Unauthorized Access Crimes

By
Stephen Steh

Submitted in Partial Fulfillment of the Requirements
for the Degree of

Masters of Science in Criminal Justice

in the

Department of Criminal Justice and Forensic Sciences

Youngstown State University
July, 2009

Unauthorized Access Crimes

Stephen Steh

I hereby release this thesis to the public. I understand that this thesis will be made available from the OhioLINK ETD Center and the Maag Library Circulation Desk for public access. I also authorize the University or other individuals to make copies of this thesis as needed for scholarly research.

Signature:

_____

Stephen R. Steh, Student Date

Approvals:

_____

Patricia Wagner, Thesis Advisor Date

_____

James Conser, Committee Member Date

_____

Gordon Frissora, Committee Member Date

_____

Peter J. Kasvinsky, Dean of School of Graduate Studies & Research Date

Abstract

This paper examines the concept of unauthorized access crimes statutes in the fifty states and the federal system in order to determine the concept of what exactly the crime of unauthorized access constitutes. This paper will also determine whether these same crimes could be prosecuted under preexisting statutes that were already in effect in the United States criminal codes prior to the invention of the computer. Through a review of previous literature on the subject of computer crime laws, and more specifically unauthorized access laws, additional insight as to the purpose and intent of these laws will also be drawn. Case law on unauthorized access and any related criminal activity will also be examined. This information will help to determine whether the intentions of the legislatures have been to criminalize what is commonly referred to as hacking.

Acknowledgments

I would like to thank all of those who helped during the process of this thesis. I would first like to thank my thesis advisor, Atty. Patricia Wagner, who has had to read through so many different drafts of this research. I would also like to thank my committee members, Dr. James Conser and Dr. Gordon Frissora, who provided invaluable insight, and plenty of reading material on the subject of computer crimes. I also have to thank the department secretary, Patty Stanovcak who helped me as I was stumbling through all of the official paperwork and procedures. I also need to thank my fellow graduate assistants, Kelly, Justin and Phil, who were also writing their theses at the same time. They provided a much needed sounding board for ideas. Last but not least I have to thank my parent Stephen and Kim, my stepfather Jeff and my sisters Sarah and Rebecca, who had to put up with me as I researched and wrote this thesis.

Table of Contents

Signature Page i

Abstract ii

Acknowledgements iii

Table of Contents iv

Chapter 1 – Introduction 1

Hacking 3

Computer Crime Legislation 6

Unauthorized Access 9

Research Questions and Reasons for Study 10

Chapter Summary 11

Chapter 2 – Literature Review 12

Research Questions 25

Chapter Summary 25

Chapter 3 – Methods 27

Data 27

Chapter Summary 30

Chapter 4 – Results & Findings 32

Legislative Definitions 32

Unauthorized Access Legislation 35

Case Law 39

Results Summary 42

Chapter Summary 45

Chapter 5 – Conclusions 47

Chapter Summary 51

Bibliography 52

Appendix A Statute Chart 55

Appendix B Court Cases 59

CHAPTER 1

INTRODUCTION

Computers affect almost every facet of life in today's society. Everyday tasks often require interaction with some sort of computer. Whether it is the personal computer that may be used in a work environment, the automated teller machine used to withdraw cash, or a personal computer used at home, there is a high likelihood of interaction with a computer on a daily basis. With this increasing reliance on computers, it is almost inevitable that the computer becomes a target or an instrument in criminality. Computer crimes cover a broad swath of offenses, varying from crimes where the computer is incidental to the crime, to those crimes where the computer, or the information held therein, is the target. Traditional crimes such as money laundering, stalking, espionage, vandalism, and identity theft have all begun to migrate from their analog roots to the digital frontier.

The computer has become a necessity in the modern world, and its infiltration into every life was rapid. It was only three decades ago that the legislative bodies began to address computer crimes with their own statutes. The networks that were in existence were relegated to use by universities and the scientific community. It was only two decades ago that the personal computer began to work its way into homes and not just places of business. The World Wide Web was in its infancy, yet to fully recognize its potential to change the way we interact, learn, and conduct daily tasks. A decade ago the true potential was starting to be seen, albeit at relatively slow speeds. Only within the

last ten to fifteen years, has the personal computer and the internet started to evolve into a needed device for communication, business and commerce.

Computer crime, often referred to as cyber crime, takes on many different forms. When dealing with computer crimes there are generally three different categories that come about (Brenner, 2004). The first category of computer crime involves those offenses where the computer, or the information it contains, is the target. The second category involves crimes where the computer is used as a tool in the commission of the crime. The final category involves those crimes where the computer is simply used during the commission of a traditional crime, such as a drug dealer maintaining records of transactions on a computer.

Many crimes have come to the attention of the media and the public over the past few decades that are either a result of or spurred on by the increasing use of computers. The crime of identity theft has existed long before computer use became rampant; however, it has become increasingly easy to commit identity theft. Traditionally identity theft relied on discarded bills, or other mail that was retrieved while "dumpster diving", or going through a person or corporation's trash. Another option for those who wanted to steal someone's identity was to steal mail from their mailbox to obtain personal information.

Now, with more and more households containing some sort of personal computer, the information can be obtained in new ways. Phishing scams have developed as a popular way to obtain information such as social security numbers, maiden names, and bank account numbers. Phishing involves the creation of authentic looking emails from websites of banks or federal offices in an attempt to coerce a person into voluntarily

submitting their personal information in response to the fraudulent website or email. The offender then uses the information gained to withdraw money from existing accounts, create new accounts, or open credit card accounts, just to name a few uses for the ill gotten information.

It is the crimes where the computer is the target that will be the focus herein. These are the crimes that have created an entirely new branch of legislation involving computer specific crimes. The other two types of computer crime related offenses are covered under other statutes that existed before the invention of the computer. For example, the drug dealer keeping his records electronically will still be prosecuted for the sale of a controlled substance; the information on the computer will simply be used as evidence in the state's case.

Hacking

The first crime that comes to mind for most where the computer is the target of the offender would more than likely be hacking as it has come to be known. Hacking can trace its roots back to the first analog telephone systems. The art of "phone-phreaking", or exploiting the phone system, can be seen as the first instances of hacking. Over the years, those who can be viewed as early hackers would use various means to place free phone calls and get around the automated switching systems. The magazine *2600: The Hacker Quarterly*, owes its name to a discovery in the 1960's that involved the use of a plastic toy whistle that produced a tone at 2600 hertz, which could gain the person access

to operator controls in the phone system. The 2600 hertz whistle was easily found as the free toy in the Cap'n Crunch cereal.

The use of this exploit was discovered and capitalized on by John Draper who then used a 'blue box", a device that is used to create various tones, in order to gain control of long distance switching systems. After the phone companies and the authorities found Draper, he was charged under the federal laws concerning wire fraud, under U.S.C. Title 18, section 1343 (Draper, 2007). This section is still used today in the prosecution of modern day computer crime cases which involve fraud, such as phishing or credit card fraud.

The art of phone phreaking continued to grow out of this original discovery. The early phone phreakers used blue boxes, which obtained their name from the first one confiscated by police having been the color blue, to manipulate the electromechanical switches that were used by the phone companies that operated on the same circuit as the voice transmissions (Wang, 2006). Once the phone companies changed their systems to electronic switching, the phone phreakers found new electronic methods to hack the phone systems (Wang, 2006). These activities of phone phreakers laid the foundation for future activities of hackers, who are often viewed as the stereotypical computer criminal.

