Catholic University Journal of Law and Technology

Volume 25 | Issue 1 Article 7

1-18-2017

Is WiFi Worth It: The Hidden Dangers of Public WiFi

Ellie Shahin
Catholic University of America (Student)

IS WIFI WORTH IT: THE HIDDEN DANGERS OF PUBLIC WIFI

Ellie Shahin*

I. INTRODUCTION

The ever-expanding growth of hotspot-using devices is exposing unaware consumers to a world of privacy risks that are easily preventable. The use of cell phone ownership rose to 91 % of all adults in 2013.[1] There are currently nearly fifty million public access wireless Internet hotspots available around the world.[2] In determining which devices[3] were most popular, Global Web Index makes it clear that laptops and cell phones are commonly used to browse the Internet by a significant majority of people; 91% of people use their laptops and 80% of people use their cell phones.[4] The average person spends ninety minutes a day on their cell phone, which totals to almost one month per year.[5]

* J.D. Candidate, The Catholic University of America: Columbus School of Law, 2017; B.A. in Communications with a Concentration in Public Relations, George Mason University, 2013. I would like to thank Professor Daniel Zachem for his assistance throughout this process. Additionally, I thank the Catholic University Journal of Law and Technology for their hard work and input. Finally, I thank my friends and family, especially my mom, for their support, and for sticking by my side through the stressful months of this research and writing process.

1 Lee Rainie, *Cell phone ownership hits 90% of adults*, PEW RESEARCH CENTER (June 6, 2013), http://www.pewresearch.org/fact-tank/2013/06/06/cell-phone-ownership-hits-91-of-adults.

2 *The Global Public Wi-Fi Network Grows to 50 Million Worldwide Wi-Fi Hotspots*, MARKET WIRED (Jan. 20, 2015, 8:00 AM), http://www.marketwired.com/press-release/the-global-public-wi-fi-network-grows-to-50-million-worldwide-wi-fi-hotspots-nasdaq-ipas-1984287.htm.

3 In discussing hotspot devices, this paper is referring to laptops, cell phones (more commonly known as "smart phones"), tablets, game consoles, smart watches and wristbands, and any other mobile device that has the capability to connect to a mobile hotspot.

4 Dave Chaffey, *Mobile Marketing Statistics compilation*, SMART INSIGHTS (Apr. 27, 2016), http://www.smartinsights.com/mobile-marketing/mobile-marketing-analytics/mobile-marketing-statistics.

5 *23 Days a Year Spent on Your Phone*, MOBILE STATISTICS, http://www.mobilestatistics.com/mobile-news/23-days-a-year-spent-on-your-phone.aspx

More significantly, the "average American adult spends 11 hours per day with electronic media"[6] which makes it clear that the digital world has become a staple in the day to day life of the average American.

Currently, there are nearly fifty million public hotspots, and that number is projected to skyrocket to three-hundred and forty million by 2018.[7] Three-hundred and forty million hotspots would provide approximately one hotspot for every twenty people on planet Earth.[8] As of 2015, "61% of U.S. homes are WiFi equipped and 64% of smartphone users still connect to WiFi when they leave the house too."[9] The use of publicly available hotspots is slowly spreading throughout the world; for example, New York is transforming all old payphones into free hotspots.[10] Combining the rapid expansion of easily accessible hotspots, the number of devices that are capable of connecting to those hotspots, and the number of people owning those devices, consumers are opening themselves up to a dangerous world of privacy risks.

There have been a number of statutes enacted to protect consumers from hackers,[11] however, there is little to no legislation that protects consumers from the types of computer crimes that are at risk of occurring by using public hotspots. With the number of hotspots increasing day-by-day, consumers expose themselves to the unwanted monitoring of their personal information, and the risk of theft of their personal information.[12] Hotspots leave users susceptible to computer crime because wireless internet "uses radio waves [and] the openness of these signals at public hotspots, combined with the right eavesdropping software, can allow others to take information without your knowledge."[13] This type of behavior is comparable to eavesdropping on a pri-

---

(last visited Sept. 15, 2016).

6 Matt Petronzio, *U.S. Adults Spend 11 Hours Per Day With Digital Media*, MASHABLE (Mar. 5, 2014), http://mashable.com/2014/03/05/american-digital-media-hours/#XhxSh9gRtSq9.

7 A.J. M., *The Growth of Global WiFi*, REPUBLIC WIRELESS (Apr. 1, 2015), http://pwk.republicwireless.com/the-growth-of-global-wifi.

8 *Id.*

9 *Id.*

10 *Id.*

11 Credit Card Fraud Act, 18 U.S.C. § 1028(a)(7) (2012) (explaining that "knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law" shall be punished); *see generally* Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2012) (explaining that any user that any users that intentionally accesses information on a computer without authorization shall be fined or otherwise punished).

12 *The Hidden Dangers of Public Wi-Fi*, NORTON, http://us.norton.com/dangers-of-public-wifi/promo (last visited Sept. 15, 2016) [hereinafter *Hidden Dangers*].

13 *Id.*

vate conversation in an overcrowded public area.[14]

This Note will explore the necessity for protection of consumers using public hotspots in the United States, and particularly, analyzes whether or not privacy rights and protection should extend to the types of computer crimes that are prevalent due to the use of public hotspots. This Note will provide a detailed analysis of relevant statutes and laws and, in turn, argue why they are insufficient. This Note will also argue that while the privacy rights infringed upon are not deserving of constitutional protection, consumers are nevertheless entitled to protection from a potential invasion of privacy. It will also discuss what privacy rights are at risk in the usage of public hotspots, and argue that the risks presented by public hotspots are too great to not receive heightened protection by way of the law. This Note will next explore possibilities as to what can be done to assist in keeping consumers safe from harmful computer crimes that invade their privacy. Lastly, this Note will argue how hotspot providers should be liable for increasing the protection of any users who may access their hotspot, and what options are available for those providers.

II. HISTORY OF HOTSPOTS

In order to understand how hotspots expose consumers to a world of privacy risks, it is important to understand what comprises a hotspot; "a hotspot is any location where [wireless internet access] is made publicly available."[15] Hotspots are most commonly found in cafes and coffee shops, airports and airplanes, and hotels and conference rooms that are commonplace for business meetings.[16] Public access hotspots have made completing assignments for work or school in public much more accessible and attractive, and users are no longer limited to the time where the computers at the public library were the only way to do work outside of the home. Wireless Internet was originally created as a way to eliminate the hassle created by Ethernet cables.[17] Wireless Internet was revolutionary because it allowed users to move about freely and remain connected to the Internet. Who wants to sit at their desk all day and watch Netflix, when bed is an option? Wireless access works by using "a little box called a router that plugs into your telephone socket" which connects a computer to

---

14 *Id.*

15 Bradley Mitchell, *Hotspot,* ABOUT TECH, http://compnetworking.about.com/cs/wireless/g/bldef_hotspot.htm (last updated Aug. 29, 2016).

