The Ethical Issues Surrounding Wi-Fi

Nicole Houston, Devin Reams, Natalie Zelinsky

Introduction

In examining wireless-internet technologies (Wi-Fi), several ethical issues are exposed. While the unauthorized use of Wi-Fi is illegal in a few select cases, what is considered permissible still varies from state to state. What does not vary, however, is the fact that individuals are going to great lengths to locate unsecured wireless access points whether it is for their own benefit or the benefit of others. Neighbors are turning into hackers as unauthorized access is becoming more rampant. While the laws are still being developed, it is clear that there are ethical and moral dilemmas behind these acts. This brings up the issue of whose responsibility it is to protect wireless networks. While the manufacturer designs the product, the owner of the network chooses how to use the product and how to protect themselves as owners. In other words, it is ethical for manufacturers to accept partial responsibility for protecting their consumers. Using ethical decision-making approaches, the ethical problems surrounding Wi-Fi and why people commit unethical actions will be determined.

Wardriving

The act of searching for Wi-Fi networks by moving vehicle is becoming increasingly common. The tools used to locate open networks are now freely available on the Internet and they are allowing people to liberally search for free connections. Many are using GPS devices to measure the locations of networks and then log these locations onto websites for others to use. This type of Wi-Fi searching is called wardriving and its legality is not yet clearly defined in the United States for one main reason: wardriving does not in any way imply using wireless access points without explicit authorization. Instead, these wardrivers log the locations on websites dedicated to identifying access points for others to use. According to the FBI, it is not illegal to scan for access points. However, once a theft of service, denial of service, or theft of information occurs, it becomes a federal violation.[1]

The people that seek out these locations are doing nothing other than logging location points for the prospective use by others. However, they are doing so while knowing that once

they log these access points, others will be using them illegally. Wardriving can be related to being charged with acting as an accessory to a crime: while the person is not actually committing the crime, they are assisting in doing so by another person and not preventing the actions in any way. This goes against societal values because intentional actions are leading to crime. According to "virtue ethics," there are certain ideals toward which we should strive. These ideals, such as excellence and development toward the common good, allow for the full development of our humanity.[2] Living by the ideal of development toward the common good, a person committing an act knowing that it not only leads to illegal activity but also affects a person's property in some way, shape or form, is committing this act unethically. Therefore, it is surmised that the act of wardriving is unethical.

In an informal survey,[3] several reasons people engage in the practice of stealing Wi-Fi access points are:

- To access adult Web sites or send spam without leaving a trail
- To experience the thrill of being "where you aren't supposed to be" and finding networks
- To sell Wi-Fi owners security services
- To relieve boredom

The security division of a London consulting firm, KPMG, set up a dummy access point to observe the behavior of wardrivers. The study found that, on average, there are 3.4 attempts per day to access a dummy wireless network.[4] In a recent case, a wardriver found an unsecured wireless network at a Lowe's home improvement store. After documenting the location, he went back with a friend and proceeded to get into their system with the goal of stealing credit card numbers from customers of the store. The men were caught after they had managed to get six credit card numbers, but the damage could have been far worse. In the end, the FBI arrested both men and the main culprit is currently serving nine years in federal prison.[5] An associate of the two men, however, was charged with a misdemeanor for checking his e-mail over Lowe's' network, proving that officials are starting to take notice of offenses such as these and a transition is taking place from being solely unethical to becoming illegal.

It is instances such as this that make wardriving especially dangerous. While it is not always the same person documenting the location and illegally accessing the network, intentions are not good. According to the fairness or justice approach to ethics, the basic moral question

asks whether or not an action is fair or demonstrates favoritism and/or discrimination.[6] Wardriving demonstrates discrimination by imposing unfair burdens on those with identifiable wireless access points. Wardriving is unethical because of the knowledge that once the logging is complete, it is only being used illegally which in turn hurts the owner of the network.