Merriam-Webster's dictionary defines hack as it relates to computers as "to write computer programs for enjoyment or to gain access to a computer illegally." Merriam-Webster's also defines a hacker, as it relates to computers as "an expert at programming and solving problems with a computer or a person who illegally gains access to and sometime tampers with information in a computer system." The Oxford Compact Dictionary defines hack as "use a computer to gain unauthorized access to data." The

National Conference of State Legislatures (NCSL) dedicates a page to "Computer Hacking and Unauthorized Access Laws" on their website, wherein they define hacking: "Hacking is breaking into a computer system, frequently with the intention to alter or modify existing settings. Sometimes malicious in nature, these break-ins may cause damage or disruption to computer systems or Networks."

Hacking is often given a negative connotation. The general public, through some fault of the mass media, hear the term hacker and assume the worst. Hackers, however, are not all malicious. Many simply seek to gain knowledge and further their understanding of how things work. Those who wish to commit malicious acts are often referred to as crackers, especially by those who consider themselves hackers. The "cracker" nomenclature has begun to infiltrate the mainstream, The NCSL website specifically states, "people with malevolent intent are often referred to as "crackers"—as in "cracking" into computers." There have been three different types of hackers that have been recognized for many years. These three types of hackers are referred to as black hats, grey hats and white hats.

The first of the hackers is the black hat. The black hat is the closest to the stereotypical negative view of the hacker. The black hats are the hackers that break into systems for the purpose of causing damage and chaos (Knetzger, Muraski 2008). The black hats are looking for any exploits that allow them to cause damage or steal information, and they have no qualm with dispersing the information of software exploits to fellow hackers. The rest of the hacker community, in an effort to differentiate themselves from the black hats, refers to this type of hacker by the term of "cracker" (Knetzger, Muraski 2008).

The grey hat hackers are those who stand on the fine line between that of white hat and black hat hackers. The grey hat hackers seek out exploits in networks and software and will supply that information to both the black hat and white hat hackers (Knetzger, Muraski 2008).

The final category of hacker is that of the white hat. This is the hacker that will find security exploits and flaws in networks and software, and instead of divulging them to the rest of the hackers, they will notify the owners of the software or network (Knetzger, Muraski 2008). This allows for the owners to patch any problem before it is exploited for malicious purposes by a black hat hacker. The white hat hackers can often find employment with organizations for the purpose of discovering flaws before they become major issues (Knetzger, Muraski 2008).

Computer Crime Legislation

Legislation for computer specific offenses began to spring up in the mid to late 1970's amid criminal cases involving computer crimes, with varying outcomes. For example, the Supreme Court of Virginia determined in March of 1977 that there was no property interest in the labor, services or printouts of a university computer that was accessed without authorization by a Virginia Polytech doctoral candidate. Charles Lund was originally charged with, and found guilty of, grand larceny of keys, computer cards, and the use of computer time and services; Lund v. Virginia, 217 Va. 688 (1977). However, in a 1978 case that reached the United States Court of Appeals, a defendant's guilty verdict was affirmed after he was convicted of fraud by wire for using a spy

program to attempt to defraud his former employer of property that consisted of information that was held in the computer systems the company maintained, United States of America v. Seidlitz, 589 F.2d 152 (1978). In this case the courts took the view that there was a property interest in information contained on the computer that was being transmitted via phone lines back to Seidlitz. These two examples serve as two early opinions of computer crimes that were prosecuted under laws not meant to deal directly with computer related offenses, each with differing results.

Laws designed to directly combat computer crimes began to appear in the late 1970's, with Florida being the first state to pass a law directed at computer hacking. The Florida statute addressed unauthorized use of a computer and misuse of a computer, computer hardware or software. Within twenty years every state had statutes directed at computer related crimes, with the last state to pass a computer statute being Vermont in May of 1999 (Kerr, 2003). The federal government passed its first computer crime law in 1984, which was the Counterfeit Access Device and Fraud and Abuse Act (18 U.S.C. Sec. 1030). This act made it a misdemeanor to take protected information via unauthorized access to a federal government computer, or any computer involved in interstate commerce.

The U.S. Department of Justice has laid out many crimes that can be committed via a computer and the appropriate federal laws that apply to each of the crimes. The Department of Justice, in published documents on prosecution of computer crimes (Prosecuting Computer Crime, Office of Legal Education, 2007), lists approximately thirty offenses and the accompanying federal statutes that they can be prosecuted under. These statutes vary in the degree to which they target computer crimes specifically, and

many of the offenses have multiple statutes under which prosecution can be pursued. The statute on wire fraud (18 U.S.C. Sec. 1343), used to prosecute the first phone phreakers, is still used today in the prosecution of such crimes as internet fraud, which in turn encompasses such acts as phishing and online auction fraud. The statute on wire fraud can also be used to prosecute crimes such as credit card fraud, password fraud, sales of prescription drugs or controlled substances, securities fraud, and piracy and theft of intellectual properties (Office of Legal Education, Prosecuting Computer Crime, Appendix A).

The Crimes and Criminal Procedures Title 18 is but one section of the United States Code that can be used to prosecute those who have committed various crimes that involve the use of a computer. The Department of Justice also considers Titles 15 (Commerce and Trade), 17 (Copyrights), 21 (Food and Drug), 27 (Intoxicating Liquors), 28 (Judiciary and Judiciary Procedures), and finally title 47 (Telegraphs, Telephones, and Radiotelegraphs) to contain sections that may be appropriate in the prosecution of various computer related crimes (Office of Legal Education, Prosecuting Computer Crime, Appendix A).

These are just some of the examples of the federal laws that have been put in place or used to prosecute various computer related offenses. However, the focus of this thesis will be on the crime of "unauthorized access". It is this language that is consistent throughout the laws that have been adopted over the last thirty years.

Unauthorized Access

The phrase "unauthorized access" is one that appears in all of the computer crime statutes throughout the states and the federal government. The terms are found in variously named statutes, but all have similar characteristics that make them the statutes that best address the crime of hacking. The crime of hacking can best be viewed as a trespass into a computer system; in fact, some states refer to their unauthorized access crimes by the name of computer trespassing and house them with the traditional trespassing statutes (Indiana code 35-43-2, Burglary and Trespass).

In the federal code the section dealing specifically with hacking, or unauthorized access, is section 1030 of Title 18, Fraud and Related Activity in Connection with Computers. This section addresses the unauthorized access of a computer for reasons of obtaining information or to cause damage. More specifically the section also addresses dissemination of malicious code such as viruses in the following section: "knowingly cause the transmission of a program, information, code, or command, and as a result of such conduct, intentionally cause damage without authorization, to a protected computer" (18 U.S.C. section 1030 (a) (5) (a) (i)). Section 1030 of Title 18 addresses those crimes that are commonly thought of as hacking as it pertains to government interests.

The section also covers what Brenner (2004) referred to as simple hacking and aggravated hacking. Simple hacking is merely gaining the access to a system of which the perpetrator does not have authority to access (Brenner, 2004). Aggravated hacking on the other hand not only involves the unauthorized access of a computer system, but also the commission of a crime once access is gained (Brenner, 2004). Many states also

make this distinction between that of simple hacking and aggravated hacking in their criminal statutes (Brenner 2004).

State statutes have adopted similar language and divisions of simple and aggravated hacking, each with their own unique spin on the crime. The focus of this endeavor will be on these varying unauthorized access statutes and the commonalities and differences that exist across the states and federal system. This allows for a comparison of fifty-one different versions of unauthorized access crimes that will be examined.

Research Questions and Reasons for Study

The first reason for studying these fifty-one different versions of unauthorized access law is to determine, to the extent possible, what exactly unauthorized access is. As it has been stated earlier, the language "unauthorized access" is common among these computer crime statutes. The phrase unauthorized access can be seen as the offense name, or the language inside of offenses such as computer misuse or computer trespass. Included within this study of unauthorized access computer crimes will also be an analysis of relevant court cases that have dealt directly with the concept of unauthorized access. At first blush, these unauthorized access laws appear to be targeted at what has traditionally been known as hacking and through further examination of theses statutes it is also hoped that it can be determined if this is the sole purpose for these statutes.

