} In short, there appears to be room in cyberspace to carve out an exception to the requirement that the chattel owner experience actual harm. And Wi-Fi technology
should be a part of that cyberspace exception. Seemingly harmless intermeddling should be actionable.

3. Intent

The joyriding neighbor appears to satisfy the intentionality requirement of trespass to chattel. To commit a trespass to chattel, an actor must intend to commit the intermeddling contact. This means that the joyriding neighbor must intend to use another person's router. The presence of this intent is apparent. In accessing the router, the neighbor chooses a wireless network through which his or her wireless network adapter can interface. By selecting the Wi-Fi operator's network from a computer prompt, the neighbor affirmatively demonstrates an intent to use another person's router. The neighbor's intentional selection of the Wi-Fi operator's wireless connection demonstrates an intent to intermeddle with the router.

Two further points are worth noting about the joyriding neighbor's intent. First, the fact that the neighbor does not intend to harm the Wi-Fi operator does not affect the intent analysis. An actor need not intend to commit the harm that results from an intermeddling; the intent requirement is satisfied even where the actor acts under a mistake of fact. A harmful intermeddling is not excused on the basis that the actor believed that the intermeddling would not be harmful. Accordingly, the neighbor's intent to access the Internet through the router is sufficient to satisfy the intent requirement. That the neighbor does not intend to slow down the data transmission for the Wi-Fi operator, to spread a virus to the Wi-Fi operator, or to impede the market for ISP service should not affect whether the neighbor satisfies the intent requirement.

214. See id.
215. See cases cited supra note 175.
216. A third point is also noteworthy. The intent requirement distinguishes the neighbor's tortious conduct from the harmless conduct of other wireless-device users. See discussion supra subsection III.B.1.b (discussing the distinction between electrical devices that cause harmless intermeddling and those which do not). No cause of action lies against parents who operate baby monitors that happen to interfere with the performance of another's Wi-Fi router. See Restatement of Torts § 217 cmt. c, at 418. Nor is there a cause of action against cordless phone users. See id. Presumably, a person who uses these wireless devices does not intend to intermeddle with another person's use of a wireless device.
217. See Restatement of Torts § 217 cmt. c, at 418 ("[I]t is immaterial that the actor intermeddles with the chattel under a mistake of law or fact that the possessor has consented to his dealing with it.").
218. Id.
219. See id. It should be noted that one commentator has voiced a contrary view. See Kern, supra note 2, at 155. Without relying on any authority, he states: "The intent component of [trespass to chattel] requires that a roaming [Wi-Fi] user
Second, assuming that the neighbor does not know the identity of the Wi-Fi operator, such that the neighbor knows only that the Wi-Fi router belongs to some other person, the intent requirement is still satisfied. Intermeddling is present even if the actor does not know the identity of the chattel owner. Throwing a baseball at a car satisfies the intent requirement of trespass to chattel, even where the car owner is unknown to the thrower. Likewise, accessing the Internet through a wireless network that does not belong to the neighbor satisfies the intent requirement, even where the identity of the Wi-Fi operator is unknown to the neighbor. It is sufficient that the joyriding neighbor knows that the Wi-Fi connection is not his or her own.

IV. DEFENSES OF TRESPASS TO CHATTEL APPLIED TO WI-FI JOYRIDING

A joyriding neighbor could argue two defenses to the trespass to chattel claim. The first is that the Wi-Fi operator has consented to the joyriding by failing to password protect the router from unauthorized use. The second is that joyriding constitutes a permissible means for the neighbor to abate a nuisance that the Wi-Fi operator creates—hogging the wireless spectra. Neither defense should prevail. Each is discussed below.

A. The Wi-Fi Operator's Seeming Consent to Joyriding

A joyriding neighbor could argue that joyriding is permissible because the Wi-Fi operator has failed to implement security measures which would preclude the neighbor from accessing the router. A person who consents to otherwise tortious conduct cannot recover against the actor. Consent may be manifest by action or inaction, and need not be communicated to the actor. When a person's silence would be reasonably understood as intended to indicate consent, that silence is a manifestation of apparent consent.