Unauthorized Access

In 2004, the FCC had found no regulations making it illegal to log onto someone else's open network.[7] However, there are cases where individuals have been prosecuted for accessing others' open networks. In Alaska, a man's laptop was confiscated for accessing a Public Library's free Wi-Fi after library hours.[8] Another man was arrested and charged with "unauthorized access to a computer network" in Florida (after wardriving); this offense is a third-degree felony.[9] It is becoming more and more obvious that society, as reflected in our justice system, has an issue with individuals accessing others' Wi-Fi networks. The act of accessing someone's network, located via wardriving or any other method, seems unfair. In fact, using someone else's resources without their permission goes against common virtues including respectability, civility, and honesty. Accessing one's network and using their resources without their permission implies an act of stealing; someone is using bandwidth of which the owners can no longer use. In addition, the owner is put in jeopardy of losing their access if the provider deems any unauthorized actions via their connection, illegal or in excess of allotments.

Just because my neighbor leaves his hot tub open and the gate unlocked does not mean I have the right the walk into his backyard and go for a dip. To further illustrate, you will not be comfortable with your neighbor, maybe the one you have never met, walking up to the side of your house and borrowing your ladder without asking permission.[10] This is essentially what people are doing every day with their neighbors' open Wi-Fi networks; it is not just the hackers. Although there is a fundamental difference between a material object and network access, the law finds both acts to be an act of trespassing and/or theft. As previously mentioned, by playing bandwidth-intensive games, someone can severely limit the network owner's access to their own connection. Some providers may also restrict the number of users and their actions on a network. Therefore, not only do these simple acts seem innately wrong, they are ethically unfair.

People pay money for their high-speed connections and can, therefore, decide who can and cannot use their resources. By simply "borrowing" your neighbor's hot tub, ladder or Wi-Fi

connection you are, in essence, stealing. You are using someone else's property without their explicit permission. It does not matter if they do not notice; it does not matter if they are on vacation because stealing is unfair, unjust and unethical according to our society.

Some people will do anything they can to get onto a network. People are becoming increasingly aware of the dangers of leaving their Wi-Fi networks open which means more owners are now setting passwords and putting up security barriers. With that said, hackers still need, or want, access to the Internet through secured connections. Thus they employ a number of tactics and tools[11] to guess, crack, or circumvent owners' passwords and protection. A German website has been established as a resource for hackers to locate the default passwords for all wireless routers.[12] However, accessing a network through circumvention is not less unethical or illegal. Despite having the correct password, a network owner has still not given permission for use of their resources. This is unfair to them and unjust according to a number of laws. Many states, such as Florida, have adopted "Computer Hacking and Unauthorized Access Laws"[13] to persecute wrong-doers. Therefore, according to our justice system and one of our primary sources of ethics, it is unjust and illegal to "access" a lawfully created computer system without permission.

Manufacturer Responsibilities

It has been determined that accessing someone else's wireless Internet without explicit permission is unethical. However, the degree of responsibility that a manufacturer accepts in protecting wireless networks is an ethical decision in itself. One option is for manufacturers to relieve themselves of all responsibility, thus holding consumers accountable for protecting their own wireless networks. On the other hand, perhaps manufacturers should accept sole responsibility in protecting networks from those who choose to unethically steal Wi-Fi. Because ethics are rarely seen in black and white, one can expect the most appropriate ethical decision to lie somewhere in between the two extremes.

If manufacturers force consumers to be faced with complete responsibility of protecting their own wireless networks, many networks will not be secure at all. For example, studies have demonstrated that 75-80% of at-home network users ignore configuring Wi-Fi Protected Access (WPA) security despite manufacturers' warnings, such as the risk of identity theft. WPA provides a high level of security for wireless networks by using technology that constantly

changes the encryption key used in transmitting information and data. The use of dynamic encryption makes breaking into a wireless network much more difficult.[14] Now, imagine what will happen if manufacturers stop producing routers with WPA or other security capabilities at all. In this situation, manufacturers will be doing absolutely nothing to protect their consumers from the dangers and threats they know are associated with wireless networks. One may ask why it is unethical for wireless equipment manufacturers to opt out of providing security features in the first place. This situation has a lot of similarities to that of a car manufacturer being that there are many dangers known to be associated with driving. Is it ethical for car manufacturers to produce cars without seatbelts and airbags, knowing how much they decrease the risks of severe damage? Virtue ethics suggests that the development toward the common good should be strived for.[15] Therefore, wireless and car manufacturers alike should be ethically responsible for offering some form of protection for their consumers in order to contribute toward the common good of society. Moreover, the more security offered by manufacturers, the more virtue ethics will consider the actions ethical.