The need for these unauthorized access statutes will also be examined. As it was noted earlier, the resemblance to trespassing and occasionally theft statutes is

unmistakable, which begs the question of whether these unauthorized access statutes are needed or whether traditional trespassing and theft statutes would suffice for prosecution. The removal of redundant statutes could help to simplify the web of computer crimes legislation.

Chapter Summary

The chapter began with an introduction to computer crime. The history of unauthorized access and hacking was covered in this chapter. The statutes and court cases that will be elaborated on were briefly discussed. The first computer related statutes were discussed along with example court cases that may have prompted their creation. In the following chapter the literature on the subject of unauthorized access will be reviewed, along with those readings on computer crime that may be pertinent to unauthorized access.

CHAPTER 2

LITERATURE REVIEW

The rapid rise of the computer, especially the personal computer, has created a unique set of circumstances that have fueled the creation of legislation to address crimes that did not fully exist prior to the computer. In the last thirty years there has been a swell of legislation directed at computer crimes that were not needed in prior decades. This unique phenomenon of what was almost a legislative blank slate in regards to computer crime has given rise to a wide variety of research in the area of computer crime.

Computer crime also has the distinct feature of being multi-jurisdictional, which means that many studies involving computer-related crime begin by examining international law. Much of the research that is available focuses on many different countries, or international means of combating computer crimes through legislation. Earlier research examined the need for the flurry of computer crime legislation that took place during the 1980's.

A study by Raymond Michalowski and Edwin Pfuhl (1991) looked at the cause of this upsurge in computer crime related legislation. Michalowski and Pfuhl (1991) begin their examination of the reason for the surge in computer crime legislation with the fact that many of its proponents claimed that there was a high potential for a rash of computer based crime to occur. These proponents also suggested that new legislation was then required to combat this upcoming surge in computer crime. Michalowski and Pfuhl (1991) further state that there is very little evidence that the criminal justice system could not successfully apply the laws that already existed to combat this wave of computer

crime. It is also noted that the general concern among the population for computer related crime was almost non-existent.

Michalowski and Pfuhl (1991) suggest that one of the possible reasons for the low level of computer crime was that law enforcement did not recognize computer crimes because of the lack of legislation. They therefore concluded that the passage of these new computer crime statutes would cause an upsurge in the arrest rate for computer related crimes. The authors also contended that this would be very difficult to measure due to the fact that very little information is collected about the arrest rates for computer crime and the Federal Bureau of Investigation's Uniform Crime Report (UCR) did not maintain data on the subject, and still does not.

Due to this lack of information Michalowski and Pfuhl (1991) created a questionnaire for prosecutors to determine the number of computer crimes that were occurring across the country. Michalowski and Pfuhl (1991) sent out questionnaires in 1986 to 35% of county prosecutors in states that had computer crime laws. This excluded four states that had no such law at the time; Arkansas, Vermont, West Virginia and Indiana. The authors received responses from nearly 40% of the prosecutors that were sent the survey. The results of their questionnaire showed that computer crimes were a very small fraction of the prosecutors' case load. Michalowski and Pfuhl (1991) found that of the 69 prosecutors that returned their questionnaire, there was only an average of 2.2 computer crimes per jurisdiction. Since this questionnaire asked about all the computer crime cases that the prosecutors reviewed since the passage of the computer crime statutes in their state, it can also be found that this results in only .5 computer

crimes per year per jurisdiction. This showed then that the computer crime wave that was predicted to occur, and required the passage of the new legislation, had not happened.

Michalowski and Pfuhl (1991), in another surprising statistic, found that 57.3% of the computer crimes that were reported were from only two jurisdictions, neither of which was named by the authors. Both of these jurisdictions that had much higher rates of computer crime contained a prominent computer industry. Because of the computer industry, in these two jurisdictions there was a heightened awareness to computer related crimes, and an increased opportunity to commit computer related crimes. Michalowski and Pfuhl (1991) note that these two jurisdictions still only reviewed 4.8 cases per year, a very small number compared to most property crimes. Overall computer crimes were a very minor part of these prosecutors' case loads.

The above numbers from Michalowski and Pfuhl (1991) were merely those cases that the prosecutors reviewed. Of the reviewed cases there were 92 prosecutions and 84 convictions. Of these prosecutions and convictions, once again a large number of them were from the two jurisdictions that held a substantial computer industry. A total of 68 prosecutions and 54 convictions came from just these two jurisdictions. The author's state that these high numbers in the two jurisdictions mean that even with an average of .3 prosecutions per jurisdiction a year, many prosecutors did not try a computer related crime for years.

Michalowski and Pfuhl (1991) also decided to find out whether these prosecutors had used other statutes to prosecute computer related crime. These prosecutors reported 50 more computer crimes that were prosecuted under other criminal statutes. Michalowski and Pfuhl (1991) state that these numbers would help to explain the low

level of prosecution under computer crime statutes, but it would not explain why it was felt that there was a need to pass computer related statutes. The authors then begin to delve into possible explanations for the passage of computer crime laws since there appears to have been no rash of computer crime, and no major economic losses incurred.

Michalowski and Pfuhl (1991) found that the research in the area showed very little political pressure from those in the computer industry to pass these targeted laws. The authors also found that computer crime garnered very little media attention that would have resulted in popular attention to the need for computer crime laws at the time. Michalowski and Pfuhl (1991) also draw attention to the fact that technological change can create legal problems because it threatens already existent social relations. The authors note that there have been several technologies that came prior to the computer that caused the creation of their own bodies of law. These include such inventions as the automobile, telegraph, telephone and radio. These bodies of law develop as the technologies do, causing legal problem to remain, until they are well established and rooted in society. Michalowski and Pfuhl (1991) make the point that the mere threat of change can cause the desire to create these laws governing new technologies. Michalowski and Pfuhl (1991) make reference to the example of the technology of movable type, and the ability of others beside the church to interpret scripture and spread their thoughts, playing a part in the collapse of feudalism because the Catholic Church attempted to govern its use and ultimately failed. The point the authors appear to be making at this point is that the passage of computer crime laws could have been a knee jerk reaction to attempt to control the unknown.

The problem with computer crimes according to Michalowski and Pfuhl (1991) begins with the fact that computer data is volatile and intangible. The taking of this electronic data or property does not fit the traditional theft or trespass statutes. The property that is trespassed on is entirely virtual; there is no physical entry of a person. The taking of data also provides a unique view of theft, since the original owner is not deprived of their property. The thief simply copies the file and leaves the original intact. Michalowski and Pfuhl (1991) argue that it was this uncertainty of whether electronic data could be considered property that led legislators to act, and create laws specifically governing computer crimes.

Since the production of the research of Michalowski and Pfuhl (1991), there has been an upswing in the amount of computer related crime. There has also been a rise in the media coverage of computer related crimes, such as many viruses and a few instances of hacking; e.g. the notorious hacker Kevin Mitnik.

While conducting research into the area of unauthorized access, and computer crime in general, the literature is vast and developing in a fashion very similar to the development of computers. Many authors delved into computer crime in general but only a few directly examined the concepts of unauthorized access and computer trespassing. One of the most notable studies was that of Orin Kerr (2003), who looked at the concept of what unauthorized access truly is by dividing the concept into its two individual parts.