16 *Id.*

17 John Patrick Pullen, *Here's How Wi-Fi Actually Works*, TIME.COM, (Apr. 24, 2015), http://time.com/3834259/wifi-how-works/.

the Internet by using radio waves, rather than a cable.[18] The router's job is to send messages to and from the Internet by creating a gateway from a mobile device to the Internet.[19] Public hotspots "use one or more wireless routers to create wireless Net access over a large area."[20] In its simplest form, wireless Internet functions much like the radio: wireless Internet is transmitted through a series of signals across two radio frequencies that aid in sending and receiving messages to connect a personal device to a large wireless Internet network.[21] This radio wave function is what allows consumers to travel throughout their home while remaining connected to the Internet.[22]

Although hotspots are a seemingly perfect way to connect to the Internet on the go, there are many issues that arise with their increased usage - the danger lies in the fact that many hotspot users are not aware of the potential risks.[23] Hotspots are "almost always unencrypted, which means that anyone with cheap, easily available software can listen in and access everything being sent over the network."[24] In effect, unencrypted networks open up users to potentially having *any* information that they store on their Internet accessing personal device stolen.[25] The four types of hacks that can occur while using public hotspots are: (1) sniffing, (2) evil twins, (3) man-in-the-middle-attacks, and (4) sidejacking.[26] Sniffing "allows hackers to passively intercept data sent between a web browser and web servers on the Internet."[27] This allows hackers who are sniffing to retrieve your email, search history, or any files transferred on that network.[28] When a hacker is sniffing personal information off of a device, it is unlikely that the user will receive any notifications or warnings in regards to a hacker passively accessing personal information.[29] However, "[a]n evil twin is a rogue WiFi access point that appears to be legitimate but actually has been set up by a hacker to fool wireless users into connecting a laptop or mobile

---

18 Chris Woodford, *Wireless Internet*, EXPLAINTHATSTUFF!, http://www.explainthatstuff.com/wirelessinternet.html (last updated Mar. 15, 2016).

19 *Id.*

20 *Id.*

21 Pullen, *supra* note 18.

22 *Id.*

23 PRIVATE WIFI, WHITEPAPER: THE HIDDEN DANGERS OF PUBLIC WIFI 5 (2014), http://www.privatewifi.com/wp-content/uploads/2015/01/PWF_whitepaper_v6.pdf [hereinafter PRIVATE WIFI].

24 *Id.*

25 *Id.* at 3.

26 *Id.* at 5.

27 *Id.*

28 *Id.*

29 *Id.*

phone to a tainted hotspot."[30] To put this simply, when a consumer goes to log on to a wireless network, a seemingly legitimate network will be available to log in.[31] This access point will actually be run by a hacker, and by logging on to the network, they will be able to access potentially any information that is stored on a user's device.[32]

A rogue wireless access point is one of the most serious threats to network security.[33] A rogue wireless access point is set up by an attacker attempting to gain access to a network environment that they are not authorized to access.[34] In addition to monitoring all Internet traffic, an evil twin allows a hacker to access a user's computer and prompt for "credit card information posing as a standard pay-for-access deal."[35] So a user may be on a wireless network in a café thinking they need to pay by the hour, but in reality it is a fraudulent wireless network that has now successfully collected the user's credit card information.[36] Man-in-the-middle attacks "intercept and modify" data going between the user and the hotspot server.[37] Sidejacking uses a "program that can intercept or log traffic passing over a digital network, to steal a session cookie containing usernames and passwords from a variety of websites, such as Facebook or LinkedIn."[38] What all of these hacking forms have in common is that they allow a hacker to access a public wireless access hotspot and collect personal information that an unknowing consumer stores on their personal Internet-accessing device.[39]

It is a common misconception that paying for a wireless network automatically secures it. Hacking, or wireless eavesdropping, can happen through essentially any hotspot.[40] This is evident in the fact that "39% of U.S. adults have accessed or transmitted sensitive information while on public WiFi without taking any steps to protect their data."[41] Individuals are also misinformed in thinking that firewalls and secure webpages will also protect them from hacking when only a virtual private network – which encrypts all data going in and

---

30 *Id.*
31 *Id.*
32 *Id.*
33 Ron Pacchiano, *Rogue Access Points: The Silent Killer*, PRACTICALLY NETWORKED, http://www.practicallynetworked.com/support/030306wirelesssecurity.htm (last visited Sept. 9, 2016).
34 *Id.*
35 PRIVATE WIFI, *supra* note 24, at 5.
36 *Id.*
37 *Id.*
38 *Id.*
39 *Id.*
40 *Id.* at 7.
41 *Id.* at 6.

out of the consumer's device – can protect consumers from the risks that public hotspots present.[42] This Note will later go into an in-depth discussion about the functions and security that virtual private networks provide.

There is an ever-present risk when using public hotspots, and due to the rapid increase in the usage of technology, the law is having a difficult time keeping up with computer crimes. Certain public hotspots request that a user accept the terms and conditions, which may include a clause stating that "sniffing" or eavesdropping is prohibited, but if there is no such clause then these actions are not prohibited or illegal.[43] In fact, there are no laws that currently prevent people from sniffing on a public hotspot.[44] The only way to fully and properly protect consumers is to have a virtual private network installed on the computer prior to logging on to a public hotspot. This requires an additional step to be taken by consumers to ensure that their actions online are secure, but this is a step that frequent users of public access wireless internet should be willing to take.

III. ANALYSIS

a. Legislation enacted through the years

The Computer Fraud and Abuse Act ("CFAA") "makes it illegal for anyone to distribute computer code or place it in the stream of commerce if they intend to cause either damage or economic loss."[45] The CFAA focuses on the potential financial risk that computer hacking can cause, and "provides criminal penalties for either knowingly or recklessly releasing a computer virus into computers or interstate commerce."[46] The potential punishment for someone in violation of the CFAA is a prison sentence of up to twenty years, and a fine of up to $250,000.[47]

The CFAA was first utilized after the release of the first Internet virus,

---

42 PRIVATE WIFI, *supra* note 24, at 6.

43 Simon Hill, *How Dangerous Is Public Wi-Fi? We Ask an Expert*, DIGITAL TRENDS (Aug. 15, 2015, 3:00 AM), www.digitaltrends.com/mobile/how-dangerous-is-public-wi-fi/; *see also* 18 USC § 1030(a)(2) (2012) (stating that the intentional accessing of a computer becomes a punishable offense only through a perpetrator obtaining sensitive information).

44 Hill, *supra* note 44.

45 *Computer Crime Laws*, PBS, http://www.pbs.org/wgbh/pages/frontline/shows/hackers/blame/crimelaws.html (last visited Sept. 16, 2016) [hereinafter *Computer Crime Laws*].