However, if manufacturers accept absolute responsibility in protecting wireless networks there will be an immense amount of work involved on their behalf. For instance, all wireless routers sold must have an un-broadcasted, one-of-a-kind service set identifier (SSID) name and password unrelated to any and all default lists. This helps to prevent unauthorized access to Wi-Fi networks by creating a unique username and password for each user automatically. With the SSIDs set up to be un-broadcasted, unauthorized users will not only have to crack a password, but an identifier name as well in order to join a Wi-Fi connection. As a result, network protection will be doubled. The downside for manufacturers in selling wireless routers equipped this way is that they will have to keep record of each router's SSID and password in case customers forget, or lose track of, their log-in information, thus increasing the volume of data needed to be stored and the number of customer service calls manufacturers receive. Furthermore, routers must also be sold with enabled WPA. Unfortunately, WPA must be configured with each computer that uses the router; therefore, manufacturers will be responsible for configuring each and every customer's router to their computer in order for the WPA to work properly. Nonetheless, the question arises as to whether it is ethical to require manufacturers to create and implement all security features. To answer this question, we will use the fairness or justice approach to ethics once again, which essentially asks how fair an action truly is.[15] In this

case, manufacturers are not being treated fairly because they are over-compensating to resolve an issue that involves both manufacturers and consumers. When there is more than one party involved in an issue, it only seems fair to delegate responsibilities for resolution. As a result, placing the entire burden on one party is unethical and manufacturers should not be solely responsible for securing wireless networks. Much like riding in a car, passengers are still responsible for using the seat belts that manufacturers put into place.

As illustrated in the two previous scenarios, it is ethically wrong for manufacturers to opt out of protecting consumers against potential wireless network dangers and it is also wrong for manufacturers to be exclusively responsible for all security settings. A solution to this problem is for manufacturers to build user-friendly security into their equipment, along with providing educational information and how-to instructions for at-home security enabling. Currently, wireless broadband router manufacturers offer advanced security measures such as modifiable network identifier names and passwords, address filtering, firewalls and WPA to protect wireless networks. With nearly all of the manufacturers' security measures, the consumer must make the final steps to ensure all features are properly installed, configured and adjusted for maximum security. As a solution, many manufacturers provide online tutorials and detailed, step-by-step instructions that describe how to enable the router's security settings.[14] Based on these actions, it is clear that manufacturers feel morally responsible for protecting consumers, but also rely on consumers to be responsible for their fair share as well.

Many writers on the subject of Wi-Fi agree that consumers and manufacturers should share the burdens associated with wireless networks. Jeffrey L. Seglin of the New York Times suggests that the right thing for consumers with wireless connections to do is to take the time to keep them private if they want them to remain private networks.[16] To go along with Seglin, Bob Breeden, Assistant Special Agent at the Florida Law Enforcement Department, believes that those who own Wi-Fi networks need to take the time to secure them.[17] Based on the virtue and fairness approaches for moral decision-making, it is clear that it is ethical for manufacturers to accept partial responsibility for protecting their consumers. They do this by offering multiple levels of Wi-Fi protection that can easily be implemented by the consumer. This is also ethical because it creates a well-balanced relationship between the manufacturer and consumer. Here, both parties are participating fairly in virtuous efforts to protect the well-being of everyone involved with securing wireless networks.

Conclusions

It has been demonstrated that Wi-Fi networks pose multiple ethical dilemmas. The act of wardriving, while not yet considered a crime, leads directly to misuse and illegal access to open networks. On the same level as being an accessory to a crime, wardriving goes against virtue ethics as well as fairness ethics by imposing an unfair burden on the owner of a private network. Wardriving, as it also goes against societal values such as honesty and respecting others' rights to their private property, is therefore considered unfair and unethical.