Kerr's (2003) research focuses heavily on case law, and examines what court rulings from roughly the late 1970's to the early part the 2000's, have said about unauthorized access. Kerr (2003) also makes the comparisons of unauthorized access in computer statutes to that of trespass. Kerr (2003) begins by pointing out that there are

many minor ambiguities between trespass laws from jurisdiction to jurisdiction, but the basics of the crimes are always the same. However, he points out that this is not true of computer crimes. Kerr (2003) examines the unauthorized access laws specifically and delves into the problem of not having one basic definition for the crime.

Kerr (2003) points out that it is not the traditional crimes that are committed via a computer that causes legal questions. His example is that a death threat is still a death threat even if it is in an electronic format. The problems arise from what he calls crimes of computer misuse. The common crimes of computer misuse that he lists are those of hacking, virus and worm dissemination, and denial of service attacks. The two forms of computer misuse that Kerr (2003) discusses are that of exceeding privileges on a computer (hacking) or denying privileges to someone who has them (denial of service).

The author lays out the three crimes that would, at first glance, cover computer crimes; these are theft, burglary and trespass. The first problem laid out by Kerr (2003) is that there is a requirement for physical entry in the cases of trespass and theft. However, Kerr (2003) notes the striking similarities to computer crimes. He likens hacking to the equivalent of a cyber trespass, and also shows how a burglar and a hacker may both gain access to commit a crime within, very similar to theft.

Kerr (2003) focused on the theft laws that were often used to prosecute computer misuse before the adoption of unauthorized access statutes. Kerr (2003) states that it took some creativity for the courts to conclude that there was a property interest in the theft, and that the person was deprived of the property. Over time the courts ruled that the use of a computer is property, the data on the computer is property and even the passwords used to access the computer could be considered property. Kerr (2003) states that the

courts very easily declared that there was a property interest in computers, but had a difficult time explaining the actual deprivation of property. In cases of computer misuse such as denial of service, the courts could easily show that the denial deprived the authorized user of use, and therefore a theft occurred. It became much more difficult in cases where copies of files or programs were downloaded by unauthorized users. The software or files remained on the computer, in turn making it much more difficult to show that the victim was deprived of their property. Kerr (2003) states that for the most part if it was determined that harm had occurred to the victim as a result of the property being taken, there was then a theft. The rulings all rested on a determination of whether or not harm was incurred due to the theft.

To address this awkward fit of traditional laws with the world of computers, by the late 1990's the legislative bodies of the U.S. had all passed statutes that addressed computer related crime directly (Kerr, 2003). The common factor among the many different statutes that were passed by the states and the federal system is that the trigger is that of unauthorized access or the exceeding of authorized access (Kerr, 2003).

Kerr (2003) contends that the evidence suggests that the legislators who passed the unauthorized access crime statutes intended this to be analogous to trespass. Many states label their laws as such, calling their unauthorized access crimes by names such as computer trespass or breaking into a computer. Kerr (2003) breaks down the term unauthorized access and examines each part. The first question becomes what is access to a computer. Many interpretations from the courts are given, such as whether a virtual entrance has been made to the computer. Kerr (2003) likens the password screen requiring a username and password to a locked door, where access is not made until a

valid username and password is given or the screen is deceitfully bypassed. Some courts, however, have said that just sending a signal to a computer and receiving a response back is access.

Authorization is also examined by Kerr (2003), who examines multiple scenarios that could be considered unauthorized. These include the using of false credentials, such as stealing a password and username to gain access to a computer or network. Kerr (2003) also examines whether the breach of terms of service or agreements on websites, akin to contractual agreements, would be considered unauthorized.

In the section following the breakdown of unauthorized access, the judicial decisions that have affected unauthorized access are examined. Kerr (2003) admits that there have been very few cases that have examined what unauthorized access truly means. He begins with the case of State v. Allen 260 Kan. 107 (1996), which looked to define what access means. In this case Allen dialed up a Bell telephone computer that controlled long distance calling; he was then given a prompt screen for a user name and password. Investigators only speculated that Allen had guessed a password correctly, and had no proof that the password was entered. The only evidence that existed was that he had dialed the computer. The prosecutor stated that the action fell under the unauthorized access statute, because it contained the phrasing "to approach" a computer. The Kansas Supreme court ruled that this did not constitute unauthorized access, and they also stated that if the unauthorized access law had been applied in this case, it would be overly broad and unconstitutional. In the very similar case of State v. Riley 846 P.2d 1365 (1993), the court used the same guiding principal of State v. Allen 260 Kan. 107 (1996); however,

they found that Riley was guilty because he approached the computer multiple times to attempt to gain access.

The judicial rulings for authorization were also studied by Kerr (2003). He discusses three different areas that authorization cases fall into. The first is the case of Untied States v. Morris 928 F.2d 504 (1991), which he gives its own category. The second is that of an employee using their employer's computer against the employer's interests. The final category is that of breaches in contractual obligations between the computer user and the computer owner.

In the leading case of United States v. Morris 928 F.2d 504 (1991), Morris was found guilty of accessing a federal interest computer without authorization. Morris had developed and spread a computer worm through many computers. Morris argued that he had authorized access to the original computers and additional computers at a few of the colleges that the worm spread to. The court rejected his argument, stating that although he had access to some federal interest computers, this did not give him the right to access other federal interest computers. From this case the intended function test was developed. The intended function test states that the designers intended the software to be used in a certain way, and exploiting weaknesses that allow for unintended functions causes the access to become without authorization.

Employees exceeding their authorization on an employer's computer are another instance where the courts have struggled to define unauthorized. In the case of United States v. Czubinski 106 F.3d 1069 (1997), the court stated that companies had an interest in limiting what an employee could do on a company computer to those activities that serve the company. In the case of Fugarino v. State 531 S.E.2d 187(2000), Fugarino

argued that his action in deleting code off of the company's server was not knowingly without authorization. The courts ruled that the retaliatory and vindictive manner in which he conducted himself showed that he knew it was without authorization.

In the remaining instance Kerr (2003) discusses the implications of contractual computer user and computer owner relationships. Contractual obligations often consist of some sort of click-through screen on a computer or a website that sets some sort of restriction on the use of the machine or site. Other than the self-policing by the user, no other form of code-based restriction exists to prevent the unauthorized use from occurring accidentally or purposefully. With this topic Kerr (2003) strays into civil cases that have established case law for the definition of unauthorized. These cases have stated that the breach of a contract can constitute an unauthorized access by the user.

Kerr (2003) points out that authorization can be established either by the use of code or by contract. The breach of code based authorization is usually accomplished by using false identification or credentials to gain access or by exploiting a weakness in the code that will cause the program to malfunction and allow access in a way that was never intended by the original creator of the program. Kerr (2003) also suggests that the circumvention of code based regulation should be the only thing that is considered unauthorized, not the breach of a contractual agreement.

Kerr (2003) also offers his own educated opinion on the definitions of unauthorized and access. He first tackles the concept of access and states that this should be broad and defined as any command sent to a computer. Although, he criticizes the broad scope the legislation and case law has taken on the subject of unauthorized access, he contends that access should be a broad topic and the unauthorized part should be

narrowly construed. This will allow the law to adapt to the ever-changing landscape of the computers.

Instead of a narrow definition of access, Kerr (2003) gives a narrow definition of unauthorized so that the statutes can become more clear-cut. His definition of unauthorized would strictly cover only the category of circumventing code based restrictions and not include breaches of contractual agreements. To summarize Kerr's (2003) argument, the computer, when code based restrictions are circumvented, is "tricked" into allowing the person to have access, through means such as stolen credentials or exploitation of a weakness in the software, much resembling the crime of fraud.

