Louisiana Law Review

Volume 69 | Number 2
*Winter 2009*

# Trespassing Through Cyberspace: Should Wireless Piggybacking Constitute a Crime or Tort Under Louisiana Law?

Grant J. Guillot

# Trespassing Through Cyberspace: Should Wireless Piggybacking Constitute a Crime or Tort Under Louisiana Law?

TABLE OF CONTENTS



## I. INTRODUCTION

Imagine sitting inside your car while it is parked in the vicinity of a coffeehouse. Awaiting several important e-mail messages, you decide to pull out your laptop computer to access an unsecured wireless network. Ten minutes later, a policeman knocks on your window and tells you to step out of the car. For reasons you do not comprehend, you are under arrest for violating a criminal statute. By accessing the coffeehouse's network as a non-paying customer, you have subjected yourself to criminal liability. You will likely be required to pay a fine or even serve time in jail. You must face these criminal ramifications despite the fact that the coffeehouse could have secured its wireless network, thereby preventing non-paying customers from accessing it.

This scenario may seem astonishing and unlikely, but it actually happened to a twenty-year-old Washington man just last

year.[1] In fact, within the past two years, in at least five states, individuals who accessed unsecured wireless networks without permission have been arrested and charged.[2] Although no such event has occurred in Louisiana, the legislature and courts of this state should anticipate that "wireless piggybacking" will become a growing concern in both the criminal and civil context.

As computerized technology continues to evolve, an increasing number of individuals and businesses utilize wireless Internet networks instead of relying on land-based connections.[3] In fact, many United States municipalities are in the process of, or have strongly considered, providing free or low-cost wireless Internet services for their residents.[4] Furthermore, most laptop computers are now manufactured with built-in wireless technology that automatically gathers a series of wireless networks from which a user can choose a connection or to which the user is immediately and involuntarily connected.[5] Although Americans continue to embrace wireless networks in increasing numbers,[6] the law governing this technology remains obscure.[7]

Wireless piggybacking, or "war driving," is the practice of "searching for a close unsecured wireless network, connecting to

---



1. Gregg Keizer, *WiFi User Charged for Not Buying Coffee*, EE TIMES ONLINE, June 22, 2006, http://www.eetimes.com/showArticle.jhtml?articleID=189600767.

2. *Id.*; Matthew Bierlein, *Policing the Wireless World: Access Liability in the Open Wi-Fi Era*, 67 OHIO ST. L.J. 1123, 1123–24 (2006); Eric Bangeman, *Illinois WiFi Freeloader Fined US$250*, ARS TECHNICA, Mar. 23, 2006, http://arstechnica.com/news.ars/post/20060323-6447.html; John Cox, *Michigan Man Fined for Using Free Wi-Fi*, NETWORK WORLD, May 23, 2007, http://www.networkworld.com/news/2007/052307-fine-using-free-wifi.html?nlhtw=0521wirelessalert2&; Andrew Wellner, *Using Free Wireless at Library Described as Theft*, ANCHORAGE DAILY NEWS, Feb. 24, 2007, http://www.adn.com/news/alaska/story/8667098p-8559268c.html.

3. Mark Jewell, *Experts: Wi-Fi Eavesdropping Persists Despite Stronger Security*, BOSTON GLOBE, Aug. 7, 2007, http://www.boston.com/news/local/massachusetts/articles/2007/08/07/experts_wi_fi_eavesdropping_persists_despite_stronger_security/.

4. Rob Lever, *U.S. Cities Wi-Fi Dreams Fading Fast*, SYDNEY MORNING HERALD, Sept. 22, 2007, http://www.smh.com.au/news/Technology/US-cities-WiFi-dreams-fading-fast/2007/09/23/1190486120402.html.

5. Marshall Brain & Tracy V. Wilson, *How Wi-Fi Works: Wifi Hotspots*, HOWSTUFFWORKS, Apr. 20, 2001, http://computer.howstuffworks.com/wireless-network2.htm.

6. Jewell, *supra* note 3.

7. Robert V. Hale II, *Wi-Fi Liability: Potential Legal Risks in Accessing and Operating Wireless Internet*, 21 SANTA CLARA COMPUTER & HIGH TECH. L.J. 543, 552 (2005).

it, and surfing the web through it."[8] Although several states and other nations have brought wireless piggybacking within the scope of their pre-existing criminal statutes,[9] none have recognized a civil remedy available to victims of wireless piggybacking. The Louisiana legal community thus far has not investigated whether wireless piggybacking constitutes a criminal offense or tort. With the ever-increasing use of the Internet and wireless technology, it is very likely that Louisiana courts will have to examine the cyberspace legal interests of the state and its Internet subscribers in the near future.

This Comment asserts that Louisiana, following in the footsteps of other states, will likely apply its criminal statutes to wireless piggybacking when faced with this issue. However, Louisiana's state courts will probably conclude that the unauthorized use of wireless networks does not fall within the scope of the state's tort laws. Given that other states have not yet applied their tort laws to wireless piggybacking, it is unlikely that Louisiana courts will choose to do so in the near future.

Part II of this Comment explores the increasing use of wireless networks, the issues raised by wireless piggybacking, and the concept of cyberproperty. Part III investigates recent multi-state and international developments regarding the unauthorized accessing of wireless networks. Part IV examines the utility of applying Louisiana's criminal statutes to wireless piggybacking while noting the issues raised by the attempted application of state tort law to this activity. Part V provides a brief conclusion.

## II. BACKGROUND

### *A. The Wireless Network Explosion*

Wireless local-area networks, also known as "wireless-fidelity" networks or "Wi-Fi" networks, allow individuals to access the Internet via "radio or infrared frequencies on the unlicensed 2.4 and 5 GHz radio bands."[10] Access to these networks is often

8. Odia Kagan, *Internet Law—Too Close for Comfort: Is it Legal to "Borrow" Wireless Internet From Your Neighbors?*, INTERNET BUSINESS LAW SERVICES, May 5, 2006, http://www.ibls.com/internet_law_news_portal_view.aspx?s=latestnews&id=1686. The term "war driving" is more often associated with one who drives to an area within reach of another's wireless network and accesses the network without permission. *Id.*

9. Bierlein, *supra* note 2, at 1125–26.

10. Hale, *supra* note 7, at 543–44 (citing *Wi-Fi: Unplugging Devices*, CNETNEWS.COM, Sept. 13, 2003, http://news.com/Wi-Fi:+Unplugging+devices/2100-7351_3-5072011.html).

available in private locations such as businesses and residences.[11] Public areas called "HotSpots" also provide access.[12] These HotSpots include locations such as coffee shops, airports, and hotels.[13] In fact, several websites offer wireless users detailed maps that identify these areas across the country and even abroad.[14] Moreover, city governments are taking increasing interest in providing their citizens with free wireless access, as evidenced by the fact that more than $230 million was spent on wireless-related municipal projects in 2006.[15] In the wake of Hurricane Katrina, New Orleans was the first major city to consider providing free wireless Internet access to its residents.[16]

With the expansion of wireless availability in Louisiana and the other forty-nine states, more Americans have begun to access Wi-Fi networks instead of connecting to the Internet using a land-based connection. One survey predicted that Wi-Fi use in private residences will increase from approximately 9 million in 2004 to about 28 million in 2008.[17] Additionally, experts in the field estimate that by 2008, approximately 22 million Wi-Fi users will access the Internet from over 53,000 HotSpots across the nation.[18] These statistics reveal that Americans have already integrated Wi-Fi technology into their lives and will continue to do so at an increasing rate.