When people—hackers and neighbors alike—access a network without the owner's permission they are committing a crime.[13] Since we place much of our moral judgment on the justice system, the fact that this is illegal suggests that it is also unethical. Also, given that these individuals are being dishonest, disrespectful and unfairly using others' property, we can look to virtue and fairness ethics to deem these acts unethical.

Individuals choose to make these unethical decisions each and every day causing new dilemmas to arise. This raises the question regarding how much responsibility manufacturers should assume in protecting wireless networks. If we suggest it is entirely the responsibility of the manufacturer or consumer, the fairness framework of moral decision making tells us the situation, in either case, is unethical. Thus, it should be a shared responsibility to protect wireless networks because fairness ethics suggests that one party should not take on an unfair burden of responsibility and virtue ethics implies that the two should work together to benefit the common good.

Works Cited

[1] C. Hurley, M. Puchol, F. Thornton, R. Rogers, Wardriving: Drive, Detect, Defend: A Guide to Wireless Security. Massachusetts: Syngress, 2004.

[2] M. Velasquez, C. Andre, T. Shanks, S.J., and M. J. Meyer, "Ethics and Virtue." Markkula Center for Applied Ethics. Issues in Ethics. Spring 1988. .

[3] E. H. Freeman, "Wardriving: Unauthorized Access to Wi-Fi Networks." Information Systems Security, Mar/Apr 2006: 11-15.

[4] “Commuters Hack Wireless Networks.” BBC News. [Online Document], 26 March, 2003. Available at: http://news.bbc.co.uk/2/hi/technology/2885339.stm.

[5] K. Poulsen, “Long Prison Term for Lowe's Wi-Fi Hacker.” SecurityFocus. 16 Dec. 2004 Available at: http://www.securityfocus.com/news/10138.

[6] M. Velasquez, A. Claire, T. Shanks, S.J., and M. J. Meyer, “Thinking Ethically: A Framework for Moral Decision Making.” Issues in Ethics. Winter, 1996.

[7] P. Boutin, “How to Steal Wi-Fi.” Slate. [Online Document], 18, Nov. 2004. Available at: http://slate.msn.com/id/210991.

[8] A. Wellner, “Using free wireless at library described as theft.” Anchorage Daily News. [Online Document], 24 Feb. 2007. Available at: http://www.adn.com/news/alaska/story/8667098p.

[9] E. Bangeman, “Florida man charged with felony for wardriving.” Ars technical. [Online Document], 07 July 2005. Available at: http://arstechnica.com/news.ars/post/20050707-5068.html.

[10] G. Kewney, “WiFi theft: no, you can’t just walk into my house if the door is open.” [Online Document], 07 July 2005. Available at: http://www.newswireless.net/index.cfm/article/2317.

[11] “Wi-Foo- The Secrets of Wireless Hacking.” [Online Document], 04 March 2007. Available at: http://www.wi-foo.com/.

[12] “Default Password List.” [Online Document], 04 March 2007. Available at: http://www.phenoelit.de/dpl/dpl.html.

[13] “Computer Hacking and Unauthorized Access Laws.” National Conference of State Legislatures. [Online Document], 04 March 2007. Available at: http://www.ncsl.org/programs/lis/CIP/hacklaw.html.

[14] Linksys: A Division of Cisco System, Inc. 25 February 2007. Available at: www.linksys.com.

[15] Velasquez, Andre, Shanks, S.J., and Meyer. “Thinking Ethically: A Framework for Moral Decision Making.” Santa Clara University. [Online Document], 2 March 2007. Available at: http://www.scu.edu/ethics/practicing/decision/thinking.html.

[16] S. Ryst, “News Analysis.” BusinessWeek. 27 February 2007

[17] J. Seglin, “The Right Thing.” The Columbus Dispatch. [Online Document], 20 February 2007. Available at: http://www.dispatch.com/features-story.php?story=dispatch/2006/02/26/20060226-H2-03.html.