---

220. See Restatement of Torts § 217 cmt. c, at 418. ([A]n intention is present when an act is done for the purpose of using or otherwise intermeddling with a chattel . . . . ).
221. See discussion infra section IV.A.
222. See discussion infra section IV.B.
223. See Restatement of Torts § 892A, at 364 ("One who effectively consents to conduct of another intended to invade his interests cannot recover in an action of tort for the conduct or for harm resulting from it.").
224. Id. § 892, at 362 ("[C]onsent may be manifested by action or inaction and need not be communicated to the actor.").
225. Id. § 892 cmt. c, at 363 (explaining "apparent consent").
The neighbor's consent argument is based solely on the fact that the Wi-Fi operator fails to implement a password so that others cannot access the Internet through the router. The argument effectively implies that anyone should be permitted to access a wireless network unless the Wi-Fi operator institutes security measures. The argument draws support from cyberspace jurisprudence. In *EF Cultural Travel BV v. Zefer Corp.*, the First Circuit considered whether a website owner had provided consent for the defendant to use automated software to search its website. The court concluded that because the website owner had not expressly restricted the use of the website, the owner had implicitly consented to the defendant's conduct. In dicta, the court commented that a lack of consent can be manifest by the presence of password protection.

Other courts have considered the issue of consent. In *CompuServe*, the court opined that the ISP provided "tacit" consent for anyone on the Internet to send e-mail to its subscribers, but that the ISP had affirmatively revoked its consent to the defendants. The basis for this finding of "tacit" consent was that the ISP had created a system for allowing anyone on the Internet to e-mail its subscribers. In other words, consent was based on the fact that the ISP system was designed for the purpose of allowing anyone on the Internet to send e-mails to subscribers.

The *Bidder's Edge* court also opined on the doctrine of consent. The court held that eBay had granted "conditional" consent to Internet users to access its website. The consent was granted upon an express condition on its website stating that users were not to use robotic data-collection devices on its site. In other words, a presumption of consent existed, and eBay acted to limit that presumption. Restriction of website access was obtained by making a

---

227. 318 F.3d 58, 60, 62–63 (1st Cir. 2003).
228. *Id.* at 60, 62–63.
229. *Id.* at 63. The court actually held that the owner had "authorized" the conduct, rather than "consented" to the conduct. *Id.*
230. *Id.* ("[P]assword protection itself normally limits authorization by implication (and technology), even without express terms.").
232. *Id.* at 1023.
233. *Id.* at 1023–24.
235. *Id.*
236. *Id.* at 1060, 1070.
237. See *id.*
statement on the website, implicitly suggesting that a presumption of consent did exist.²³⁸ Relying on these cases, the joyriding neighbor could argue that the absence of any password protection by the Wi-Fi operator implies that the Wi-Fi operator consents to anyone using the router. Zefer seems to imply that the absence of password protection denotes consent to use property in cyberspace.²³⁹ Further, like the ISP in CompuServe, a Wi-Fi operator creates a system specifically designed to allow anyone within its range to access the Internet.²⁴⁰ Because the very function of the Wi-Fi connection is to provide any person within its physical range access to the Internet, that function arguably creates a presumption that the Wi-Fi operator consents to anyone accessing the Internet through the router.²⁴¹ Finally, just as the website owner in Bidder's Edge could easily restrict the presumption that anyone could access the owner's website,²⁴² the Wi-Fi operator can easily restrict the presumption that anyone can use the Wi-Fi operator's router: the Wi-Fi operator need merely set up a password.²⁴³ By failing to implement a password, the Wi-Fi operator seems to assume the risk of Wi-Fi joyriding.

Despite these arguments in favor of construing the Wi-Fi operator's failure to implement a password as implicit consent for others to joyride, such a presumption should not exist. As an initial matter, Zefer's statement that a password denotes an absence of consent does not imply that an absence of a password denotes consent.²⁴⁴ An analogy may illustrate the disconnect between these propositions. Consider a bicycle owner. If the owner locks the bicycle, the lock demonstrates that the owner does not consent to another person's use of the bicycle. But if the owner does not lock the bicycle, this does not imply that the owner consents to another's use of the bicycle. It is entirely possible that the bicycle owner does not lock the bicycle because the owner has trouble remembering combinations, or perhaps disdains spending time entering combinations to unlock property. Analogously, the absence of a password on a wireless network does not imply that the Wi-Fi operator consents to another's use of the router. That absence implies nothing more than the fact that the Wi-Fi operator chooses not to implement a password. Perhaps the Wi-Fi operator disdains having to spend time entering a password each time the oper-