Susan Brenner (2004) further associates the idea of unauthorized access with a means to criminalize hacking. Brenner (2004) categorizes hacking into two distinct divisions, that of simple and aggravated. Simple hacking, according to Brenner (2004), is defined as "gaining access to a computer system without authorization." Aggravated hacking is then defined as "gaining access to a computer system or part of a computer system without authorization for the purpose of committing a crime such as copying or altering information in the system" (Brenner, 2004). Both of these definitions contain, once again, the concepts of unauthorized and access at their core. Brenner (2004) further solidifies these definitions with a review of the relevant laws at both the federal and the state levels.

The federal statute 18 U.S. Code S 1080 is the section that criminalizes hacking and cracking according to Brenner (2004). Within this section the common thread of "access without authorization" and "exceeding authorized access" can be found, along

with a high level of *mens rea*, that of either knowingly or intentionally. Specifically, 18 U.S. Code § 1030(a)(1) deals with the unauthorized or exceeded authorization when accessing information that may be of disadvantage to the U.S. and protects against the taking of such information.

Brenner (2004) also covers the various state cyber-crime laws that relate to hacking and cracking. The author points out that every state prohibits hacking, and further defines hacking as "unauthorized access to a computer or a computer system". The author also goes on to use the more unusual definition of cracking, "unauthorized access used to commit theft, damage or other offenses." Brenner (2004) also points out that while there are exceptions, most states criminalize the two types of hacking as she defined earlier, simple and aggravated. The norm that runs through these laws is that of simple hacking being a misdemeanor and aggravated hacking being a felony.

Brenner (2004) also points out that the structure and naming conventions for the prohibition of unauthorized access can vary a great deal from state to state. Simple and aggravated hacking can either be contained in the same statute or multiple statutes, some states even take the concept further and divide unauthorized access into a multi-tier crime with varying levels of severity and punishment based on harm. Brenner (2004) states that while there is a high level of similarity in the states unauthorized access laws, how they are characterized varies widely, pointing out that some states classify the crime as unauthorized access, while others consider it computer trespass, unauthorized use, or computer tampering.

While the scope of this paper is to examine the statutes regarding unauthorized access that have been adopted throughout the United States, there have been similar

trends of criminalizing unauthorized access throughout the world. Some of these studies of the unauthorized access crimes of other countries can help to shed some light on where future legislation in the United States may head, possible problems with the legislation, and the overall usefulness of the criminal sanctions.

Ian Walden (2004) examined the attempts to harmonize computer law in Europe, and the effects that this would have on existing UK computer crime law, specifically the Computer Misuse Act 1990. In particular the area and concept of unauthorized access is examined and has relevance to this study on U.S. unauthorized access laws. According to Walden the UK, under their Computer Misuse Act 1990, uses the phrasing of Unauthorized Access. The definition from the Computer Misuse Act 1990 looks similar to some of the U.S. counterparts. It reads, "Access of any kind by any person to any program or data held in a computer is unauthorized if – (a) he is not himself entitled to control access of the kind in question to the program or data; and (b) he does not have consent to access by him of the kind in question to the program or data from any person who is so entitled." This definition appears to coincide with the intent behind the U.S. equivalent unauthorized access laws.

However, Walden's (2004) exploration of the suggestions for harmonization of European computer crime laws finds recommendations for the use of "without rights' as opposed to "unauthorized access." Walden (2004) contends that these two animals are not of equal footing, and that the use of "without rights" encompasses a far broader definition than that of "without authorization." Walden (2004) suggests that the use of without rights would send the criminal law into the area of civil law. By using the term "rights" he suggests that actions that were traditionally the realm of civil liabilities, such

as the use of an illegal copy of Windows, could now be punishable through criminal statutes.

Another interesting concept that is studied by Walden (2004) is that of an optional additional *actus reus* that can be added to unauthorized access. The current *actus reus* is to "cause a computer to perform any function." The additional *actus reas* would be the "infringing a security measure." Walden (2004) suggests that this language and additional *actus reas* would help to encourage the use of security measures by owners of the computer systems so that they can enjoy the full protections of the law. Walden also states that a similar measure was proposed and failed during the passage of the Computer Misuse Act 1990. It would have added a provision wherein computer hackers could use the lack of security measures as an affirmative defense.

Research Questions

1) What is unauthorized access? Each state's law is similar, but varies in some areas, so what activity is truly being criminalized?

2) Are unauthorized access crimes aimed at criminalizing hacking only?

3) Are these unauthorized access statutes needed to prosecute these crimes? Would statutes defining traditional crimes be sufficient to prosecute offenders?

Chapter Summary

In this chapter the relevant literature was discussed in detail. The work of Orin Kerr (2003) was discussed, as he has done significant research into computer crime and unauthorized access. Michalowski and Pfuhl's (1991) research into that of unauthorized

access and its need and development was also covered, providing a more historical look at legislation. Authors such as Brenner (2004) and Walden (2004) provide a more recent over view of the laws and also provide a view into the international stage of computer crime and unauthorized access. In the following chapter the methods that were used to gather the data for this research will be discussed.

CHAPTER 3

METHODS

Through this research the goal is to come closer to understanding what exactly unauthorized access is in its legal structure. The language of the statutes will also be examined to determine if the intent of these unauthorized access statutes is to criminalize computer hacking. The use of the language "unauthorized access" is a common thread among computer crime legislation, often appearing as a separate offense or in conjunction with other elements of a crime. In order to examine unauthorized access, the individual statutes from the states and the federal system will be examined for similarities and discrepancies. Any common threads can help to shed light on the true intent of these statutes. The need for these focused unauthorized access statutes will also be examined. As it has been stated by other authors (Michalowski and Pfuhl, 1991), these statutes were created out of a perceived necessity to avert a supposed inevitable computer crime wave that never occurred during the 1980's. Has there since been a need for these targeted offenses, or would traditional statutes for crimes such as trespass be sufficient to prosecute offenders?

Data

In order to better understand the crime of unauthorized access, the first step was to identify the state statutes that correspond with the most basic of computer crimes. These crimes quite often resembled a digital version of trespassing, and some were even

housed with their analog brethren. The statutes for the fifty states and the federal system are easily accessible through internet resources. In general, each state has an online reference for its codified laws. For those few states that did not currently have their statutes online, sites such as findlaw.com have the most recent codified laws available for research and reference.

Through these online legislative references, each state's law on computer related crimes was gathered for analysis. The computer crime legislation in each state was then further scrutinized to find those laws that dealt with the concept of unauthorized access. These not only dealt with unauthorized access, but at their core either criminalized the unauthorized or attempted unauthorized access to a system or network and a few also included the addition of damages to be incurred as an element of the crime.

Once these criminal statutes had been gathered, they were categorized, seeking out statutes that contained similar language. While the laws have the general theme of unauthorized access, and the seemingly common intent to criminalize the act of hacking, there were some key areas in which these laws differed. A spreadsheet was used in order to facilitate the organization and sorting of these criminal statutes so that their differences can be better examined (See Appendix A).

Some of the key areas that were looked at while comparing these laws were: the criminalization of attempted access in the statute, whether access only was needed or intent to commit a crime therein was also required for conviction, whether an affirmative defense was given within the statute, and whether monetary damages added additional penalties to the criminal act. Why each of these was chosen and their usefulness in determining what "unauthorized access" will be examined in more detail.

While examining these criminal statutes that dealt with unauthorized access, some similarities, differences, and rarities began to stand out. One of the first noticeable reoccurrences in the language of these statutes was the use of the term attempt within. Every state has a broad attempt law that is designed to cover the instances of inchoate (i.e. incomplete) crimes; however, some states have deemed it necessary to include provisions for attempt directly within the unauthorized access statutes. This occurred with enough frequency that it warranted attention.