46 *Id.*

47 *Id.*

which was named the "Morris Worm."[48] In November of 1988, Robert Morris released a computer virus that spread across computers similar to a biological infection spreading across people.[49] However, Mr. Morris' conviction was unique; "the unamended version of the 1984 CFAA resulted in only one prosecution."[50] The CFAA has since been amended many times to include acts such as the National Information Infrastructure Act in 1996.[51] The current CFAA is designed to target varying aspects of computer crime, but it does not target all aspects of computer crime.[52] For example, section (a)(1) of the CFAA prohibits transmitting classified government information that was obtained without authorization; section (a)(2) prohibits the theft of financial information; section (a)(6) makes it a crime to traffic passwords for the purpose of affecting interstate commerce or a computer owned by the government.[53]

The CFAA is ineffective in protecting the consumers from hackers who use hotspots to obtain private information in order to cause harm.[54] It is designed to protect users from viruses, however, the type of legislation that this Note is proposing is not meant to protect users from computer viruses, but rather it is meant to protect the average American citizen from having their personal information accessed via hotspot. The CFAA is seemingly designed in large part to protect the government from being defrauded by way of computer hacking. This Act makes it a crime to use unauthorized access to collect account passwords in section (a)(6), but that only applies to computers owned by the government, or where interstate commerce is affected.[55] Aside from the government, the CFAA is designed in large part to protect financial harm, but hackers who steal information by way of a hotspot have access to more than just financial information. The Act does not say anything about prohibiting hackers from accessing passwords or photographs that may place a user in a compromising position. In large part, the CFAA is insufficient when it comes to adequately protecting consumers who need to be protected by large scale hacking.

---

48 *Id.*

49 Timothy B. Lee, *How a grad student trying to build the first botnet brought the Internet to its knees*, WASH. POST (Nov. 1, 2013), https://www.washingtonpost.com/news/the-switch/wp/2013/11/01/how-a-grad-student-trying-to-build-the-first-botnet-brought-the-internet-to-its-knees/.

50 *Computer Crime Laws*, *supra* note 46.

51 *Id.*

52 *Id.*

53 *Id.*

54 *See Hearing on Protecting Mobile Privacy: Your Smartphone, Tablets, Cell Phones, and Your Privacy Before Subcomm. on Privacy, Tech. and the L. of the S. Comm. on the Judiciary*, 112th Cong. 3, 8 (2011) (statement of Justin Brookman, Dir. Consumer Privacy Ctr. for Democracy and Tech.).

55 18 U.S.C. § 1030(a)(6) (2012).

Due to the common misuse of the CFAA, there have been many calls to reform it.[56] Prosecutors often mischarge a crime under the CFAA for crimes that do not constitute a true computer crime.[57] In one case in particular, a mother was charged for using a fake social media profile to bully a teenage girl over the Internet.[58] The victim of the Internet abuse in that case resulted in the suicide of the teenage bully victim.[59] The prosecution charged the mother with "'unauthorized access' to MySpace's computers for creating a fake MySpace account in violation of the website's terms of service" which requires stretching the purpose of the CFAA to fit this particular crime.[60] This case required turning a civil contract dispute into a criminal offense through the misuse of the CFAA.[61] This type of misuse is not rare, and is the reason that reform is necessary.[62] This is another area of the law where the code section prohibiting the act needs to be more narrowly tailored to fit the purpose, yet broad enough to grow and develop as technology grows and develops, however, this Note is focusing on the lack of legislation surrounding hackers accessing personal information via wireless access hotspot.

The Electronic Communications Privacy Act ("ECPA") is codified in multiple sections of the United States Code, and was signed into law in 1986.[63] The act "amended the Federal Wiretap Act to account for the increasing amount of communications and data transferred and stored on computer systems."[64] "The ECPA protects against the unlawful interceptions of any wire communication—whether it's telephone or cell phone conversations, voicemail, email, and other data sent over the wires."[65] The ECPA makes it a federal crime to access computer messages either that have been archived on a computer or in transit.[66] The ECPA does have exceptions; for example, employees of an Internet service provider to intercept an email that they reasonably believe may contain a

---

56 Kim Zetter, *Hacker Lexicon: What is the Computer Fraud and Abuse Act?*, WIRED (Nov. 28, 2014, 6:30 AM), http://www.wired.com/2014/11/hacker-lexicon-computer-fraud-abuse-act/.

57 *Id.*

58 *Id.*

59 *Id.*

60 *Id.*

61 *Id.*

62 *Id.*

63 *Computer Crime Laws, supra* note 46; Electronic Communications Privacy Act, 18 U.S.C. §§ 2510-2521, 2701-2710 (2016) (This statute was signed into law in 1986 and "protects against the unlawful interceptions of any wire communications . . .".).

64 *Computer Crime Laws, supra* note 46.

65 *Id.*

66 *Id.*

virus.[67] Also, much like traditional wiretapping, the act "allows the government to obtain a warrant to access electronic communications or records."[68]

Once again, although the ECPA sounds ideal, it is still lacking significantly. The ECPA was signed into law in 1986, which was long before hotspots started sweeping the nation.[69] This is the reason that legislation protecting unsuspecting users from wireless network hackers needs to be written in a way that allows it to grow as rapidly as technology is growing. The ECPA, much like the CFAA, is not equipped to handle the large-scale theft of information that is made widely available by the use of hotspots. "There are other laws in the federal statutes that have been applied to hacker cases. These laws aren't designed specifically to counter computer crime, but have been applied to certain cases when existing law has proved inadequate in scope . . ."[70] Some of the federal laws that have been enacted are: the Economic Espionage Act, the Wire Fraud Act, the National Stolen Property Act, and the Identity Theft and Assumption Deterrence Act.[71]

There are also state laws in place.[72] "According to a March 1999 study in Information & Communications Technology Law, 33 states have enacted their own laws to combat computer crime, while 11 more have laws pending in legislatures."[73] Almost all of those state laws make it a crime to access or use computers and databases without authority, to use a computer for fraud, or to sabotage a computer; but as discussed earlier, there are no current laws that prevent Internet sniffing.[74] To draw the distinction, it is necessary to realize

---

67 *Id.*

68 *Id.*

69 *Id.*

70 *Id.*

71 *Id.* The Identity Theft and Assumption Deterrence Act is codified in 18 U.S.C. § 1028(a)(7) and makes it a crime when one "knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or otherwise promote, carry on, or facilitate any unlawful activity that constitutes a violation of federal law . . . .". Identity Theft and Assumption Deterrence Act 18 U.S.C. § 1028(a)(7) (2012). Much like the CFAA and ECPA, this is a very specific statute that targets one effect of computer crimes, however does not prevent or punish the types of crimes that are cause by hotspots. The Identity Theft and Assumption Deterrence Act punishes those who unlawfully access information and assumes ones identification with the intent to then carry on unlawful activity that constitutes a violation of federal law. This is a high standard that is unlikely to be met by a hacker using one of the four previously mentioned methods to access personal information such as ones Facebook password unless they have the intent to then assume their identification and commit federal crimes. *See generally*, 18 USC § 1343 (2012), 18 USC § 2314 (2012), 18 USC § 1001 note (this act may be cited as the "Identity Theft and Assumption Deterrence Act of 1998.").

72 *Computer Crime Laws*, *supra* note 46.