²³⁸. See id. This fact also influenced the court in EF Cultural Travel BV v. Zefer Corp., 318 F.3d 58, 63 (1st Cir. 2003).
²³⁹. See Zefer, 318 F.3d at 63.
²⁴¹. See id.
²⁴². See Bidder's Edge, 100 F. Supp. at 1070.
²⁴³. See Kern, supra note 2, at 155–56.
²⁴⁴. See Zefer, 318 F.3d at 63.
ator accesses the Internet, or perhaps the owner simply has a bad memory for remembering passwords. Failure to install protective devices so that another cannot use property does not imply that a property owner consents to the use. Hence, Zefer's observation that the presence of a password implies the absence of consent should not be construed as meaning that an absence of a password implies the presence of consent.

On a more substantive level, the cited cases should not be interpreted as suggesting that a Wi-Fi operator has consented to joyriding because none of the cited cases deal with wireless networks. The fact that the consent in the cited cases was manifest by ISPs and website owners distinguishes them from the context of wireless networks. An ISP usually realizes economic benefit when Internet users make use of the ISP's services, including its e-mail service. E-mail exchange increases demand for the ISP service. Likewise, a website usually becomes more commercially valuable as more Internet users view the website. In short, the commercial model for the Internet has developed such that the conduct of e-mailing ISP subscribers and viewing websites are activities that propagate economic benefits for ISPs and website owners. For this reason, the presumption is sound that these property owners consent to otherwise trespassory contact in cyberspace.

The situation of a Wi-Fi operator is markedly different than that of an ISP or a website owner. A joyriding neighbor engages in free-riding parasitic behavior. Although the Wi-Fi operator may not necessarily be harmed by the behavior, the Wi-Fi operator does not stand to gain any economic benefit. In the absence of any possibility that the Wi-Fi operator could realize economic benefit from the neighbor accessing the Internet, the presumption that the owner has consented appears unjustified. Other than altruistic tendencies, there is no reason

245. See Kern, supra note 2, at 156 ("It is not clear that a court would use [the same test for consent as in the website trespass cases] with respect to a roaming Wi-Fi user because a wireless network may in some cases have more of a private character than a website.").

246. See, e.g., NetZero ISP, http://www.netzero.com (last visited May 15, 2006) (offering e-mail service as a benefit for Internet users who pay the ISP a fixed monthly fee).

247. See, e.g., Earthlink ISP, http://www.earthlink.net/membercenter/benefits/ (last visited May 15, 2006) (listing the ability to exchange e-mail as a benefit that Internet users realize when subscribing to the ISP service).


that a Wi-Fi operator would consent to joyriding. Presuming consent would be imposing a choice where the Wi-Fi operator was unaware of the conduct and preferred not to implement a password. In the Wi-Fi context, there is no reason to create a presumption of consent based on the absence of a password.

The absence of password protection also does not denote an assumption of risk that excuses the joyriding neighbor's conduct. It is true that by not implementing a password the Wi-Fi operator assumes the risk that a neighbor will joyride. But that fact does not excuse the neighbor's conduct. Assumption of risk is relevant in examining only a claim of negligence. The inquiry at hand is one of intentional tort. As much as a chattel owner may put at risk the safety of a chattel, if an actor commits an intentional trespass on the chattel without the owner's consent, the actor is still liable. Assumption of risk is not a defense to intentional tort. Consider a china-shop owner who invites a bull owner to shop at the china shop—with the bull. Unquestionably the china-shop owner assumes a great risk in extending that invitation. Yet if after walking into the china shop with the bull, the bull owner strikes the bull intending for the bull to destroy all the china, the bull owner is still liable for the resultant damage. That the china-shop owner places at risk all the china by allowing the bull to enter the shop is of no consequence. The intentional act of the bull owner creates tortious liability. Similar to the china-shop owner, the Wi-Fi operator places at risk the router's use. That risk is of no consequence because the joyriding neighbor intentionally acts to interfere with the Wi-Fi router. The intent is dispositive.