---

11. Brain & Wilson, *supra* note 5.

12. Hale, *supra* note 7, at 543–44. New Orleans's Louis Armstrong International Airport recently became a HotSpot after spending $400,000 to provide patrons with free Internet access. Jacquetta White, *Wireless Internet Access Now Available at N.O. Airport*, TIMES-PICAYUNE (New Orleans), Oct. 31, 2007, http://blog.nola.com/times-picayune/2007/10/wireless_internet_access_now_a.html.

13. Hale, *supra* note 7, at 543–44.

14. *Id.* (citing WiFinder, Find Public Access Wi-Fi Hotspots, http://wifinder.com/ (last visited Oct. 6, 2008)).

15. Jewell, *supra* note 3.

16. Alan Sayre, *Big Easy Launches Free Wireless System*, BUSINESS WEEK, Nov. 25, 2005, http://www.freepress.net/node/11537/print. New Orleans mayor Ray Nagin believed that the implementation of free city-wide wireless access would help residents and businesses regain online access in light of storm-related telecommunication failures in attempt to show the nation that "[the city authorities] are building New Orleans back." *Id.*

17. Bierlein, *supra* note 2, at 1130 (citing Rebecca Lieb, *Wi-Fi Moves In*, CLICKZ, Oct. 4, 2004, http://www.clickz.com/showPage.html?page=3416331).

18. Bierlein, *supra* note 2, at 1130 (citing Matthew Yi, *Wi-Fi Hits the Spot: Businesses Find Wireless Internet Connection Entices Customers to Stay and Pay a Little Longer*, S.F. CHRON., Aug. 25, 2003, at E1, http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2003/08/25/BU213993.DTL&type=printable).

Most Internet subscribers who install and use wireless technology have the ability to prevent unauthorized use of their network by securing it with a password.[19] Yet, Jupiter Research conducted a survey last year and determined that 40% of the population either had not activated the security mechanisms on their wireless networks or was not sure if they had done so.[20] Furthermore, many older Wi-Fi systems cannot easily be secured with safety mechanisms such as passwords, and newer systems can be difficult to secure if the user is running more than one computer on the network, which is often the case.[21]

*B. Issues Raised by Wireless Piggybacking*

As the number of Internet subscribers who use wireless technology continues to rise, the number of wireless piggybackers will certainly increase. One study reported that 14% of Internet subscribers admitted to accessing their neighbor's Wi-Fi network without permission, though far more people probably have done so.[22] While some experts in the field insist that the unauthorized use of Wi-Fi networks is harmless,[23] others call attention to serious concerns raised by wireless piggybacking.[24] Although one policy analyst described wireless piggybacking as "the Twenty-first century equivalent of lending a cup of sugar,"[25] wireless piggybacking raises significant problems.

First of all, the Internet subscriber who utilizes an unsecured wireless network may be held liable for any illegal actions undertaken by a piggybacker using the subscriber's network.[26] When a piggybacker accesses websites using the subscriber's wireless network, the Internet Protocol address (or IP address) of the webhost of each site he visits is imported into the network,

---

19. Steve Hargreaves, *Stealing Your Neighbor's Net*, CNNMONEY, Aug. 10, 2005, http://money.cnn.com/2005/08/08/technology/personaltech/internetpiracy/index.htm?cnn=yes.

20. Jewell, *supra* note 3.

21. Hargreaves, *supra* note 19.

22. *Id.*

23. Timothy B. Lee, *Hop on My Bandwidth*, N.Y. TIMES, Mar. 16, 2006, http://www.nytimes.com/2006/03/16/opinion/16lee.html?_r=2&oref=slogin&oref=slogin.

24. Michel Marriott, *Hey Neighbor, Stop Piggybacking on My Wireless*, N.Y. TIMES, Mar. 5, 2006, http://www.nytimes.com/2006/03/05/technology/05wireless.html?ex=1299214800&en=de40126b08550e0a&ei=5090&partner=rssuserland&emc=rss.

25. Lee, *supra* note 23.

26. Kagan, *supra* note 8.

leaving a record of the visited websites.[27] Consequently, the websites are immediately associated with the subscriber.[28] For example, a piggybacker could utilize an innocent subscriber's network to illegally download copyrighted files.[29] These actions could attract the attention of copyright workers who may bring suit against the subscriber, having traced the illegally downloaded file(s) to the subscriber and not the piggybacker.[30] Similarly, a subscriber may be held criminally liable for the actions undertaken by a piggybacker using the network to view child pornography or to engage in other illegal activities.[31] As explained by an attorney specializing in computer-related legal issues:

> [C]ybercriminals, knowing that they could be traced back to their accounts using IP addresses, sit in their car on your street using your open access. When the FBI comes looking for the person downloading movies or child pornography, or luring children or sending denial-of-service attacks, they come looking for the person whose account was used, not the car driver. While you may be able to prove that your computer wasn't used for these illegal activities, or that no one was home at the time the activities occurred, it can be very tricky. It's far easier to secure your network with a passphrase.[32]

Second, and more commonly, wireless piggybacking can cause a subscriber's network to suffer a diminution in performance.[33] By accessing the subscriber's wireless network, the piggybacker consumes bandwidth and, consequently, may slow down the connection and complicate the subscriber's ability to access and utilize his own network.[34] While a subscriber may not suffer much inconvenience from the actions of one wireless piggybacker, he may begin to notice a reduction in Wi-Fi performance once multiple piggybackers start accessing his wireless network.[35] Furthermore, one unauthorized user can greatly interfere with the

---

27. *What is an IP Address?*, HOWSTUFFWORKS, Jan. 12, 2001, http://computer.howstuffworks.com/question549.htm.
28. *Id.*
29. Kagan, *supra* note 8.
30. *Id.*
31. *Id.*
32. Parry Aftab, *The Privacy Lawyer: Wireless Freeloaders are Breaking the Law*, INFORMATIONWEEK, Aug. 15, 2005, http://www.informationweek.com/story/showArticle.jhtml?articleID=167100929.
33. Kagan, *supra* note 8.
34. *Id.*
35. *Id.*

subscriber's network by downloading very large files or by simultaneously downloading several small files.[36]

Third, wireless piggybacking can cause substantial damage to the subscriber's computer system.[37] Wireless piggybackers may utilize unsecured networks to "release malicious viruses and worms that could do irreparable damage."[38] These computerized "diseases" could inconvenience the subscriber much more severely than would the simple act of accessing his computer network without permission. Thus, even mere access can lead to a serious impairment of the subscriber's entire computer system if viruses and worms infest the computer.

Finally, subscribers who fail to secure their networks also run the risk of giving piggybackers access to their private files, exposing them to the possibility of identity theft.[39] Piggybackers often access unsecured Wi-Fi networks to "peer into files containing sensitive financial and personal information"[40] or to "use the computer as a launching pad for identity theft."[41] Therefore, a subscriber who does not secure his wireless network has the potential to lose much more than the full enjoyment of his Internet service. The ever-increasing use of wireless technology creates a need for the State of Louisiana to consider from both a criminal and civil standpoint whether legal ramifications exist when one accesses another's wireless network without permission.