73 *Id.*

74 *Id.*; *see also* Hill, *supra* note 44.

that sniffing the information off of a computer on its own is not per se a crime. The crime occurs when the act amounts to fraud; however there is no statute that specifically prohibits and penalizes the gathering of information on its own. The very nature of Internet crimes limits the scope of the state to enact laws prohibiting cyber crime: "while most law enforcement has historically been left to the states, states are ill equipped to deal with the extraterritoriality of computer crime."[75] Because computer crimes occur across state borders there are multiple barriers that may interfere with effectuating punishment; for example, states may not have the authority to execute search warrants, and subpoena witnesses.[76]

Although statutes are in place to attempt to prevent cyber crime, the risks presented by hotspot hackers go far beyond identity theft and fraud, by having any and all information stored on a consumer's computer accessed by hackers puts one at risk of having digital and physical property stolen.[77] If a consumer is on a public hotspot and working on a novel, it can be stolen in its entirety; this is not protected because it does not necessarily amount to fraud, and providers of public wireless Internet do not always include language in their terms and agreements that prohibits hacking on their publically available wireless networks. Hackers would also have access to online purchase history, which places users at risk of not only allowing hackers to know when and where a potentially valuable package will be delivered, but also allowing potential criminals to know their address as well. For example, if a user places an order for a valuable item while using a public access wireless network, a hacker has the ability to access the scheduled delivery date, as well as what exactly is going to be inside the package. Hackers can access a hotspot user's schedule, personal photos, files and documents, potential client information that may be relevant to a consumer's profession, and medical information.[78] Credit card fraud and identity theft is simply the tip of the iceberg, as the world has grown to rely so heavily on technology, users store more and more private information on their computers, which is why the need for laws criminalizing this type of hacking is so significant to protect consumers.

In order to properly protect consumers and providers of public access wireless Internet, there needs to be some form of legislation enacted specifically to target the type of hacking at issue. The legislation that needs to be enacted needs to be narrowly tailored to punish the crimes that hackers commit, but at

---

75 *Computer Crime Laws*, *supra* note 46.
76 *Id.*
77 *Hidden Dangers*, *supra* note 13; PRIVATE WIFI, *supra* note 24.
78 This is not an exhaustive list.

the same time it needs to be broad enough to change as technology changes. First, the statute needs to make unlawful the various types of hacking that can be done through wireless hotspot access. It is crucial to specify the types of hacking by definition but not limit it in effect by naming specific types of hacking. For example, a state could make it a felony to sit in a coffee shop and "sniff" the wireless network for users private information, and then subsequently distributing or using the credit card number for personal gain, whether that gain be a profit from selling it, or using it to purchase goods or services for personal gain. With current legislation, the act of distributing or using the credit card for personal information would constitute fraud, however, the initial act of accessing the information is not punished as a separate crime even though it is the predicating act of the fraud. Additionally, the statute would need to require providers of wireless Internet to meet certain standards to ensure that customers were protected; this topic will be later discussed, however, if a provider is going to make wireless internet available without providing adequate warnings for users they must provide protection for customers of their services. Finally, the statute needs to make clear what is protected and what is not, and from whom the information is protected. The government has the Constitutional right to access information that is shared by citizens via their electronic devices, but that does not mean that all information transmitted via electronic transmission should be accessible. If the government wants to access personal and private information that they have the right to access, their networks should have heightened security to eliminate any chance of a security breach. The statute needs to make clear who has access to the private information we store electronically, and who exactly a "hacker" is. By creating and enforcing the proper legislation, while this type of cyber crime may not be entirely prevented, is necessary to impose the proper punishment for the crime.

b. Should a computer receive constitutional privacy rights?

Before discussing whether or not the constitutional right to privacy should extend to computers, and therefore making computer crimes violations of the United States Constitution, it is important to first have a solid understanding of what rights are protected by the Constitution. The right to privacy is not expressly stated in the United States Constitution; however, the Supreme Court of the United States has said that the right to privacy can be found within the Bill of Rights.[79] For example, the Fourth Amendment prevents unlawful

[79] *Your Right to Privacy*, ACLU, https://www.aclu.org/your-right-privacy (last visited Sept. 15, 2016).

searches and seizures by law enforcement without the existence of probable cause,[80] while the First Amendment protects beliefs, the Third protects the home, and the Fifth protects one from self-incrimination.[81] American citizens also have the "freedom to make certain decisions about our bodies and our private lives without interference from the government – which includes public schools."[82] These interpretations by the Supreme Court go beyond what the text of the Bill of Rights says verbatim, which further allows for the expansion of privacy rights to adapt and grow as time passes and technology grows.

Although the right to privacy is not explicitly mentioned in the Bill of Rights, the Supreme Court of the United States has found in numerous cases that there is an implicit right to privacy that exists for United States citizens. In 1965 the Supreme Court heard the case of *Griswold v. Connecticut*, which ultimately ruled that the United States Constitution protects a right to privacy.[83] In *Griswold*, the case determined that although there is no right specifically enumerated in the Bill of Rights, it has "penumbras, formed by emanations from those guarantees that help give them life and substance."[84] Although the writers of the Constitution may not have explicitly mentioned a right to privacy, it is within the powers of the Supreme Court to infer that citizens of America are entitled to a right to privacy.

Just two years later, in 1967, the Supreme Court heard the monumental case of *Katz v. United States*.[85] The Court found that the fourth amendment's protection against unreasonable searches and seizures extends to places where one has a reasonable expectation of privacy.[86] Although this Note does not explore the potential risk that WiFi brings to unlawful searches and seizures, it is significant to note that nearly fifty years ago, long before the evolution of technology, the Supreme Court was acknowledging the importance of the privacy one reasonably expects as a citizen of the United States, whether or not they are a law abiding citizen. It is not absurd to argue that users of public access wireless hotspots expect that their information will remain personal and private. Even though it is logical and reasonable to assume that any information

---

80 *Id.*

81 Tim Sharp, *Right to Privacy: Constitutional Rights & Privacy Laws*, LIVE SCIENCE, (June 12, 2013), http://www.livescience.com/37398-right-to-privacy.html.

82 ACLU, *supra* note 80.

83 Griswold v. Connecticut, 381 U.S. 479, 485-86 (1965).

84 *Id.* at 484.

85 *See generally* Katz v. United States, 389 U.S. 347 (1967) (holding that listening to and recording a person's conversation in a public telephone booth constituted an unreasonable search and seizure under the Fourth Amendment of the Constitution).

86 *Id.* at 361 (Harlan, J., concurring).

placed on the Internet has the potential to be accessed by an unlawful third party, it is unreasonable to believe all users of Internet accessible devices live in a state of constant fear that their information is being accessed unlawfully.

Additionally, in 2014 the Supreme Court heard the case of *Riley v. California*.[87] This is significant because the Court addressed the right to privacy one has in regards to their cell phone.[88] The Court found that the reasonable expectation of privacy that was highlighted in *Katz* extends to the data on one's cellular device.[89] This case is substantial because it highlights the fact that the Supreme Court acknowledges that the information that we keep on our cell phones is private, and therefore deserves protection unless it can necessarily cause immediate harm to another.[90] The cell phone that the Supreme Court was concerned with in this case belonged to the arrestee, and the Court still found that his expectation of privacy extended to the information stored on his cell phone.[91] This case was only decided two years ago, but technology is constantly expanding, and the need for law to extend to the data users store in situations other than where they are being arrested is crucial.