Another common trend within these statutes was the intent that was required in many jurisdictions. While most states required that only an unauthorized access to a computer system was required for the commission of the crime, others went further and determined that there needed to be the intent to commit another crime therein. This was a significant difference between statutes and need to be included in the research.

Additionally there were states that contained unique language that required some attention during this research. These categories were far less common, but occurred enough that it could help to shed light on the intentions of these unauthorized access crimes. These less frequent categories include provisions for affirmative defenses within the statutes. While these were very rare, they do provide valuable insight into what law makers felt should not be included as criminal acts in the statute. In addition to this rare category, there was a slightly more common occurrence to include language within the statutes to create divisions of the crime of unauthorized access based on the amount of damages that were incurred by the victim.

These various categories will help to narrow down what exactly unauthorized access seeks to criminalize. In addition to the examination of the unauthorized access

statutes, other tangential evidence of intent and purpose of these statutes will be included in the analysis. Within the overall computer crime statutes, or whatever section of the law these unauthorized access crimes may reside in, there is often the inclusion of definitions at the start of the section. In many instances the term access is defined outright, and in more rare cases, the term unauthorized is defined. These definitions then can also help to determine the intention of the legislatures when the enacted these statutes.

The final analysis that occurs in this research is that of case law. Legislation does not exist in a vacuum. Once the laws are enacted the judicial bodies may rule on various issues of language, clarity and intention of these laws. Case law was not limited strictly to cases involving crimes of unauthorized access. Also included were many cases that included issues that were in the same or similar vein of unauthorized access laws. Finally, those cases that sought to apply more traditional crime definitions to the computer world, such as trespass and theft, were examined to determine whether the unauthorized access statutes may be redundant.

Chapter Summary

This chapter discussed the methods for retrieving the data that was used to conduct this research. The methods used in sorting through the criminal statutes and the case law were also briefly discussed. The information that was scrutinized for more insight into the nature of the unauthorized access statutes was also discussed. In the

following chapter, the information that was retrieved during this research will be discussed. The conclusions that can be drawn from this information will also be covered.

CHAPTER 4

RESULTS AND FINDINGS

With the advent of the computer, and the unique issues that have resulted from the increased reliance on it, a rare opportunity has been afforded us to view the creation and adaptation of legislation that did not exist before. A plethora of computer related crimes and legislation has grown over the past three decades that has created a tangled web of statutes that address many different issues. The crime of unauthorized access is but one of these many comport related crimes and the focus of this dissection of current legislation.

Through the qualitative analysis of the criminal law statutes on unauthorized access, the case law that is of relevance to the crime of unauthorized access, and the current literature that exists, many trends can be identified and the intention and usefulness of the legislation can be examined. As it was stated in the previous chapter, there are many concepts and definitions that run as a common thread between the unique legislation of the states and the federal system.

Legislative Definitions

In identifying the intentions and purpose of unauthorized access crimes, one of the first places to identify these terms is the definitions section of the legislation. Many states have enacted entire sections of law that are dedicated solely to computer crimes (i.e. Oklahoma's Computer Crimes Act §21-1951 or Alabama's Computer Crime Act

§13A-8-100). These sections often contain definitions for terms such as unauthorized and access. While it was very rare to see a definition outlined for the term unauthorized within these definitions, the term access was very common. In fact the definition for access that was given by the states was very common, consisting of, in many cases, almost identical wording from one state's statutes to the next.

These definitions are one of the first steps into determining the exact nature of the crime of unauthorized access as it stands in the U.S. today. For the definition of access, Oklahoma has one of the typical definitions of the term access as it relates to computers. Oklahoma defines access as; "to approach, gain entry to, instruct, communicate with, store data in, retrieve data from or otherwise use the logical, arithmetical, memory or other resources of a computer, computer system or network" (OK §21-1952-1). The state of South Carolina's and the state of California's definitions for access are almost word for word identical to that of Oklahoma's.

A very similar definition for the term access can be seen for West Virginia. West Virginia's definition of access is, "to instruct, communicate with, store data in, retrieve data from, intercept data from or otherwise make use of any computer, computer network, computer program, computer software, computer data or other computer resource" (WV §61-3C-3 (a)). This definition only diverges slightly from that of the previously mentioned statutes, explicitly covering the use of software and programs that the previous statutes do not directly address. It would appear that the added computer software, data, and the like, is to eliminate any possible confusion over what constitutes access to the computer. The previously mentioned Oklahoma statute covers the same concepts of software and programs, especially through the use of the language "memory

or other resources." Computer software and programs must use memory and resources of the computer in order to function, so the same concept is covered with different language.

As for authorization, this receives a definition within the context of the computer crime statutes far less often than that of the concept of access. West Virginia is one of these states that define the concept of authorization. West Virginia Code §61-3C-3(b) defines authorization as, "the express or implied consent given by a person to another to access or use said person's computer, computer network, computer program, computer software, computer system, password, identifying code or personal identification number."

Also in some of the definitions you will find the term hacking, or computer hacking defined further. For instance, South Carolina has a definition for the term computer hacking. There definition states that computer hacking is, "accessing or attempting to access all or part of a computer, computer system, or a computer network without express or implied authorization for the purpose of establishing contact only; (2) with the intent to defraud or with the malicious intent to commit a crime after contact is established" (SC §16-16-10 j(1) & (2)).

Ohio's Revised Code also contains a definition for the term Computer Hacking. In their definition Computer Hacking consists of, "Gaining access or attempting to gain access to all or part of a computer system, or a computer network without express or implied authorization" (O.R.C. 2913.01 (II) (1)). The interesting note here is the fact that within these definitions for computer hacking both the terms access and without authorization occur, furthering the link between unauthorized access and the criminalization of computer hacking.

Unauthorized Access Legislation

Every state and the federal system have adopted a law that criminalizes what is often referred to as unauthorized access. While much of these laws remain the same across jurisdictions, there are also some unique elements in other jurisdictions. In examining these trends and the more unique aspects, it may shed light on the intent of these laws and further our understanding of unauthorized access.

Laws that criminalized acts such as computer hacking began to come to fruition in the late 1970's. Florida was the first to create a statute directed at the act of computer hacking. By the late 1990's every state and the federal system had statutes aimed at unauthorized computer access. The first federal level crime was passed in 1984, making it a misdemeanor for a person to obtain information through unauthorized access to a federal interest computer or any computer involved in interstate commerce (18 U.S.C.A. Sec. 1030).

Upon review of the current legislation there is language that is common across the jurisdictions. First the level of *mens rea* is consistently high throughout the statutes. They always require that the conduct was intentional or knowing, and not simply reckless or negligent. The damaging of the computer or information or misuse of the information that was obtained was never required in any jurisdiction, however they often aggravated the offense.

The differences in these statutes begin to come about when examining the level of activity by the offender. In thirty-seven of the states the mere access to a computer is

enough for an offense to have taken place. Proof that further harm was committed or another crime was to be committed after the access was gained, is not required for prosecution to occur. Maine's Criminal Invasion of Computer Privacy law is a typical example of this kind of statute. Maine's law reads; "intentionally access any computer resource knowing the person in not authorized to do so." This is similar to many other jurisdictions that criminalize the mere access to the system.

The computer and hacking culture have a uniqueness that does not exist with traditional property crimes. Often the breaking into a computer system is done not to gain access to information or to facilitate the commission of another crime, but to prove that the security measures that were put in place by the system owner are not good enough. It can often be seen that the intruder simply leaves the equivalent of a cyber note that says that they have been there and that the security in place is insufficient. Depending on the type of hacker that is breaking into the system, white, grey or black hat, the intruder may even leave details on how they broke in and even some suggestions on how to better secure the system. This is something that one would not see in a traditional property crime. After an offender were to defeat the security at a jewelry store or bank, they would not simply leave a note that says how they got in and how they should better secure the location, then leave the premise without taking any valuables from the premise. There are statutes for traditional property crime that exist where parallels can be drawn. For example, Pennsylvania's unauthorized use of automobiles and other vehicles statute criminalizes the operation of a vehicle without the owner's consent (18 Pa. C.S.A. § 3928).