### *C. Affording Subscribers a Private Remedy*

Several scholars argue that state property laws should apply to computerized technology because the subscriber of a computer service should enjoy freedom from interference with his property, just as an automobile owner should enjoy freedom from interference with his car.[42] Because the owner of a chattel has the right to protect his property from interference, so too should the

36. *Id.*
37. Marriott, *supra* note 24.
38. *Id.*
39. *Id.* Identity theft costs victims, including individuals and businesses, tens of billions of dollars each year. An overwhelming majority of victims are not aware of the potential threat of identify theft imposed by their failure to secure their networks. Press Release, The Office of Governor Arnold Schwarzenegger, Governor Schwarzenegger Signs Legislation to Protect Consumers Using Wireless Devices (Sept. 30, 2006), http://gov.ca.gov/index.php?/press-release/4227/ [hereinafter Schwarzenegger Release].
40. Marriott, *supra* note 24.
41. *Id.*
42. Greg Lastowka, *Decoding Cyberproperty*, 40 IND. L. REV. 23, 23–24 (2007).

subscriber have a right to protect his property rights.[43] However, the proposed application of state property laws to wireless piggybacking raises several concerns.

On one hand, a state runs the risk of minimizing the benefits of the Internet by assigning property rights to subscribers, thereby affording them a private cause of action against wireless piggybackers.[44] Arguably, the most important facet of the Internet is its ability to encourage the open dissemination of information.[45] By connecting individuals on a cross-state and cross-nation basis, the Internet promotes the enrichment of personal knowledge and fosters an international awareness of social issues.[46] Piggybackers, like most Internet users, are vital benefactors to this enormous online library of information. However, if piggybackers were fearful of the legal ramifications of accessing another's unsecured wireless network without permission, then they would no longer contribute to the collection of online information.[47] Therefore, by assigning property rights to subscribers of wireless networks, states may jeopardize the enormous free-flow of information found on the Internet.[48]

On the other hand, proponents of the criminalization of wireless piggybacking may argue that while piggybackers contribute to the open dissemination of online information, they also harm the economy by impeding Internet subscription sales. If a piggybacker can utilize another's Internet service without the fear of criminal ramifications, he will likely be less inclined to purchase his own Internet subscription. Additionally, an Internet subscriber may decide to discontinue his subscription if he becomes too frustrated with a piggybacker's actions, or he may contemplate becoming a piggybacker himself.[49] Thus, a state's failure to criminalize wireless piggybacking may inhibit the sale (or encourage the cancellation) of Internet subscriptions, thereby discouraging economic growth.

Another problem raised by the inclusion of wireless networks in the realm of property law is the difficulty in determining the

---

43. *Id.*

44. Ethan Preston, *Finding Fences in Cyberspace: Privacy, Property and Open Access on the Internet*, 6 J. TECH. L. & POL'Y 57, 57 (2001).

45. *Id.*

46. *Id.*

47. *Id.*

48. *Id.*

49. A subscriber whose network suffers a diminution of performance at the hands of piggybackers may decide that the money paid for the subscription is not worth the compromised speed of the connection. Instead, he may decide to access another's unsecured network for free.

extent to which wireless networks can be deemed personal property or, more specifically, chattels. In order to afford subscribers a private remedy against wireless piggybackers, states must first recognize that the subscriber has a right to freedom from interference with his network.[50] As discussed later in this Comment, states should identify the subscriber's personal property interest in his computer system and wireless router.[51]

## III. CURRENT WIRELESS INTERNET NETWORK LAWS

The issue of whether wireless piggybacking is illegal under current law raises difficult questions. Although some federal legislation exists regarding the unauthorized use of computer networks, these laws are intended to apply more to hacking than the non-permitted accessing of computer networks.[52] The state courts and legislatures that address the application of property rights to the Internet disagree on how exactly the issue should be approached.[53] While most, if not all, states have statutes that prohibit the accessing of computerized technology without permission, "unauthorized" and "without permission" are vague terms that are interpreted differently from state to state.[54] Further complicating the criminalization of wireless piggybacking is the likely defense used by the piggybacker—by failing to secure his network when he has the ability to do so, a subscriber consents to the communal use of his wireless network.[55] Nevertheless, securing an Internet connection is not always a simple task,[56] and

50. Through the doctrines of trespass to chattels and conversion, Louisiana has recognized that a plaintiff may recover if he can prove that someone has intentionally interfered with his chattel. FRANK L. MARAIST & THOMAS C. GALLIGAN, LOUISIANA TORT LAW § 2.06 (2d ed. 2007).

51. *See infra* Part II.B.

52. Hale, *supra* note 7, at 551. Federal laws such as the Computer Fraud and Abuse Act (CFAA) were intended to target theft-related acts rather than lesser crimes, such as unauthorized use of a wireless internet network. *Id. See also* 18 U.S.C. § 1030 (2000, Supp. 2004 & Supp. 2005).

53. Hargreaves, *supra* note 19. California recently sought to protect consumers from piggybackers by enacting a law that requires manufacturers of wireless network equipment to warn consumers of the harm they may suffer through the actions of wireless piggybackers or instruct them on how to secure their wireless networks. *See* Schwarzenegger Release, *supra* note 39.

54. Benjamin D. Kern, *Whacking, Joyriding and War-Driving: Roaming Use of Wi-Fi and the Law*, 21 SANTA CLARA COMPUTER & HIGH TECH. L.J. 101, 143 (2004).

55. Ned Snow, *Accessing the Internet Through the Neighbor's Wireless Internet Connection: Physical Trespass in Virtual Reality*, 84 NEB. L. REV. 1226, 1229 (2006).

56. Hargreaves, *supra* note 19.

individuals who fail to do so should not necessarily be divested of their ownership rights.

Additionally, it may be difficult to apprehend and charge wireless piggybackers due to the increasing number of piggybackers and the difficulties associated with linking the offender to the offense.[57] Although a wireless piggybacker typically accesses websites using his own computer, the websites he views and the files he downloads are ultimately associated with the Internet subscriber.[58] Thus, it may be very difficult for a subscriber to prove that a particular piggybacker has actually committed the offense.

However, experts agree that the chances of a piggybacker being arrested and charged are dependent upon the severity and frequency of the offense and the location of access.[59] If a piggybacker uses another's wireless connection to check his e-mail or to shop on-line, then he is less likely to face charges than he would be for using the connection to engage in identify theft or to view child pornography.[60] This statement, supported by the incidents of piggybacking-related arrests within the past two years, suggests one of the following possibilities: either piggybacking is illegal in itself and an offender is more likely to be caught if his underlying online activity is illegal, or more likely, a piggybacker must be committing some underlying criminal offense while piggybacking in order to be arrested.

Also, a piggybacker who occasionally accesses his neighbor's Internet connection is less likely to be arrested and prosecuted than one who does so habitually and frequently.[61] In addition, a piggybacker who accesses his neighbor's Wi-Fi network is far less likely to be arrested and charged than one who consistently parks his car outside of HotSpots simply to access the establishment's wireless network.[62] The tendency of law enforcement agencies to arrest piggybackers who habitually access Wi-Fi networks from HotSpots suggests that these agencies are much more likely to perform arrests when an offender utilizes a business's network without purchasing its products or services.