There is a significant distinction between the rights guaranteed and protected by the Fourth Amendment, and rights that should be constitutionally enforced to ensure privacy rights are protected with respect to WiFi hotspots.[92] This distinction is the reason that new legislation is required to ensure the protections that are needed by citizens. While the Fourth Amendment protects against unreasonable searches and seizures, there are exceptions.[93] For example, the Fourth Amendment is not implicated by private searches.[94] In the *Katz* case, the Supreme Court determined that the Fourth Amendment does not protect information that is knowingly exposed to the public, even if the government is accessing the information.[95] It is dangerous however, for this exception to expand to say that unlawfully accessing the information that one "knowingly exposes" on the Internet is an exception to the rights guaranteed by the Fourth Amendment.

The most significant distinction is the difference between the rights of the

---

87 Riley v. California, 134 S. Ct. 2473 (2014).

88 *Id.* at 2494-95 (holding that law enforcement officers must obtain a warrant before searching an arrestee's cellphone incident to arrest).

89 *Id.*

90 *Id.* at 2494 (citing Kentucky v. King, 563 U.S. 452, 460 (2011) (holding that the need to protect against imminent injury constituted grounds for a warrantless search)).

91 Riley, 134 S. Ct. at 2478.

92 Shaina Hyder, *The Fourth Amendment and Government Interception of Unsecured Wireless Communications*, 28 BERKELEY TECH. L.J. 937, 938 (2013).

93 U.S. CONST. amend. IV.

94 United States v. Jacobsen, 104 S. Ct. 1652, 1665 (1984).

95 Katz, 389 U.S. at 351.

government to access private information versus a hacker attempting to access the private information that individuals may keep online. One major risk of providing the same exceptions to civilians as the government is the risk of identity theft. If legislation is not effectuated to properly punish those who wrongfully access the personal information of others via hotspot hacking, then there is a strong argument available for defendants to say that there is nothing prohibiting them from accessing the information that people "knowingly expose" on the Internet.

The right to privacy has grown to protect personal information and how personal information is used.[96] Many websites use "cookies" that gather "information from visitors such as name, address, email, demographic info, social security number, IP address and financial information."[97] This information is then often turned over to third parties to assist with marketing.[98] This flow of information creates a risk of fraud or identity theft, which has resulted in legislation that provides opt-out options and internal protections.[99] There have been a series of laws passed since 1974 that attempt to protect the information about individuals that is accessed; however, not all service providers are bound by law to develop protections for users.[100]

The right to privacy protects a person's personal information from public scrutiny.[101] Does hacking lead to the type of public scrutiny that the Constitution is designed and interpreted to protect? Computer hacking creates significant problems, and these problems are not limited in scope to the United States.[102]

One significant issue that courts have to deal with, since the Constitution does not protect computers, is jurisdiction.[103] If a hacker commits offenses in both the United States and Amsterdam, does the court's jurisdiction expand to cover the same offenses that technically occurred in Amsterdam?[104] What if a

---

96 *Personal Information*, CORNELL.EDU, https://www.law.cornell.edu/wex/personal_Information (last visited Sept. 15, 2016).

97 *Id.*

98 *Id.*

99 *Id.*

100 *Id.*

101 Sharp, *supra* note 82.

102 *See, e.g.*, Axel Arnbak, *9 Problems of Government Hacking: Why IT-Systems Deserve Constitutional Protection*, FREEDOM TO TINKER (Feb. 20, 2014), https://freedom-to-tinker.com/2014/02/20/9-problems-of-governments-hacking-why-it-systems-deserve-constitutional-protection/ (In response to a proposed hacking law in 2008, the German Constitutional Court created a new human right protecting the 'confidentiality and integrity of IT-systems.).

103 *Id.*

104 *Id.*

hacker is located in the United States, but using an encrypted connection violates laws in Amsterdam?[105] Which court has jurisdiction?[106]

Extending Constitutional rights to computers not only protects consumers, but also will more effectively, forcefully, and universally punish those who violate the right to privacy. However, it would be difficult to establish that the right to privacy in regards to a computer is the type of right that the Constitution was intended to protect. And while revising and amending current statutes and acts is both significant and necessary to accomplish the goal of protecting consumers from hackers, awarding Constitutional privacy rights to computer use is not likely to solve the problem, nor is it essential to solve the problem that consumers face. The difficulty with extending Constitutional rights to protect citizens from cyber crimes is the ever-evolving component that accompanies technology. For example, if the Supreme Court interpreted the Constitution to protect citizens from cyber crime and virtual identity theft via hotspots, it presents the risk of unconstitutional vagueness; a blanket ban against cyber crimes in regards to wireless hotspots may be too broad, but a narrowly tailored ban against cyber crime in regards to wireless hotspots will eventually become irrelevant because technology will outgrow the Supreme Court's ruling. For these reasons, there needs to be legislation that can organically grow with technology at a comparable rate.

c. Privacy rights are infringed upon, and deserve protection

There are measures that can be taken to protect a computer from potential hacking.[107] With the constant and rapid changes in technology however, it is only a matter of time until hackers develop a new way to access private information. Although criminals will always violate the law and take the risk of the punishment, there needs to be universal legislation that severely punishes those who specifically use public hotspots to take advantage of the unknowing and unprotected consumer. This legislation needs to be malleable, and able to grow and change as rapidly as technology grows and changes. The way the law is currently designed, the only victim is the one who has their information stolen.

Developing laws that grant privacy rights that extend to the computer risks producing a slippery slope. For example, if the law extends to protect a user's Internet search history, what does that mean for those who use the countless

---

105 *Id.*

106 *Id.*

107 *Securing Your Computer to Maintain Your Privacy*, PRIVACY RIGHTS CLEARINGHOUSE, (Aug. 2016), https://www.privacyrights.org/securing-your-computer-maintain-your-privacy.

sources available on the World Wide Web to commit crimes? This is where there most significant distinction is drawn: statutes need to be implemented to criminalize the acts of civilian hackers who compromise the private information of other citizens, and not the investigative tools utilized by the government that have the potential to compromise private information that is stored on cell phones, computers, and other electronic devices. In addition to the private information that is stored on electronic devices, one's Internet search history may potentially reveal a great deal of private information.[108] Internet search histories can reveal some of the most intimate and personal details that people value. It is naïve to believe that everything done on the Internet is secure; however, it is not unreasonable to believe that one is safe to search for information that they may find important. Because Internet search histories are so revealing, "most of us would want it to be protected against snooping and disclosure."[109] The reason it is significant to distinguish between the information that civilian hackers may obtain as opposed to the government is that one generally assumes the risk of government observation when they partake in activities online.[110] However, it is extreme to say that by placing an order online you voluntarily accept the risk of having your credit card information or address stolen by a civilian hacker.

If a law is enacted to make the obtaining and disclosing of private information on one's computer illegal, what does that mean in cases of criminal prosecutions? Specifically, the cases that involve the Internet search history of the accused in order to satisfy an element of the crime – if not the whole crime. It is unknown to the public what the policies and practices are when the government seeks search histories for criminal investigations.[111] It is important to know that "the major online search engines … log and retain information about users' search queries. The retained information includes not only the search terms entered into the search engines" but also information that allows the government to know exactly who accessed that information.[112] Which, in layman's terms, simply means that the government has ways to store information

---

108 Nathan Freed Wessler, *How Private is Your Online Search History*, ACLU (Nov. 12, 2013, 12:04 PM), https://www.aclu.org/blog/how-private-your-online-search-history ("A search for 'psychologists in Pittsburgh' is pretty revealing; a search for 'birth control morning after pill' or 'gonorrhea treatment' even more so.").