It should lastly be noted that the Wi-Fi operator's failure to password protect the network is not akin to establishing consent through

250. See Gates v. Navy, 617 S.E.2d 163, 167 (Ga. App. 2005) ("It is well-settled that the defenses of . . . assumption of the risk and contributory negligence are not valid defenses to intentional, wilful, or wanton and reckless torts . . . .") (internal citations omitted); see generally W. PAGE KEETON ET AL., supra note 87, § 68, at 480-98 (discussing assumption of risk in context of negligence defenses).

251. See discussion supra Part III.

252. Gates, 617 S.E.2d at 167; see also W. PAGE KEETON ET AL., supra note 87, § 18, at 113 ("The mere fact that one is willing to incur a risk that conduct in deliberate violation of the rules of a sporting contest will be committed does not mean that one is willing for such conduct to be committed.").


254. See id.

255. The bull-in-the-china-shop example is by no means completely analogous to the Wi-Fi scenario under consideration. The narrative is cited only for the general proposition that assumption of risk is no defense to an intentional tort, and nothing more than that. Unlike the bull owner, the joyriding neighbor presumably does not intentionally slow down the router or transmit a virus through the router. That difference does not detract from the inference drawn from the bull narrative: assumption of risk is not a defense to an intentional tort.
silence. Silence or inaction can denote consent, but only where the chattel owner has knowledge of the actor using the chattel.\textsuperscript{256} Silence or inaction does not denote consent where the actor is oblivious to the trespassory conduct.\textsuperscript{257} Accordingly, failure to password protect a wireless network could possibly be viewed as consent through silence only if the Wi-Fi operator were aware of the conduct prior to choosing not to password protect the network. The Wi-Fi operator’s inaction is not consent unless the Wi-Fi operator is aware of the tortious conduct.\textsuperscript{258} But even then, a single oral objection to the use would preclude the possibility that the Wi-Fi operator consents where the Wi-Fi operator has not password protected the network.\textsuperscript{259} Fences and locks are not necessary to show that a property owner does not consent to another’s use of the property.\textsuperscript{260} A simple, one-time oral communication should suffice.

B. The Joyriding Neighbor’s Seeming Abatement to a Wi-Fi Nuisance

Another defense that the neighbor could argue is that joyriding is permissible under the abatement-of-nuisance doctrine.\textsuperscript{261} The common law permits an actor to commit an act which would otherwise be a trespass to chattel when the act is committed for the purpose of abating a private nuisance that is caused by the chattel owner.\textsuperscript{262} A private nuisance occurs where there is interference with a land-
owner’s private use and enjoyment of land.\textsuperscript{263} Abatement of the nuisance is permissible to the extent that the abatement is considered reasonable.\textsuperscript{264} For instance, courts have considered it reasonable for a neighbor to cut tree branches which were overhanging into the airspace over the neighbor’s land.\textsuperscript{265}

The joyriding neighbor could argue that the Wi-Fi operator is causing a nuisance on the neighbor’s property. There are a limited number of channels within the bandwidth frequencies on which Wi-Fi radio signals can exist.\textsuperscript{266} By operating a wireless network, then, the Wi-Fi operator causes a shortage of channels on which the neighbor could operate a wireless network or other wireless device. The neighbor cannot set up his or her own wireless network because someone else is hogging the band. In other words, the neighbor cannot enjoy the use of the radio signals on the airspace over the land, so a nuisance seems arguably present.

After arguing that the Wi-Fi operator is causing a nuisance, the joyriding neighbor could further argue that a reasonable abatement of this nuisance would be to make use of the wireless network. By using the Wi-Fi operator’s network, the neighbor abates the harm that the Wi-Fi operator has created. A shortage of bandwidth is of no concern to a neighbor seeking wireless Internet access if the neighbor can access the Internet through Wi-Fi radio signals that are already present in the airspace over the neighbor’s land. Thus, the neighbor could argue that the otherwise tortious conduct of joyriding is excused based on the neighbor’s abatement of the Wi-Fi operator’s nuisance.\textsuperscript{267}

This abatement-of-nuisance argument would not likely succeed. To begin with, nuisance claims relating to radio-frequency interference are preempted by the Federal Communications Act ("FCA").\textsuperscript{268} The FCA contains no provision that would prohibit a person from us-