---

57. *Id.*
58. Kagan, *supra* note 8.
59. Hargreaves, *supra* note 19.
60. *Id.*
61. *Id.*
62. *Id.*

*A. Criminal Law Developments*

Although states and other nations have been hesitant to allow Internet subscribers to take private action against wireless piggybackers, several have permitted the apprehension and prosecution of those who engage in piggybacking. They have done so primarily by bringing wireless piggybacking within the scope of their preexisting criminal statutes.[63] However, among the American jurisdictions that criminalize the general unauthorized access of computer networks, the requisite elements of the offense and the ability to apply the language to wireless piggybacking differ from state to state. For example, while some state laws require actual damage to the property in order for criminal liability to be imposed upon the offender, others do not impose such a stringent prerequisite.[64] Also, while some states hold that the offender must actually know that his use is not permitted in order to face criminal liability, others stipulate that he must have reason to believe that his use is not authorized.[65] Nevertheless, most states have not addressed the issue of whether criminal liability should attach to the unauthorized access of a wireless network, and one would have substantial difficulties in attempting to predict how each state would decide the issue.[66]

Regardless of the inconsistency in the way in which state courts and legislative bodies interpret and implement their computer network access laws, several states have already begun arresting and charging individuals who access a wireless network without permission. Most states have imposed criminal penalties against piggybackers by using statutes prohibiting the unauthorized access of a computer network. For example, in 2005, a Florida man who accessed an unsecured wireless network from his laptop in his parked car on a street was apprehended and charged with violating a statute that prohibits the non-permitted access of a computer

63. Bierlein, *supra* note 2, at 1125–26.
64. Kern, *supra* note 54, at 143.
65. *Id.*
66. Some states may not impose liability upon wireless piggybackers because of the subscriber's ability to secure his connection. These states would likely take the position that by failing to secure his network, a subscriber consents to its use by others who do not first obtain his permission. Other states may impose limited liability on non-habitual offenders and aggressively prosecute only those who commit the offense in a recurrent or severe manner. This practice would be consistent with states' tendencies to apprehend and charge only those who access a subscriber's wireless network on a frequent basis or in a substantially debilitating way.

network.[67] A few months later, an Illinois resident was arrested and charged with the unauthorized access of a computer network after he accessed a non-profit agency's wireless network from his laptop in his parked car.[68] Also, in May 2007, a Michigan resident was arrested for violating a statute prohibiting the unauthorized access of a computer network after he accessed a local café's wireless network from his car.[69]

Some states have even arrested piggybackers under statutes that do not specifically pertain to the unauthorized access of computer networks. In 2006, in Clark County, Washington, deputies arrested and charged a man of theft of services after he habitually parked his car outside a coffee shop and accessed the shop's wireless network without ever buying any products.[70] Under Washington's theft of telecommunication services statute,[71] the man was liable because he "knowingly and with intent to avoid payment" utilized a telecommunication device "to obtain telecommunication services without having entered into a prior agreement with a telecommunication service provider to pay for the telecommunication services."[72] Also, in February 2007, an Alaskan man was cited and investigated for charges of theft of services after he was warned by the police to cease using a library's wireless network to play online games from his parked car.[73] The man violated the Alaska statute when he "obtain[ed] the use of . . . a computer network . . . with reckless disregard that the use by that person is unauthorized."[74] Thus, although states have not yet expressly criminalized the unauthorized use of wireless computer networks, several American jurisdictions have already

---

67. Bierlein, *supra* note 2, at 1123–24. He was charged under Florida Statutes section 815.06, offenses against computer users, because he "willingly, knowingly, and without authorization" accessed a computer network. *Id.* at 1124 n.10. *See also* FLA. STAT. § 815.06 (2006).

68. Bangeman, *supra* note 2. The man was charged with computer tampering, because he "knowingly and without the authorization of a computer's owner" accessed the agency's wireless network. 720 ILL. COMP. STAT. 5/16D-3 (2003).

69. Cox, *supra* note 2. He was arrested for violating Michigan Compiled Laws section 752.794, fraudulent access to computer networks, because he "intentionally access[ed] . . . [a] computer network to devise or execute a scheme or artifice with the intent to defraud or to obtain . . . a service by a false or fraudulent pretense . . . ." *Id. See also* MICH. COMP. LAWS § 752.794 (2004).

70. Keizer, *supra* note 1.

71. WASH. REV. CODE § 9A.56.262 (2000).

72. *Id.*

73. Wellner, *supra* note 2.

74. ALASKA STAT. § 11.46.200 (2006).

begun to take criminal action against piggybackers by bringing the act within the scope of their current laws.

In addition, other nations have imposed criminal liability upon wireless piggybackers. A man from London was arrested and sentenced for accessing his neighbor's wireless network from his car without permission.[75] Further, a teenager from Singapore was arrested and convicted for accessing a neighbor's wireless network without permission, a clear violation of the country's Computer Misuse Act.[76] The boy "knowingly . . . secure[d] access without authority to [a] computer for the purpose of obtaining, directly or indirectly, any computer service."[77] Thus, the criminalization of wireless piggybacking transcends national borders and is certain to become a hot topic in countries that have not yet encountered this issue.

*B. Tort Law Developments*

Despite the fact that some states and other nations have prosecuted individuals for using a wireless connection without authorization, few, if any, have allowed subscribers to take civil action against wireless piggybackers. A state may be able to afford a subscriber a private remedy against a piggybacker by recognizing the subscriber's ownership interest in his computer system. As explained above, wireless piggybacking can potentially cause severe damage to the subscriber's computer should the piggybacker upload a virus or worm onto the subscriber's system.[78] Accordingly, a subscriber may be afforded a private remedy when a wireless piggybacker engages in this action.

Additionally, a state may acknowledge the ownership interest that the computer owner possesses in his wireless router.[79] In order to implement a wireless network, an Internet subscriber must first purchase and install a wireless router.[80] A wireless router connects

75. Jane Wakefield, *Wireless Hijacking Under Scrutiny*, BBC NEWS, July 28, 2005, http://news.bbc.co.uk/1/hi/technology/4721723.stm. He was arrested for violating the United Kingdom's Computer Misuse Act, 1990, c.18, § 1 (Eng.), which makes it a criminal offense to "secure access to any program or data held in any computer" when "the access he intends to secure is unauthorised" and "he knows at the time when he causes the computer to perform the function that that is the case."

76. *Probation for Using Neighbor's Wireless Link*, MSNBC, Jan. 16, 2007, http://www.msnbc.msn.com/id/16651095/.

77. Computer Misuse Act, 1998, Cap 50A (Singapore), *available at* http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan002107.pdf.

78. *See supra* Part II.B.

79. Snow, *supra* note 55, at 1229–31.

80. Brain & Wilson, *supra* note 5.

directly to the Internet and generates a signal that can be detected within a certain distance by computers equipped with wireless network adapters.[81] Consequently, if the transmitted signal is not secured, it can be accessed by anyone who owns a desktop or laptop computer equipped with an internal or external wireless card.[82] On average, consumers pay $90 for wireless routers.[83] Thus, the router could certainly be considered a chattel in which the owner should enjoy full ownership rights, including freedom from interference. Just as an individual commits a trespass when he drives his neighbor's car without first obtaining consent, a wireless piggybacker commits a trespass when he uses his neighbor's wireless router without permission. Although it may require a theoretical stretch, the application of property rights to wireless networks and the affording of a private remedy to subscribers against wireless piggybackers seems reasonable.