109 *Id.*

110 Sara Gates, *FBI Web Surveillance: Bureau Creates Unit To Eavesdrop on Internet Communications*, HUFFINGTON POST (May 24, 2012, 12:41 PM), http://www.huffingtonpost.com/2012/05/24/fbi-web-surveillance-secret-unit_n_1539835.html.

111 Wessler, *supra* note 109.

112 *Id.*

that is obtained by using search engines, as well as the person identifying information, that can link a user or computer to the aforementioned search.[113] This allows the search engines and government to know who accessed what information. In criminal investigations, law enforcement might be seeking two kinds of information from someone's search engine: "records of search queries entered by a particular person or persons; and a list of the names, IP addresses, or other identifying information for some or all people who have entered a particular query into the search engine's webpage."[114] The information that the search engines store then turn to aid law enforcement officers with investigations; this invites another party to access the information that is stored online.

If exceptions are made for criminal prosecutions, then where is the line drawn? It seems as though the only privacy invasion is to ensure that dangerous people get the punishment that he or she may deserve. This may open the door however, to more and more private information being collected, therefore crossing the fine line between public and private information.[115] Jared Loughner, "the alleged gunman responsible for shooting… in a crowded Arizona supermarket that left 6 dead and 14 injured, including … Gabrielle Giffords" searched the web to find Ms. Giffords' whereabouts prior to the shooting.[116] This allowed him to know exactly where the target of his crime would be, and further making his search history highly relevant to the case against him.[117] Rosario DiGorlamo admitted guilt after years of pleading his innocence after Internet search histories for "lethal karate blows to the back of the head were revealed."[118] These are prime examples of the fact that while storing this type of information may make or break a case, it also provides a greater risk to all Internet users. Additionally, it has to be proven that the identifying factors and search queries actually belong to the person who is charged with the crime.[119] These are prime examples of the fact that while storing this type of information may make or break a case, it also provides a greater risk to all Internet users. Additionally, it has to be proven that the identifying factors and search queries actually belong to the person who is charged with the crime.[120] This therefore creates the necessity for ones identifying features to be stored alongside their

---

113 *Id.*

114 *Id.*

115 Louie Helm, *Anything You Search For Can and Will Be Used Against You in a Court of Law*, SINGULARITY HUB, (Feb. 15, 2011), http://singularityhub.com/2011/02/15/anything-you-search-for-can-and-will-be-used-against-you-in-a-court-of-law/.

116 *Id.*

117 *Id.*

118 *Id.*

119 *Id.*

120 *Id.*

Internet activity, which presents the troublesome situation of how and where that information is stored and whether or not it is easily accessible. If the government is able to do back end searches through the search engine queries of a potential murder suspect, how and where that information is stored may present a series of risks. While accessing secured information would require the use of a subpoena,[121] the information is still being stored and a skilled hacker would be able to access it. In addition to that risk, the simple fact that the government is permitted to access and store this type of information may mean running the risk of leaving innocent people susceptible to hacking. This is not to argue that the government is unreliable with personal information, it is just particularly troublesome considering the fact that throughout the years hackers have successfully accessed the private information of many citizens that is typically stored and maintained by the government.[122]

While most people can accept the fact that access to Internet search queries and identifying information can be used to prosecute those who have committed heinous crimes, they are not ok with their personal identifying information being accessed.[123] The use of Internet search queries in criminal investigations creates a potential slippery slope for privacy rights. A method of encryption that is so secure cannot exist because it could potentially prevent the government from accessing information that is necessary for a criminal conviction in a serious crime; however, leaving doors for the government to enter open

---

121 Daniel Zwerdling, *Your Digital Trail: Does the Fourth Amendment Protect Us*, NPR (Oct. 2, 2013), http://www.npr.org/sections/alltechconsidered/2013/10/02/228134269/your-digital-trail-does-the-fourth-amendment-protect-us.

122 *See generally* Julie Hirschfeld Davis, *Hacking of Government Computers Exposed 21.5 Million People*, N.Y. TIMES, July 10, 2015; Nir Kshetri, *Why the IRS Was Hacked Again and What the Feds Can Do About It*, U.S. NEWS (Feb. 16, 2016), http://www.usnews.com/news/articles/2016-02-16/why-the-irs-was-hacked-again-and-what-the-feds-can-do-about-it; *US government hack stole fingerprints of 5.6 million federal employees*, THE GUARDIAN (Sept. 23, 2015. 5:44 PM), https://www.theguardian.com/technology/2015/sep/23/us-government-hack-stole-fingerprints.

123 Helm, *supra* note 116.

> While at first glance, it appears that any invasion of privacy will only insure that Federal prosecutors are able to give a dangerous man the punishment he deserves, it also continues a trend of admitting more and more private information from suspects' computers into court rooms and is a reminder of how little privacy exits online these days. Information posted on sites like Facebook and MySpace have already been used by police, probation officers, and university officials to punish criminals who were dumb enough to make information of their wrongdoing public.

Id.

leaves doors for hackers to potentially walk through as well. So lawmakers must decide what is more important: the government's need to access information on the computers of others versus the privacy rights one holds in their computer.

The government had the burden of proving crimes before the existence of the Internet, and therefore the personal information and identifying factors that are available to assist in criminal prosecutions should not weigh more than the privacy rights that consumers face and frequently lose by using hotspots. It would be ignorant to say that the evolution of technology has not come in to assist with very serious criminal prosecutions, however, it is also significant to acknowledge the importance of protecting consumers from hackers. Computers can become accessible to prosecuting attorneys via subpoena or court order,[124] but it is not that simple to protect one's personal information from hackers. The information that needs to be protected from hackers is not always the kind of information that would be relevant in a criminal prosecution; the private and personal information that is at risk and that requires protection is the type of information that will open up an unsuspecting civilian to identity theft. So, although accessing one's Internet search history may be impacting the way in which criminals are being prosecuted, that does not mean that it is acceptable to further expose civilians to the risk of having their personal and private information stolen.

d. Can consumers be completely safe?

"If a hacker can get into a machine, they can see every sensitive file, even if it's not open at the time."[125] Even if public hotspot users accept the fact that their personal information transmitted online is always at a potential risk of being hacked, it is a common misconception that information stored on the device itself is inaccessible.[126] So long as the hacker can access the wireless network that a consumer is on, they can see every single file stored on the computer.[127] For some people this information may just be a thousand photographs of cute dogs, and some school work, while others may store very secure information on their computers, and therefore put themselves and potentially others at risk of having that information accessed by the wrong person.

---

124 Zwerdling, *supra* note 122.

125 Dirk Gates, *5 tips for using public Wi-Fi securely*, INTRO WORLD (Nov. 24, 2015), http://www.infoworld.com/article/3007288/network-security/5-tips-for-using-public-wi-fi-securely.html.