\textsuperscript{263} Id. § 821D, at 100 ("A private nuisance is a nontrespassory invasion of another’s interest in the private use and enjoyment of land.").
\textsuperscript{264} 66 C.J.S. Nuisances § 89, at 635 (1998).
\textsuperscript{265} Hickey v. Mich. Cent. R.R. Co., 55 N.W. 989, 990–91 (Mich. 1893); see also 66 C.J.S. Nuisances § 87, at 634 ("It has been held that the person aggrieved may cut off branches of a neighbor’s trees overhanging his land, remove a part of an adjoining owner’s wall which overhangs his premises, or cut off the eaves of a building overhanging his property.").
\textsuperscript{266} See Klaus, supra note 41; Linksys White Paper, supra note 42, at 6.
\textsuperscript{267} See RESTATEMENT OF TORTS § 264, at 498 (outlining the abatement-of-nuisance defense to trespass to chattel).
ing all possible frequencies on an unlicensed bandwidth. It would not likely apply. Because preemption precludes the neighbor from raising a nuisance claim, and because the FCA does not likely apply in that situation, the neighbor cannot likely raise this nuisance-abatement argument.

Assuming arguendo that the neighbor could raise the nuisance-abatement argument, it would be highly unusual that abatement would be permissible. Abatement is permissible only in situations of extreme or urgent necessity. The complained-of nuisance must actually exist. In the Wi-Fi context, then, abatement would be permissible only if the Wi-Fi operator were causing a shortage of channels on the unlicensed frequencies, and only if the neighbor actually unsuccessfully attempted to access the Internet using his or her own Wi-Fi equipment and ISP. This situation is highly unlikely. As an initial matter, two wireless networks are capable of coexisting within the same close proximity. Crowding out a wireless network would occur only if multiple other wireless devices were also in operation in the same close proximity. The circumstance of close proximity suggests that those other wireless devices crowding out the neighbor's wireless network would likely belong to the neighbor. If the neighbor need merely stop using his or her microwave oven to operate the wireless network, the complained-of nuisance would not appear to be "extreme." Abatement would not be permissible.


270. The FCA grants the FCC authority to regulate bandwidths. See id. § 303. A requirement for operating a device on unlicensed frequencies is that the operator must accept interference. See 47 C.F.R. § 15.5(b) (2004). Thus, insofar as a device satisfies technical specifications, the FCC appears to permit interference that such devices may cause within the unlicensed bandwidth. See 47 U.S.C. § 333; Ellen P. Goodman, Spectrum Rights in the Telecosm To Come, 41 SAN DIEGO L. REV. 269, 287-88 (2004) ("[T]he FCC has opened the bands for low-power transmissions by operators or members of the public without mandating licensing or coordination. The only requirement is that the equipment used in these unlicensed bands must satisfy certain technical specifications.").


272. See Hewlett Packard, Wi-Fi and Bluetooth—Interference Issues, at 1 (Jan. 2002), available at http://www.hp.com/rnd/library/pdf/WiFi_Bluetooth_coexistence.pdf ("Only in extreme conditions, such as setting a Bluetooth-enabled cell phone down next to an operating microwave oven, is it likely that communications will cease altogether.").

273. See id. at 2 ("[T]here can be no more than three different Wi-Fi networks operating in close proximity to one another.").

274. See 66 C.J.S. Nuisances § 89, at 635 (stating that abatement is permissible only in instances of "extreme" or "urgent" necessity).

275. See id.
Even more important in the abatement analysis is the fact that joyriding is not usually the result of the posited circumstances. Joyriding does not usually occur after a neighbor has subscribed to ISP services, has purchased a Wi-Fi router, and then has unsuccessfully attempted to connect to the ISP using that Wi-Fi router. Neighbors do not joyride because they are unsuccessful at operating their own Wi-Fi connection; they joyride to avoid paying ISP fees. The facts necessary to support a nuisance-abatement argument are simply implausible.  