Even though state legislatures and courts have failed to grant subscribers a cause of action against piggybackers, some jurisdictions have strongly considered expanding the trespass to chattels doctrine to encompass cyberspace-related property rights.[84] While the tort of trespass to chattels has suffered a significant decline in frequency of application since its inception, several courts and scholars have suggested that it may undergo rebirth in light of the computer technology renaissance.[85] As one court noted, "A few courts . . . breathed new life into the common law cause of action for trespass to chattels by finding it viable online."[86] While conversion is the tort that is much more commonly used to afford a private cause of action to victims of property damage, trespass to chattels is deemed to be the more appropriate tort to utilize in cases that involve less than complete destruction of property.[87] As Prosser stated,

> [The tort of trespass to chattel's] chief importance now is that there may be recovery where trespass would lie at

---

81. *Id.*

82. *Id.*

83. Jeffery Batersby, *Don't Think You Need a Home Network? Think Again. Here's How—and Why—to Get Started*, MACWORLD, July 26, 2004, http://www.macworld.com/2004/07/features/getconnected/index.php?pf=1.

84. *See supra* Part II.B.

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

86. *Id.* Another court in agreement has stated, "The trespass to chattels issue requires adapting the ancient common law action to the modern age." Ticketmaster Corp. v. Tickets.com, Inc., No. CV99-7654-HLH(VBKx), 2003 U.S Dist. Lexis 6483, at *10 (C.D. Cal. Aug. 10, 2003).

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

> common law, for interferences with the possession of chattels which are not sufficiently important to be classed as conversion, and so to compel the defendant to pay the full value of the thing with which he has interfered. Trespass to chattels survives today, in other words, largely as a little brother of conversion.[88]

For example, in *CompuServe v. Cyber Promotions*, a federal district court in Ohio held that the generation of signals created by the defendants using the plaintiff's computer equipment to send unsolicited e-mails to its subscribers resulted in a trespass to chattels.[89] Because the defendant overburdened the plaintiff's computer equipment with unsolicited mass e-mails, thereby causing significant portions of the equipment to be unavailable to its subscriber, the plaintiff was able to show interference with and actual damage to its chattels.[90] Also, in *Sotelo v. DirectRevenue Holdings*, a federal district court in Illinois found that the defendant's installation of spyware onto the plaintiff's computer comprised a trespass to chattels through the over-burdening of resources and diminution of performance.[91] In both cases, the plaintiffs did not suffer complete destruction to their property and, thus could not bring a conversion claim against the defendants.[92] However, the tort of trespass to chattels enabled both plaintiffs to recover if they were able to prove interference with and actual damage to their chattels.[93] Since courts have postulated that the doctrine of trespass to chattels is applicable to computerized technology, the extension of this tort to unauthorized wireless access seems reasonable.

Although several U.S. jurisdictions have demonstrated great inconsistency in bringing cyberproperty within the scope of trespass laws, none has done so more than the courts of California. The first case to apply the tort of trespass to chattels to computer networking devices was *Thrifty-Tel v. Bezenek*.[94] In that case, two teenagers used a confidential phone number to call into a long distance telephone company.[95] They repetitively entered random six-digit codes in hopes of finding a valid access code and

88. W. PAGE KEETON ET AL., PROSSER & KEETON ON THE LAW OF TORTS § 14 (5th ed. 1984).
89. 962 F. Supp. 1015 (S.D. Ohio 1997).
90. *Id.*
91. 384 F. Supp. 2d 1219, 1229–33 (N.D. Ill. 2005).
92. *CompuServe*, 962 F. Supp. 1015; *Sotelo*, 384 F. Supp. 2d 1219.
93. *CompuServe*, 962 F. Supp. 1015; *Sotelo*, 384 F. Supp. 2d 1219.
94. Thrifty-Tel, Inc. v. Bezenek, 54 Cal. Rptr. 2d 468 (Cal. Ct. App. 1996).
95. *Id.* at 471.

connecting to the network.[96] The boys then used a computer program to continuously dial in an attempt to decipher a working access code.[97] Paying customers of the telephone network were unable to use the network because the boys overburdened the system.[98] The telephone company sued the boys' parents for fraud and conversion.[99] The court held that the boys committed the tort of trespass to chattels even though the offense was not pleaded.[100]

Following *Thrifty-Tel*, several other courts considered whether to apply the trespass to chattels doctrine to cyberproperty.[101] However, the most controversial decision in California cyberproperty case law, and perhaps the entire body of U.S. case law pertaining to computerized property rights, is *Intel v. Hamidi*.[102] In *Hamidi*, the defendant, a former employee of Intel, sent e-mails to many Intel employees over the span of two years.[103] The messages, which were very critical of Intel, were sent on behalf of FACE-Intel, an organization that consisted of former and current employees of the company.[104] Intel attempted to block Hamidi's e-mails but was not successful in doing so.[105] Intel wrote to him, warning him that he would be sued if he sent any further e-mails.[106] After he did so, Intel sued him for trespass to chattels.[107] Intel argued that although its server did not suffer actual damage, the company sustained a loss of production because its workers

96. *Id.*
97. *Id.*
98. *Id.*
99. *Id.* at 473.
100. *Id.* Justice Crosby noted that trespass to chattels is a very useful tort in instances where it seems too harsh to label an offense against property as a conversion. *Id.*
101. The court in *eBay, Inc. v. Bidder's Edge, Inc.* held that the defendant committed a trespass to chattels by utilizing a substantial number of eBay's resources, thus noticeably interfering with its server. 100 F. Supp. 2d 1058 (N.D. Cal. 2000). The next year, in *Oyster Software, Inc. v. Forms Processing, Inc.*, the court decided that California had abandoned the "actual damage to the chattel" requirement. No. C-00-0724 JCS, 2001 U.S. Dist. LEXIS 22520 (N.D. Cal. Dec. 6, 2001). However, just two years later in *Ticketmaster Corp. v. Tickets.Com*, the court reinstated the heightened burden of proof required for a plaintiff to recover on a claim of trespass to chattels. No. CV99-7654-HLH(VBKx), 2003 U.S. Dist. LEXIS 6483 (C.D. Cal. Mar. 6, 2003).
102. 71 P.3d 296 (Cal. 2003).
103. *Id.* at 301.
104. *Id.*
105. *Id.*
106. *Id.*
107. *Id.*

were distracted by the e-mails and because it had to waste time attempting to block Hamidi's messages.[108]

At the trial, the court issued a permanent injunction forbidding Hamidi to use Intel's computer system to send unsolicited e-mails.[109] Hamidi appealed, and a panel majority affirmed the judgment relying heavily on footnote 6 of *Thrifty-Tel*, which states: "At early common law, trespass required a physical touching of another's chattel or entry onto another's land. . . . In our view, the electronic signals generated by the Bezenek boys' activities were sufficiently tangible to support a trespass cause of action."[110]

The California Supreme Court, in a four to three decision, reversed the decision of the appellate court.[111] Relying on the pre-*Thrifty-Tel* rule, the majority insisted that some damage to the chattel is required in order for a plaintiff to recover on a claim of trespass to chattels.[112] The court also distinguished *Hamidi* from the preceding California cyberproperty cases by noting that although Hamidi's series of e-mails overburdened the system, it did not make the system more difficult for the e-mail recipients to employ.[113] Holding that actual damage is required and noting that Intel did not allege actual damage, the court ruled in favor of the defendant.[114] Although the *Hamidi* majority was not ready to concede that the doctrine of trespass to chattels should apply unequivocally to computerized property, the court did imply that a plaintiff may be able to recover on such a claim as long as he can prove actual damage to the cyberproperty.[115] Despite *Hamidi*'s status as the most recognized cyberproperty case, other jurisdictions have not necessarily followed the reasoning of the majority.[116]

---

108. *Id.*
109. *Id.* at 302.
110. Thrifty-Tel, Inc. v. Bezenek, 46 Cal. App. 4th 1559, 1566 n.6 (Cal. Ct. App. 1996).
111. *Hamidi*, 71 P.3d 296.
112. *Id.* at 311.
113. *Id.* at 303–07.
114. *Id.* at 311.
115. *Id.*
116. *See* Sherwood 48 Assocs. v. Sony Corp., No. 02-9100, 2003 WL 22229422 (2d Cir. Sept. 29, 2003) (holding that the measuring of a building with lasers constitutes a trespass to chattels and that a showing of actual damage is not required).