126 *Id.*

127 *Id.*

In an ideal world, a new law would be enacted that deters the type of hacking that commonly occurs on public hotspots, but until then, there are five ways that users can secure their information.[128] Unfortunately, all of these methods require that users take an extra step to protect their computers, which may be asking a lot of those less technologically savvy users.[129] First, users can use a two-factor authentication system.[130] This allows users to follow a few extra steps that can block most illegitimate actors from their device.[131] This sets up a security system that requires an extra step; therefore "even if a bad guy sniffs a users password, the password alone won't provide access to the company system."[132] This is not necessarily the most secure method, but it is a step above the default settings a device is equipped with out of the box.[133] Realistically, getting every electronic device user to install extra methods of protection is unlikely; however this is one option that increases the protection that a civilian has on their computer. Second, users should beware of open service set identifiers ("SSID").[134] A SSID is a unique set of thirty-two characters that is unique to each wireless network.[135] SSIDs are used to ensure that information is sent to the correct location when there are numerous wireless networks in a single location.[136] "Once a device has joined a specific network, it will jump back onto that network whenever the user is within range."[137] In order to prevent this, users should turn off or delete any saved hotspots saved on their phone.[138] This requires users to be diligent with when and how frequently they sign into a hotspot; this may be complicated because there are options available on cell phones and tablets that have the device automatically connect to any hotspot they may walk through. Users need to be aware of the settings that are preset on their electronic devices, and pay specific attention to the wireless networks that they connect to outside of the home. All users should take a minute and go through what wireless networks are stored on their mobile devices and delete all but the network used at home and work.

Third, users should always verify the network that they are connecting to

---

128 *Id.*
129 *Id.*
130 *Id.*
131 *Id.*
132 *Id.*
133 *Id.*
134 *Id.*
135 *SSID*, TECHTERMS, http://techterms.com/definition/ssid (last visited Sept. 15, 2016).
136 *Id.*
137 Gates, *supra* note 126.
138 *Id.*

which they are connecting.[139] Verifying a network is as simple as asking the provider if the named network is theirs, rather than trusting that the strongest connection is the proper one.[140] Although this task could not be simpler, it is crucial; if a user is connecting to a network in a public place, they should not sign on to it unless they have inquired as to whether or not that is the proper network from the service provider. This step requires only walking up to an employee and asking if the network that is available is the one that they provide. Protecting private information on an electronic device and be as simple as walking up to the cashier at the coffee shop or restaurant that one is in and asking if the network that is unlocked or available is the one that the coffee shop or restaurant provides for their customers. Fourth, it is important for users to avoid logging in to websites that require log in credentials.[141] This is not saying that users should not use verified hotspots that require a log in, this is saying that one should be cautious about logging in to any website that requires using personal information for access. For example, while shopping online in public may be fun and aid in passing the time, it is crucial to wait until logging in to a highly secured or home wireless network before entering home address or credit card information.

The fifth, and most secure option, is to use a virtual private network.[142] Virtual private networks were briefly introduced earlier in this Note; however, they are significant as they provide a solution to the hacking problem other than new laws. A virtual private network ensures a secure connection, which directs "all network traffic (data, voice, and video) through a secure virtual tunnel between the host device (client) and the virtual private network provider's servers, and is encrypted."[143] There are free virtual private networks available; however, they are limited and not necessarily reliable or safe.[144] The more reliable cheap virtual private networks have a subscription fee ranging from $3.00-$10.00 a month.[145] In order to protect consumers from hotspot hacking, who should be reliable for these costs? In theory, it would be cheaper and easier for the provider to provide a virtual private network service. Unfortunately, virtual private networks must be installed on the device that is actually access-

139 *Id.*
140 *Id.*
141 *Id.*
142 *Id.*
143 *What is a Virtual Private Network (VPN)?*, HOTSPOT SHIELD, https://www.hotspotshield.com/learn/what-is-a-vpn/ (last visited Sept. 26, 2016) [hereinafter *VPN*].
144 *5 Best Cheap VPNs – 2016 Update*, BEST VPN, https://www.bestvpn.com/blog/38185/5-best-cheap-vpns-2016-update/ (last visited Nov. 4, 2016).
145 *Id.*

ing the hotspot.[146] Therefore, in order to receive the highest level of security users must seek additional protection, which may not only be difficult for those who are less than tech savvy, but causes users to incur additional costs to protect against something that should be prohibited by law. While the virtual private networks can seemingly protect users from all risks posed by hackers, it is not an easy fix, which is why a law that can protect all users is the only guaranteed fix for all consumers and providers alike. Although users have options to protect themselves from hackers in theory, it is necessary to enact some form of legislation to further protect users from hackers. It is of the upmost necessity because hackers advance at the same rate, if not faster, than the speed at which users can protect themselves. This presents the recurring problem where the law meets technology.

The law is a slow moving process, while technology grows at a rate that even today's most technologically advanced users may struggle to keep up with. Hackers and others who specialize in technology are aware of its rapid development and constantly work to keep up with the changes. Therefore, legislation needs to be drafted and effectuated in a way that allows it to grow, develop, and adapt to the latest technologies.

e. Proposed Legislation

The need for legislation to protect computer privacy is necessary. Hackers accessing the personal information of unsuspecting users present the ever-prevalent risk of identity theft.[147] The main problem with identity theft is that it "costs billions of dollars."[148] A downfall of identity theft is that people do not always see the charges or realize their credit cards have been stolen until they see the charge and it is too late to cancel their card.[149] In response to the large issue with identity theft, President Obama introduced the Student Digital Privacy Act to Congress, which "would prevent companies from selling information of a student to third parties wherein the purpose is not related to education but for others such as advertising."[150] It is designed to protect student privacy by preventing universities from selling student information, including but

146 Gates, *supra* note 126.

147 *Id.*

148 Menchie Mendoza, *Obama Wants Tougher Law to Protect Internet Users from Hacking, Identity Theft,* TECH TIMES, (Jan. 13, 2015, 11:12 AM), http://www.techtimes.com/articles/26237/20150113/obama-wants-tougher-law-to-protect-internet-users-from-hacking-identity-theft.htm.

149 *Id.*

150 *Id.*

not limited to email addresses, unless that purpose is educational.[151] "Obama also called for a bill of rights that would focus on data privacy … a concept that he had introduced back in 2012."[152] This bill would allow citizens to know what information online retailers and companies are collecting about them, and how that information is used.[153] This bill would allow citizens to demand that their data only be used for the purpose for which it was given.[154] Additionally, this bill would compel companies to use heightened security when housing client's personal information.[155] Bills such as the one proposed by President Obama in 2012 force companies to use secured systems.[156] Contrastingly, businesses that provide hotspots are not required to ensure that the information that is potentially accessed in their business or through their hotspot is secured.

President Obama also proposed amending the CFAA in response to a hacking attack against Sony that occurred in 2014.[157] Currently, the CFAA requires the intent to defraud, but President Obama's proposal lowers the standard to willfully.[158] The fear many have with this lowered standard is that one can be accused of hacking simply by clicking on the wrong link, or being on a forum where hacking is being discussed.[159] There are reservations that this statute is too broad, and therefore many can find themselves "unwittingly" in danger.[160] Therefore, it is essential for legislation to properly define the terms to protect those who accidentally put themselves in a compromising position.