The remaining thirteen states require that there be proof that another offense was intended to be committed after the unauthorized access was gained. A typical example of this can be seen in the Connecticut statute for Unauthorized Use of a Computer. In this Connecticut statute it states that it is "unlawful for any person to use a computer or computer network without authority and with the intent to…cause a computer to malfunction…alter or erase data..[Or] cause physical injury to the property of another" (C.R.C. Ch. 949 §53-451(14)(b)). These statutes are similar in intent and language to the crime of burglary. Burglary is typically to trespass with the intention to commit a crime therein. The parallels can be seen easily when one considers that the crime of unauthorized access is very similar to a cyber trespass, and both crimes require the intent to commit another crime after the original trespass. The difference here is that trespass is also still an offense; these jurisdictions do not criminalize the unauthorized access, or cyber trespass, alone. The reasoning behind this can only be conjectured, there is no real way of knowing why these thirteen states have not criminalized the access alone. One possibility is that they choose to delineate the possibility that a hacker is simply testing the security, such as the example given earlier. The fact that a white hat hacker may leave information on the securing of the security flaws, and cause no damage, may be one of the reasons the simple access is not criminalized.

Keep in mind that this is an examination of the lowest offense that theses jurisdictions criminalize. In many jurisdictions the states have various levels of the unauthorized access crime, similar to the federal system. As stated by Brenner (2004), there is a criminalization of simply hacking, the mere unauthorized access to a system,

and aggravated hacking, which is the unauthorized access of a computer system for the purpose of committing a crime therein.

Often those jurisdictions that criminalize the simple access also have additional statutes that bring about harsher punishments for those who would commit a further crime once the access is gained. The federal system, for example, treats simple unauthorized access as a misdemeanor (18 U.S.C. 1030). However once further criminal or tortious acts occur the crime escalates to a felony (18 U.S.C. 1030). This division between the simple access and the aggravating criminal activity that comes thereafter can also be seen in Ohio's criminal code. Under the Ohio Revised Code, Unauthorized Use of Property (O.R.C. 2913.04) covers the unauthorized access, while the Criminal Mischief statute (O.R.C. 2909.07) covers the instances where a further crime is committed or damage is incurred to the computer system.

The seriousness of the offense is also in contention, as evidenced not only by the differences in what behavior is criminalized, but also by the vast discrepancies in the punishments from jurisdiction to jurisdiction. Examples of this can be seen in Massachusetts and Minnesota. In the state of Massachusetts, the maximum penalty for Unauthorized Access to a Computer System, which covers the act of simple access, can net a punishment of 30 days in jail and a $1,000 dollar fine (M.G.L. Ch. 266 § 120f). In Minnesota however, Unauthorized Computer Access, covering the same simple access concept, can net a convicted person imprisonment for up to ten years and a $20,000 fine (M.N. Ch. 609.891). The unauthorized access crimes that also require intent to commit another crime therein also suffer from this severe discrepancy in punishment. West Virginia has a punishment of up to a $1000 fine and one year in jail for hacking into a

computer and causing damage (W.V. 61-3C-5). Georgia for the same offense has a punishment up to a fine of $50,000 and fifteen years in prison (G.C. 16-9-93(h) (1)).

Another interesting development within these unauthorized access crimes is the language of fourteen states that specifically outlines attempted unauthorized access as a punishable offense. States typically have a broad statute that already covers attempted crimes; these statutes would appear to be broadly stating that attempted computer access is an offense that falls outside of the broader attempt laws. Under these laws that outline attempted unauthorized access, it is a punishable offense to simply attempt to enter a computer system. It may be that the legislatures wanted to ensure that the mere attempt to hack into a computer system would entail a punishable offense.

The harm that comes from an attempted unauthorized access is very speculative. In cases where the unauthorized access is the only crime, the most harm that is done is the invasion of a person's privacy since they viewed what was secured on their computer and did not remove or copy any data from the computer. With an attempted access, the harm is even further diminished since the person never even saw the information on the computer since no entry was gained into the system. Where the perpetrator never gained entry into the system, its closest equivalent is that of reaching the front door of a dwelling and not being able to pick the lock or break down the door to gain access.

Case Law

Through the review of the related literature and further exploration into the judicial decisions in the United States for computer crime, a handful of cases emerged

that were repeatedly referenced or applied pointedly to the concept of unauthorized access. These cases can help to determine the need for these unauthorized access laws and earlier cases can help to resolve the reasons behind their inception.

The first case that is of interest when dealing with computer crime, and more specifically that of unauthorized access, is that of the Minnesota Rate Cases (230 U.S. 352, 1913). While this case was heard and decided nearly seventy years before computer crime become an issue, it deals with a fundamental problem within computer crimes. That fundamental problem is that the information contained within a computer is not tangible. The hard drive or other electronic media may be physical and tangible, but the data is of no use without the computer running and interpreting the ones and zeros on the media. The Minnesota Rate Case was monumental in that it declared that there was a property interest in "future interest", which is an intangible item much like computer data.

Various courts ruled on the property interest in computers in the late 1970's and early 1980's with mixed results. In 1977 the case of Charles Walter Lund v. Commonwealth of Virginia 217 Va. 688 (1977) refused to recognize the personal use of a university computer as a theft. The defendant used the university's computer for his own proposes without authorization. The courts ruled however, that there was no interest in computer time, and that because of this no theft had occurred.

In the case of United States v. Seidlitz 589 F.2d 152 (1978) only one year later, the defendant was convicted of wire fraud after he had taken a copy of the software of a defense contractor. In this case the court clearly saw that there was a property interest in the computer program, and even though the contractor was not deprived of the original,

the fact that a copy was taken still hurt the company. In this instance, the program could fall in the hands of a rival company causing them to lose any advantage they had.

In the case of State of Kansas v. Allen 260 Kan. 107 (1996) the court dismissed the charges after the prosecution failed to provide evidence that the defendant had accessed Southwestern Bell's computers. The court determined that the definition of access was far too broad to be taken at face value. The court determined that the state would have to prove three elements to Kansas's computer crime statute (K.S.A. § 21-3755(b) (1)). These were: intentional unauthorized access to the computer, damage to the computer and a loss of value totaling more than $500. The court did not consider Allen to have accessed the computer until he went beyond the initial prompt for a valid user name and password.

In the 1985 case of State of Indiana v. McGraw 480 N.E.2d 552, (1985) the court ruled that the defendant did not commit a theft by using computer resources at the city office where he worked. The prosecution said that the defendant had unauthorized control over the computers, which were property of the city of Indianapolis. The court ruled that the city was not deprived of property, the memory was never fully used by the defendant, and what he did use could be erased: therefore, no theft had occurred.

A more recent case that dealt with the concept of theft was that of State of Oregon v. Schwartz 173 Ore. App. 301 (2001). In this case the court determined that the loss of exclusive possession of a password did in fact constitute a theft. This case, as opposed to the last, ruled that the password does constitute property, and even more so, when the password loses the exclusivity it can now be seen as a theft.

These court cases all tend to deal with the concept of property, and more specifically that fine line of when the intangible property has value. The courts have been fairly inconsistent in the application of crimes such as theft to the cyber world, judging on almost a case by case basis.

Results Summary

This research sought to answer three questions regarding the definitions and nature of unauthorized access crimes. Through the examination of the legislation and case law, conclusions can be drawn in regards to these questions. Each question will be covered individually.