## IV. APPLICATION OF LOUISIANA'S LAWS TO WIRELESS PIGGYBACKING

Although Louisiana legislators and courts have yet to address the issue of wireless piggybacking, they will surely encounter this phenomenon in the near future. As an increasing number of Louisiana businesses and households embrace wireless technology, they will desire protection of their wireless networks in order to avoid the possible diminution of their Internet subscriptions, the risk of being held criminally liable for a piggybacker's computer-related crimes, the possibility of substantial damage to their computer systems, and the threat of identity theft. Louisiana's impending encounter with these issues warrants an analysis of whether the State's criminal and tort laws could be construed to encompass wireless piggybacking.

### *A. Louisiana's Criminal Statutes*

Given that other states have arrested and charged piggybackers by applying preexisting criminal statutes, it is likely that the State of Louisiana will do the same when it sees fit to arrest and prosecute a wireless piggybacker. The Louisiana courts will first need to determine which, if any, current criminal statutes can be interpreted in a manner which could apply to the unauthorized access of a wireless network. Three statutes—those governing criminal mischief,[117] offenses against computer users,[118] and computer tampering[119]—warrant a detailed analysis to determine whether they should govern wireless piggybacking.[120] These laws

117. LA. REV. STAT. ANN. § 14:59 (2007).
118. § 14:73.4.
119. § 14:73.7.
120. Several American courts have considered computer-related items, such as internet servers, to be movable property. If Louisiana courts were to consider wireless networks to be movable property the way other jurisdictions likely would, then a straightforward application of Louisiana Revised Statutes section 14:68, unauthorized use of a movable, would suggest that wireless piggybackers would face criminal liability under the statute. *See* § 14:68. The mens rea requirement of the offense, "intentionally," indicates that there must be a specific intent to commit the crime. Since the piggybacker would most likely "actively desire" to take the subscriber's wireless network without his consent on a non-permanent basis, then it would not be terribly difficult to bring wireless piggybacking within the scope of the statute. Despite the prima facie workability of the application of the statute to wireless piggybacking, Louisiana courts have rejected the notion that this law should apply to computer usage and to intangible movables. In *Chiasson v. City of Thibodaux*, the court ruled that "[another's] use of [a] computer for personal reasons was not an 'intentional taking or use of a movable which belongs to another.'" 347 F. Supp. 2d 300, 312

should be inspected in terms of the four primary concerns raised by the unauthorized access of wireless networks.[121]

Under Louisiana's computer tampering statute, a subscriber may be held liable for the illicit activities undertaken by a piggybacker using his wireless network.[122] The statute requires that the offender (without the permission of the subscriber) introduce electronic information with the intention of "altering . . . any program or data contained within a computer."[123] The action must be committed intentionally and "without the authorization of the owner," with the offender "knowingly" engaging in the illegal online activity.[124] By intentionally utilizing the subscriber's wireless network to download files and visit web pages, a piggybacker knowingly introduces electronic information—the IP addresses of the hosts of the websites he visits—onto the subscriber's computer network.[125] Thus, the piggybacker alters the data contained within the subscriber's network by bringing in electronic information without the subscriber's permission.

An additional issue for Louisiana courts to consider is a piggybacker's ability to drain substantial amounts of bandwidth, impeding the performance of a subscriber's wireless network. As previously discussed, a diminution of network performance is more likely to occur through a piggybacker's simultaneous visitation of many websites or through his downloading of very large files.[126] Under Louisiana's computer tampering statute, a piggybacker may be held criminally liable if he "reduce[s] the ability of the owner of the computer to access or utilize the computer or any program or data contained within the computer."[127] However, although the piggybacker may

---

(E.D. La. 2004) (quoting section 14:68). The court explained that the legislature intended for the statute to be applicable in a situation where one takes another's car for a joyride without his permission. *Id.* at 312. Thus, the statute was meant to be construed in a manner that requires the physical deportation of property, and not just the mere stationary usage of it. *Id.* In addition, the court in *State v. Gisclair*, in holding that employee labor was not covered by the statute, reiterated that the law was intended to apply primarily to the unauthorized use of tangible movables, especially automobiles. 382 So. 2d 914, 916 (La. 1980). Thus, it is likely that Louisiana judges would be very hesitant to brush wireless piggybacking under the scope of this law.

121. *See supra* Part II.B.
122. § 14:73.7.
123. § 14:73.7(A)(3).
124. § 14:73.7(A).
125. *What is an IP Address?*, *supra* note 27.
126. *See supra* Part II.B.
127. § 14:73.7(A)(3).

"intentionally" access the subscriber's wireless network, he may not "knowingly" reduce the speed at which a network can perform. In order for piggybacking to be brought within the scope of this statute, a piggybacker must satisfy both mens rea elements of the offense, so the piggybacker must have knowledge that his activity may lessen the ability of the subscriber to enjoy his computer network.[128]

Additionally, a piggybacker who slows down a subscriber's network could face charges under Louisiana's statute criminalizing offenses against computer users. The statute requires that the alleged offender intentionally deny the computer user (without his permission) "the full and effective use of or access to a computer, a computer system, a computer network, or computer services."[129] A subscriber would certainly not have full use of his subscription if a piggybacker were usurping bandwidth, and (if the usurpation of bandwidth were severe enough) the subscriber may even be prevented from fully enjoying the network.[130] However, the State may face some difficulty in arguing that the piggybacker satisfies the mens rea element of this offense. After all, some wireless piggybackers may be unaware that their accessing of a subscriber's network consumes bandwidth and, thus, sometimes prevents the subscriber from reaping the full benefits of his subscription. If a piggybacker's actual intent to interfere with the subscriber's use of the network can be proven, then this statute would likely pass a thorough inspection by the courts and be deemed applicable to wireless piggybacking.

A third statute, Louisiana's law prohibiting criminal mischief,[131] may also be utilized to impose criminal sanctions on a wireless piggybacker who reduces the subscriber's network speed. In order to commit this offense, one must intentionally "tamper[] with any property of another, without the consent of the owner, with the intent to interfere with the free enjoyment of any rights of anyone thereto, or with the intent to deprive anyone entitled thereto of the

---

128. *Id.*

129. § 14:73.4(A).

130. *See supra* Part II.B.