Although this legislation may not be flawless, it is a step in the right direction. It is important for legislation that protects individual's rights from hackers to continue being proposed and modified in a way that effectively protects public hotspot users. The proper legislation walks a fine line and must be worded in a way that delicately protects those who are vulnerable to hacking, yet properly punishes those who violate the privacy rights of the trusting and unsuspecting hotspot user.

Unfortunately, this legislation is not foolproof. This proposed legislation prevents stores from selling information or providing information to third par-

---

151 *Id.*
152 *Id.*
153 *Id.*
154 *Id.*
155 *Id.*
156 *Id.*
157 Owen Williams, *Obama's Proposed Hacking Law Could Unwittingly Make You a Criminal*, THE NEXT WEB (Jan. 15, 2015), http://thenextweb.com/insider/2015/01/15/obamas-proposed-hacking-law-unwittingly-make-criminal/#gref.
158 *Id.*
159 *Id.*
160 *Id.*

ties, and therefore requires heightened protection, however, this does not necessarily prevent hackers from accessing secure information. Although this does not directly address the problem, it is a step in the right direction because limiting the information that is distributed digitally aids in lowering the amount of information that is available. To put this concept simply, it is equivalent to an item being sold for a limited time only; the less quantity that exists, the less accessible it is. By preventing the distribution of personal information to third parties, there is one less opportunity for hackers to access private information. Currently, hackers are not punished for their initial "sniffing" actions as long as they do not use the information in an unlawful way. This is an issue because the same way that not all crimes are punished equally, not all computer crimes are the same and need to be addressed as their own individual act. Hacking by way of sniffing, or seeing up an evil twin, or any of the aforementioned methods, is not legally prohibited, and that is the issue. Aside from the fraud issue, wiping all information off of one's computer presents issues that go beyond what one is capable of conceiving.

f. Liability

Another complication with online hacking is determining who is at fault. Should the hotspot provider be at fault for not protecting their customers, or should the hacker be solely responsible? Should all Internet service providers be responsible for taking adequate measures to encrypt their services so that accounts cannot be hacked? As previously discussed, there are numerous ways that users can protect their computer, but the only way that a user can fully protect their computer is by using a virtual private network.[161] So should a user be at fault for not taking the measures to install a virtual private network?

Can Internet service providers ensure that their users are safe? Google "encrypts the Gmail connection between your computer and Google – this helps protect your Google activity from being snooped on by others."[162] Google uses a function "known as session-wide SSL encryption, the default when you're signed into Google Drive and many other services."[163] Secure Sockets Layer ("SSL") encryption "is a standard security technology for establishing an encrypted link between a server and a client – typically a web server (website)

161 *VPN*, *supra* note 144.

162 *Keep Your Stuff Secure and Private*, GOOGLE, https://www.google.com/safetycenter/everyone/start/safe-networks/ (last visited Nov. 4, 2016).

163 *Id.*

and a browser; or a mail server and a mail client."[164] An SSL encryption ensures that information that should remain secure, such as credit card or social security numbers, is transmitted securely.[165] However, SSL certificates, like virtual private networks, require a monthly or annual subscription fee.[166] So once again, who should be responsible for these costs? Should this be a feature that comes default on any electronic device that has online browsing capabilities?

SSL certificates and virtual private networks are essentially useless when hackers gain access through a public hotspot, but swipe all information saved on, downloaded by, sent or received from that computer. In order to effectuate liability, there must be legislation in place that makes hacking or sniffing a hotspot a crime. Although it seems as if users can protect themselves with virtual private networks, and service providers can protect users with SSL encryptions, with technology and hackers evolving at the same speed, it is unlikely that the risks presented by public hotspots will ever be truly rectified without proper legislation. Liability is another issue that exists due to the lack of privacy protection currently in place. Although legislation or statutory solutions may be elaborate and complex, it is necessary. Should legislation be enacted to prevent these breaches of privacy, there would need to be a section that specifically issues roles to citizens and service providers. For example, restaurants that provide wireless hotspots for paying customers should be required to implement certain standards and guidelines to protect customers. Requiring all users to have a virtual private network installed on their computer could do this. Requiring users to agree to specific terms that prohibit sniffing or hacking

---

164 *What is SSL (Secure Sockets Layer) and What are SSL Certificates?*, DIGICERT, https://www.digicert.com/ssl.htm (last visited Nov. 4, 2016).

165 *Id.*

166 Jennifer Kyrnin, *The Cheapest SSL Extended Validation (EV) Certificates*, ABOUT TECH (May 8, 2014), http://webdesign.about.com/od/ssl/tp/cheapest-ev-ssl-certificates.htm; *What is an SSL Certificate?*, GLOBAL SIGN, https://www.globalsign.com/en/ssl-information-center/what-is-an-ssl-certificate/ (last visited Sept. 15, 2016).

> SSL Certificates are small data files that digitally bind a cryptographic key to an organization's details. When installed on a web server, it activates the padlock and the https protocol and allows secure connections from a web server to browser. Typically, SSL is used to secure credit card transactions, data transfer and logins, and more recently is becoming the norm when securing browsing of social media cites. SSL Certificates bind together: a domain name, server name or hostname [and] and organizational identity and location. An organization needs to install the SSL Certificate onto its web server to initiate secure sessions with browsers. … Once a secure connection is established, all web traffic between the web server and the web browser will be secure. Browsers tell visitors a website is SSL secure via several visible trust indicators.

Id.

could also do this. Although it is rare that terms and agreements are read, there are still contracts that are agreed to by the users.

IV. CONCLUSION

The current relevant statutes and laws are subpar at best when it comes to protecting users from the dangers of hackers sniffing hotspots and stealing information. Until there is satisfactory legislation implemented to protect consumers from all forms of hacking, users are at risk of having all information on their device stolen simply by using a network that was previously logged into and saved by the device. This should raise red flags for all electronic device users because without a virtual privacy network, private information can be hacked simply by walking through an area where wireless Internet is available. The risk is high, and the barriers protecting citizens is low, which is why governmental protection is the only real answer.

Although it is a stretch to say that computers and users deserve the Constitutional right to privacy, there are privacy rights being infringed, and stricter laws need to be enacted in order to protect users from not only having their identities stolen, but also any and all personal information on their computer. It has been made evidently clear that there are measures that users can take to hopefully ensure their safety when using public hotspots, however technology is not without its faults, and therefore trusting it alone is not enough.

Allowing hackers to sniff and eavesdrop on hotspots without proper laws enacted to prevent it is an infringement of privacy rights, and laws enacted to properly punish those who commit these crimes should protect consumers. It is not that this type of hacking is going unnoticed; rather there is no proper way to punish it. Legislation should be proposed and passed making it a serious offense to not only trespass onto public hotspots, but to impose severe punishment for accessing any information that the victim may have stored on their computer – whether or not the hacker finds the information to be significant. The main issue with the CFAA and current legislation is that it is too strict and therefore unlikely that hackers violate it by accessing information through public hotspots. Most people would not just drop their beloved pet off with a stranger, thereby giving up any control over the protection and safety of said pet, so why do that with your computer?