V. CONCLUSION

The seemingly harmless conduct of accessing the Internet through another's wireless network without authorization should be deemed tortious. Joyriding should result in an actionable trespass to chattel. A joyriding neighbor appears to trespass on the Wi-Fi operator's router. When the neighbor sends electronic signals through the router to access the Internet, those signals produce a physical effect on the router that is sufficient to be deemed trespassory physical conduct. The neighbor intentionally causes this contact, thereby satisfying the intentionality requirement for trespass. Harm may also be present. The Wi-Fi operator may experience delayed Internet transmission or receive viruses from the joyriding neighbor. Yet even if neither of these harms are present, a strong argument exists that the joyriding neighbor should still be liable. Recent Internet jurisprudence suggests that using another's computer equipment to access the Internet results in a trespass to chattel, regardless of whether that access results in actual harm. In an effort to thwart the negative externality that joyriding causes ISPs and manufactur-

279. Assuming arguendo that these facts did exist, joyriding does not appear a reasonable means for abating the nuisance. To be excused for an action of trespass, an actor must reasonably believe that a demand on the chattel owner to cease the nuisance would be impractical or useless. RESTATEMENT OF TORTS § 264, at 498 (1958). A more reasonable method of abatement would be for the neighbor simply to request that the Wi-Fi operator either physically relocate or cease using any one of the many wireless devices creating the shortage. Given that the Wi-Fi operator prefers that the neighbor not joyride, the Wi-Fi operator would likely acquiesce to such a request. This method of abatement—the simple request—appears more reasonable than joyriding because it would not subject the Wi-Fi operator to the potential harms discussed above. See discussion supra subsection III.B.2.

280. See discussion supra section III.A.
281. See discussion supra subsection III.B.1.
282. See discussion supra subsection III.B.3.
283. See discussion supra subsection III.B.2.a.
284. See discussion supra subsection III.B.2.a.
285. See discussion supra subsection III.B.2.b.
286. See cases cited supra note 175.
ers of Wi-Fi routers, courts would likely view the joyriding neighbor’s conduct as tortious.287

A joyriding neighbor would not likely prevail in arguing defenses against the trespass claim.288 One arguable defense is that the Wi-Fi operator implicitly consents to the neighbor's conduct when the Wi-Fi operator fails to implement security measures such as a password.289 Yet the fact that a Wi-Fi operator may not implement a password to protect access to the network should not be interpreted as consent to the neighbor's conduct.290 The Wi-Fi operator's failure to implement password protections is akin to any physical property owner failing to secure his or her property with a lock.291 Failure to secure property does not denote consent.292 Nor does the fact that the Wi-Fi operator places the network at risk of a neighbor accessing it imply that the neighbor's act is excused.293 Assumption of risk is no defense to an intentional tort.294 It is also noteworthy that the Wi-Fi operator has no economic incentive to allow the neighbor access to the network.295 In the absence of an economic benefit for the Wi-Fi operator, there is no reason to presume that the Wi-Fi operator would condone joyriding.296

Another arguable defense is that joyriding is a permissible abatement of an actionable nuisance.297 That nuisance arguably consists of the detriment that the wireless network causes to the neighbor's capability of setting up his or her own wireless network.298 This argument would not likely succeed.299 Nuisance claims arising from radio frequency interference are preempted by federal law under the FCA, and the FCA does not prohibit the interference that Wi-Fi radio signals might cause on unlicensed frequencies.300 Moreover, even if the FCA did not preempt nuisance claims, abatement is permissible only where harm actually occurs.301 Actual harm would occur only if the joyriding neighbor had first attempted to access the Internet through his or her own Wi-Fi connection, a situation which appears unlikely.302 The

287. See discussion supra subsection III.B.2.b.
288. See discussion supra Part IV.
289. See discussion supra section IV.A.
290. See discussion supra section IV.A.
291. See discussion supra section IV.A.
292. See discussion supra section IV.A.
293. See discussion supra section IV.A.
294. See discussion supra section IV.A.
295. See discussion supra section IV.A.
296. See discussion supra section IV.A.
297. See discussion supra section IV.B.
298. See discussion supra section IV.B.
299. See discussion supra section IV.B.
300. See cases cited supra note 268.
302. See discussion supra section IV.B.
joyriding neighbor would not likely prevail in arguing a defense to trespass to chattel.

Thus, Wi-Fi technology appears to introduce a new stick into the bundle of sticks that a Wi-Fi operator holds over physical property. The Wi-Fi operator should be able to control the electronic signals that are directed through his or her router. Likely an owner of an umbrella, an automobile, or a football could not preclude another person from causing electronic signals to contact their respective property. Trespass to chattel in cyberspace thereby signifies a new sort of property right, a right which emerged due to the value that the physical property has brought to the virtual world. A Wi-Fi operator should hold a unique property right in the router because of the router's capability of facilitating communication in cyberspace. For its virtual value, a physical trespass to chattel should lie.