131. § 14:59. Louisiana jurisprudence has indicated that the criminal mischief statute is not limited in its application to tangible property. See *State v. Krueutzer*, stating that "'tampering with any property of another' need not be limited to a physical act of tampering or to corporeal objects" and that "conduct that affects intangible property rights—such as the right to free use and enjoyment of one's back yard—might be said to be criminal mischief as defined by [section] 14:59(1), provided the conduct is committed with the necessary criminal intent." 583 So. 2d 1160, 1163 (La. App. 5th Cir. 1991).

full use of the property."[132] As described above, by accessing the subscriber's network without permission, a wireless piggybacker may obstruct his free use and enjoyment of the network.[133] Provided that he actually intends to prevent the subscriber from enjoying the full use of his wireless network, the piggybacker may be charged with criminal mischief.

All three statutes may be applied also in the case of the wireless piggybacker who utilizes a subscriber's network to unleash a worm or virus onto the subscriber's computer system. As previously discussed, such an "infection" may cause substantial interference and damage to the subscriber's computer system.[134] By committing these actions, a piggybacker undeniably and intentionally tampers with the computer system and deprives the subscriber of the full use of the property. In doing so, he violates Louisiana's criminal mischief law.[135] Also, by denying the subscriber the full and effective use of his computer system by infesting it with a worm or virus, a piggybacker could be charged with Louisiana's statute criminalizing offenses against computer users. Finally, a piggybacker commits computer tampering by intentionally accessing the subscriber's network and knowingly introducing the worm or virus into his computer system.

With regards to identity theft, the computer tampering statute prohibits individuals from accessing data stored within a computer without the permission of the owner.[136] A wireless piggybacker is sometimes able to access personal information from a subscriber's computer system by utilizing his wireless network, leaving the subscriber vulnerable to the threat of identity theft.[137] If the subscriber can prove that the piggybacker accessed his personal information, the state will likely be able to charge him under this offense because he accessed private information from the subscriber's computer system without authorization.[138]

In summary, it is likely that instead of relying on the legislature to enact new laws imposing criminal sanctions on wireless piggybackers, Louisiana courts will follow in the footsteps of other jurisdictions by broadening interpretations of its criminal statutes to encompass wireless piggybacking. As demonstrated, the laws of this state can be construed to apply to wireless piggybacking when

---

132. § 14:59(A)(1).
133. *See supra* Part II.B.
134. *See supra* Part II.B.
135. § 14:59.
136. § 14:73.7.
137. *See supra* Part II.B.
138. In this situation, the state may also charge the piggybacker with identity theft. *See* § 14:67.16.

the piggybacker uses the subscriber's network to engage in illegal online activity, deprive the subscriber of the full and effective use of his computer system, unleash a virus or worm onto his computer, or engage in identity theft. Perhaps the efficacy of current statutes in criminalizing wireless piggybacking explains why states with similar laws have been able to charge piggybackers under existing statutes instead of enacting new legislation specifically targeting them.

*B. Louisiana's Tort Laws*

Although several states have started applying their criminal statutes to wireless piggybacking, none has utilized existing tort laws to afford subscribers a private remedy when wireless networks have been accessed without authorization. While Louisiana will have to contemplate expanding its criminal laws in the near future to cover wireless piggybacking, it may be quite some time before the state legislature and courts afford Wi-Fi users a private remedy against offenders. Nevertheless, Louisiana courts could pave the way for the other forty-nine states by being the first American jurisdiction to afford a private remedy to victims of wireless piggybacking. Consequently, it is necessary to investigate whether Louisiana's existing tort laws could be construed to cover wireless piggybacking.

Since wireless piggybacking does not constitute a trespass to real property, courts must determine whether it falls within the scope of conversion or trespass to chattels. According to the *Restatement (Second) of Torts*, conversion requires "an intentional exercise of dominion or control over a chattel which so seriously interferes with the right of another to control it that the actor may justly be required to pay the other the full value of the chattel."[139] The Louisiana Supreme Court cited the Restatement definition of conversion with approval in *Dual Drilling v. Mills Equipment Investments*:

> We find that although conversion terminology has been borrowed from the common law, it is nonetheless securely rooted in civilian concepts of property law, offenses, and quasi-offenses. Our civilian remedies amply protect personal and real rights in movable property and should not be obscured by an application of common law conversion principles.[140]

139. RESTATEMENT (SECOND) OF TORTS § 222(A) (1965).
140. 721 So. 2d 853 (La. 1998).

Because a piggybacker's actions are not so deleterious as to justify reimbursement for the complete value of the computer system or wireless router, the tort of conversion would not be applicable to wireless piggybacking. Thus, if any of Louisiana's tort laws could apply to the unauthorized use of Wi-Fi networks, it would be the state's trespass to chattels law.

Louisiana state courts have yet to investigate whether the trespass to chattels doctrine should apply to computerized chattels, either land-based or wireless. In fact, they have only occasionally considered the application of the trespass to chattels doctrine in any matter,[141] often relying instead upon the tort of conversion.[142] Louisiana's trespass to chattels law requires an "intentional intermeddling with a chattel (movable) in the possession of another that damages the chattel, reduces its value, or deprives the possessor of the use of the chattel for a significant period of time."[143] The term chattel has been held by U.S. jurisprudence to mean "any property that is movable; not so connected with the ground as to become a part of the ground or the realty."[144] Also, "trespass to chattels has evolved from its original common law application, concerning primarily the asportation of another's tangible property, to include the unauthorized use of personal property."[145] As discussed earlier, a subscriber possesses an ownership interest in his computer system and router, both of which may be substantially impaired through a wireless piggybacker's actions.[146] Since both of these items are considered personal property (or chattels) of the subscriber, wireless piggybacking may fall within the scope of the trespass to chattels doctrine if all the elements of the offense can be proved.

---

141. See *Lafleur v. Sylvester*, holding that the taking of a manure spreader without the consent of the owner constituted both a trespass to chattels and a conversion. 135 So. 2d 91, 101–02 (La. App. 3d Cir. 1961). The court, citing *Gliptis v. Fifteen Oil Co.*, 16 So. 2d 471, 472 (La. 1944), stated that "any unlawful physical invasion of another's property is a 'trespass [to chattels].'" *Lafleur*, 135 So. 2d at 101. *See also* Strahan v. Simmons, 15 So. 2d 164 (La. App. 1st Cir. 1943) (deciding that a vendor's wrongful repossession of a movable was as a trespass to chattels). *But cf.* Johnson v. Modern Furniture & Appliance Co., 76 So. 2d 338 (La. App. 2d Cir. 1954) (holding that a plaintiff consents to repossession by not objecting to it).

142. MARAIST & GALLIGAN, *supra* note 50, § 2.06 ("The tort of trespass to chattels is of declining significance; serious cases now are treated as conversions.").

143. *Id.*

144. State v. Donahue, 144 P. 755, 758 (Or. 1914).

145. Compuserve Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1020 (S.D. Ohio 1997).

146. *See supra* Part III.B.

First of all, in order for wireless piggybacking to be brought within the scope of Louisiana's trespass to chattels law, it must first be established that the piggybacker possessed the requisite intent. A subscriber can prove the piggybacker possessed the requisite intent to commit a trespass to chattels if he can show: (1) that the piggybacker "subjectively desire[d] the prohibited consequences of [his] actions, regardless of how unlikely their occurrence [was]"; or (2) that the piggybacker "[had] knowledge that the prohibited consequences [were] substantially certain to follow from [his] conduct no matter what results [he] subjectively desire[d]."[147] Thus, the requisite intent is established by showing that the piggybacker either personally intended to access the subscriber's network without authorization or that he knew that the unauthorized access of the subscriber's network was substantially certain to occur from his conduct. Because a piggybacker likely intends to access another's unsecured network, or is at least aware that he is doing so regardless of his intentions, the subscriber should not face much difficulty in proving the requisite intent.[148]

In addition, Louisiana requires the plaintiff to prove interference with his chattel resulting in actual damages. The *Restatement (Second) of Torts*, from which Louisiana has modeled its trespass to chattels law,[149] provides:

> One who commits a trespass to a chattel is subject to liability to the possessor of the chattel if, but only if,
> (a) he dispossesses the other of the chattel, or
> (b) the chattel is impaired as to its condition, quality, or value, or
> (c) the possessor is deprived of the use of the chattel for a substantial time, or
> (d) bodily harm is caused to the possessor, or harm is caused to some person or thing in which the possessor has a legally protected interest.[150]

The trespass to chattels doctrine does not specifically require actual damage to the chattel, but Louisiana has stated that "actions for trespass to chattels require some actual damage" in order for a plaintiff to recover.[151] Of the stipulations listed in the Restatement,

147. MARAIST & GALLIGAN, *supra* note 50, § 1.04.

148. For further explanation on Louisiana's handling of intent in tort issues, see *Caudle v. Betts*, 512 So. 2d 389 (La. 1987) and *Bazley v. Tortorich*, 397 So. 2d 475 (La. 1981). *Cf.* Citizen v. Theodore Daigle & Brother, Inc., 418 So. 2d 598 (La. 1982).

149. MARAIST & GALLIGAN, *supra* note 50, § 2.06.

150. RESTATEMENT (SECOND) OF TORTS, *supra* note 139, § 218.

151. MARAIST & GALLIGAN, *supra* note 50, § 2.06.

Provision (b) seems the most applicable to wireless piggybacking. Through accessing a subscriber's wireless network without permission, a wireless piggybacker may impair the quality of a chattel depending on the nature of his actions. If a piggybacker reduces the performance level of the network by usurping a large amount of bandwidth, he would impair the chattel and ultimately affect the subscriber's ability to use his computer system to search the Internet, thus resulting in actual damages.[152]

A piggybacker could also decrease the utility of the computer system by introducing a worm or virus onto the computer which could greatly compromise the effectiveness of the system.[153] The piggybacker who infects the subscriber's computer system with a worm or virus may also face civil liability under Provision (d) because he causes harm (through the reduction of utility) to the computer system, a "thing in which the possessor has a legally protected interest."[154] Under both of these stipulations, a subscriber would be able to satisfy the actual damage requirement.

The doctrine of trespass to chattels may provide a private remedy to subscribers when piggybackers impair the performance of a computer system by usurping large amounts of bandwidth or by introducing a worm or virus into the system; however, the tort law does not seem to be applicable in cases where a subscriber becomes the victim of identity theft[155] or faces criminal liability for illegal actions undertaken by the piggybacker.[156] In essence, the subscriber would not be able to prove actual damage under these two scenarios because the piggybacker would not have damaged the property of the subscriber or prevented him from using it. Thus, if Louisiana courts were to bring wireless piggybacking within the scope of the trespass to chattels doctrine, they would likely do so only in cases where the piggybacker interferes with the performance of the wireless network or infects the subscriber's computer system with a virus or worm. This gap in Louisiana's trespass to chattels law will certainly pose a problem should the state allow subscribers to sue piggybackers for trespass to chattels.

Also, while the trespass to chattels doctrine may be utilized to protect a subscriber's property interest in his computer system, none of the provisions seem applicable to the subscriber's router.

---

152. *See supra* Part II.B.

153. *Id.*

154. RESTATEMENT (SECOND) OF TORTS, *supra* note 139, § 218(d).

155. Courts may instead find that the piggybacker committed an invasion of privacy. *See* MARAIST & GALLIGAN, *supra* note 50, § 19.03.

156. The courts may find the piggybacker liable for false imprisonment if the subscriber is arrested as a result of the piggybacker's illegal online activities. *See id.* § 2.06.

A piggybacker may utilize the signal generated by the subscriber's router in order to access his wireless network.[157] In doing so, however, he does not cause actual damage to the router because it is still capable of generating signals within a certain distance despite the fact that he has hopped onto the network.[158] The inability of the trespass to chattels doctrine to protect the property interest the subscriber possesses in his wireless router creates another gap in Louisiana's tort law, one that may need to be addressed should Louisiana courts afford subscribers a private remedy against wireless piggybackers.

Despite the theoretical applicability of Louisiana's trespass to chattels law to wireless piggybacking in certain circumstances, it is unlikely the courts will soon use this law to afford subscribers a private remedy. Given the vast number of individuals who commit wireless piggybacking on a day-to-day basis, both voluntarily and without knowledge, it is likely that the courts would fear the opening of a piggybacking lawsuit floodgate. While the tendency of U.S. jurisdictions to not address the application of this offense in a civil context may seem strange, perhaps a very small number of subscribers have ever attempted to take action against piggybackers. After all, even in the incidents in which states asserted criminal rights against piggybackers, they only did so in unusual circumstances, such as when the offender parked near a subscriber's location or did not buy anything from the business.[159] Because most people do not park within the curtilage of individuals' homes, it may be difficult for subscribers to ascertain the identity of the piggybacker. Additionally, a business's ability to file charges against a piggybacker is not always feasible because many establishments may not be able to determine exactly who is utilizing their wireless network without purchasing any goods. Thus, unless Louisiana pioneers affording a private remedy to a subscriber against a wireless piggybacker, it is unlikely that the courts of this state will bring the offense within the scope of Louisiana's trespass to chattels law.

## V. CONCLUSION

With the advent of the computer revolution, the need for jurisdictions to expand their notions of property rights to encompass computerized technology has surfaced. Since the laws governing the ownership of property evolved to include computers,

157. *See supra* Part III.B.
158. *See supra* Part III.B.
159. *See supra* Part III.A.

computer systems, and computer networks, so too will these laws expand to cover wireless Internet networks. The fact that several states and other nations have begun prosecuting wireless piggybackers suggests that it is only a matter of time before Louisiana courts encounter this issue. When they do, they must determine which, if any, of the existing criminal statutes may apply to the unauthorized access of computer networks.

Louisiana's laws prohibiting criminal mischief, offenses against computer users, and computer tampering may allow the courts to penalize wireless piggybackers without the legislature having to enact a specific statute criminalizing the offense. Far more complex, however, is the applicability of trespass to chattels laws to wireless piggybacking. No U.S. jurisdiction has addressed this issue, though it is certain to happen given the nation's ever-increasing number of wireless users. When faced with this dilemma, Louisiana courts must determine whether the reasons for allowing the prosecution of wireless piggybackers logically align with the refusal to afford Wi-Fi users a private remedy.

*Grant J. Guillot*[*]

* The author would like to thank Professor Ron Scalise for his invaluable time, guidance, and feedback. He would also like to thank Professor Bill Corbett for his assistance with this Comment. Finally, he would also like to thank his wife, Amber, for constantly reminding him to make sure he is connected to his own wireless network.