1) *What is unauthorized access? Each state's law is similar, but varies in some areas, so what activity is truly being criminalized?*

Through this research, one objective was to determine what unauthorized access, in legal terms, really is. Many jurisdictions are very willing to define access for us, and almost all define it in a very similar way. It would appear to cover the entry into a computer system, or network. The definition is often very broad, leaving much to the imagination when it comes to the actual way that the computer is accessed. This can be helpful for prosecutors, since the hackers, or crackers, are often discovering new ways, through security flaws and other methods, to enter a system.

Unauthorized is not as often defined within the statutes as access. That the concept of unauthorized is either left open to great interpretation, or it is assumed that it

would mean simply that the person does not have permission from the owner of the network or system to access it. The few definitions that are given would seem to confirm this. The West Virginia statute, one of the few that defines unauthorized, uses the term "consent" by the owner. The statute lists many things besides the computer and network, such as passwords, to which authorization can be contravened (W.V. §61-3C-3).

Kerr (2003), also looked at this problem of ill defined unauthorized access, and came to a similar conclusion that access is loosely defined and broad and should remain that way. Kerr (2003) also pointed out that a few courts had begun to interpret the ignoring of what are often referred to as "click through" agreements on websites as a form of unauthorized access. Kerr (2003) finally came to the conclusion that only the defeat of code based means of security should be used for unauthorized access and the simple ignoring or disregard for a contractual agreement should not. These cases were not covered in this research due to the fact that they are civil matters; however, they do bear some consideration since they deal with the scope and limits of unauthorized access.

2) Are unauthorized access crimes aimed at criminalizing hacking only?

When considering whether or not these unauthorized access crimes deal directly with the concept of hacking there are a few pieces of evidence to consider. First off would be the states that include a definition for computer hacking within their statutes. Within these definitions of hacking, "gaining access" often can be seen in the definition of hacking. The terms "without authorization" can also be seen in these definitions for computer hacking. These create a direct link in the legal language between unauthorized access and computer hacking. We can also see in these unauthorized access statutes

language that states the method of access as "including, but not limited to, computer hacking", further solidifying the link between the two. It is clear that the unauthorized access statutes are intended to criminalize what was traditionally considered hacking; however, they are often written broadly enough to encompass additional activities.

3) *Are these unauthorized access statutes needed to prosecute these crimes? Would statutes defining traditional crimes be sufficient to prosecute offenders?*

Unauthorized access comes in a few different varieties; however, it can be seen as the digital equivalent to the analog trespass. It is often referred to as computer trespass, and is even housed with the analog trespass statutes in some states. Since it would appear that prosecutors may have a difficult time using traditional trespass laws, due to the fact that they have a requirement of "real" property, it would seem these unauthorized access crimes are greatly needed.

The courts had a much more difficult time in the early days of cyber crime applying the already existent statutes to the new circumstance of the computer age. The cases from the late 1970's to the 1980's often failed to see the value in the computer time or the intangible programs of the computer. These judicial decisions that computers and their information were not akin to their tangible, real world, counterparts may have been one of the key factors in the development of the computer crime specific legislation. It is also interesting to note that the courts have since been more apt to prosecute for crimes such as theft in modern computer cases, with cases such as State of Oregon v. Schwartz 173 Ore. App. 301 (2001) where the defendant was successfully prosecuted for theft.

The use of other statutes to prosecute these computer crimes is possible with successful prosecutions for theft; however, crimes such as trespass do not lend themselves as easily to the application of computer crime. While theft statutes seem to carry some weight with cyber crime, especially with what seems to be the judicial pattern to declare value in computer data, trespass, the analog equivalent to unauthorized access, would appear not to fit so easily. With trespass statutes a commonality is the language to "enter or remain", which would appear to satisfy the access to a computer. However the statutes are often written in a way that either heavily suggests real property, or states clearly a building or dwelling is required.

These problems would appear to be far too large for a successful prosecution for trespass. It would appear that the need for the simple unauthorized access would be needed, since there are no laws that can clearly be applied to the entry into a computer system. However, it may be possible that those unauthorized access crimes that require data be taken or damaged are not needed. The courts have ruled that the data held on a computer has value, so once that data is copied or damaged, it could very well be possible to prosecute under those statutes such as theft.

Chapter Summary

The information that was collected for this research regarding unauthorized access was discussed. The first subject covered was that of legal definitions citied in the statutes. This helps to gain insight into the nature of unauthorized access. The individual statutes were then scrutinized for similarities and differences to help determine common

threads that can also point towards the nature and intent of these statutes. Case law that had relevance to the creation and adaptation of computer related crime statutes were also covered. Finally all of this information was brought together for a look at what unauthorized access is, and its usefulness in today's society. In the final chapter to follow, these findings and previous research will be brought together to take one final look at the purpose, intent and need of unauthorized access crimes.

CHAPTER 5

CONCLUSIONS

Unauthorized access computer crimes have a unique position within the current legal landscape. The concept of the crime has only had a few decades to develop, although it can be seen that it was a response to a growing concern of prosecuting criminals, such as hackers, that would take advantage of the emerging technologies that quickly moved to the forefront of the corporate world and everyday life. The personal computer and the internet will remain an integral part for commerce, education and entertainment for many years to come, requiring a unique approach to the prosecution of computer related crimes.

While the field of computer crime and legislation has only had around three decades to develop; there are already commonalities in the legislation and judicial rulings. In the early days of computer related crime the system struggled to find a way to handle the uncommon characteristics of these crimes. Early judicial rulings saw an unwillingness to find property interest in computer time or the data that was processed by the computers. In cases in the late 1970's such as Lund v. Commonwealth of Virginia 217 Va. 688 (1977) the court did not feel that there was a property interest in computer time. Even though the defendant in that case used the university computer for personal activities without authorization, the court felt that there was no harm done. It could be seen that the unauthorized access crimes have been developed out of the need to criminalize behavior such as that in Lund. If the defendant had committed the crime today, the statutes on unauthorized access could be applied.

Current court rulings have found that the intangible data that resides as mere ones and zeros on electronic media does now have value, and should be treated similarly to any other real property. For example, the case of State of Oregon v. Schwartz 173 Ore. App. 301 (2001) showed that the judiciary sees value in this intangible property. By ruling that the loss of the exclusivity of an electronic password constituted a theft, the court acknowledged the value of computer data in today's society. We can see the beginning of this move towards value in data as early as the late 1970's with cases such as United States v. Seidlitz 589 F.2d 152 (1978) where the court saw value in the program that the defendant copied from the corporate computer. The defendant was found guilty of fraud by wire, and the court stated that even though the company was not deprived of their property, since the defendant only made a copy, the loss of exclusivity could damage their edge over their competition. This is one of the earliest rulings that found that there is value in computer data.

Once again it can be seen that many of the above cases would more than likely much more easily prosecuted using today's statutes that prohibit unauthorized access. The mere entry into the computer system, through any means, can be prosecuted in many jurisdictions, not even requiring that any further acts are committed after the entry. While the evidence suggests that computer hacking may have been one of the strong motivating forces behind the creation of these unauthorized access laws, there are instances that appear to have been written to apply in situations that do not involve hacking. As previously stated, the states that define hacking often give a definition that is undeniably tangled up with unauthorized access. However, there seems to be some departure to cover means that may not be considered computer hacking. This trend can

be seen in the language used by the legislature in states such as Ohio, where the wording often includes terms such as "including but not limited to, hacking" when discussing the method used for the unauthorized access. In the case of State of Ohio v. Moning 2002 Ohio 5097 (2002), a police officer was found guilty of exceeding his authorization by using the law enforcement data base to find information on acquaintances. In this case the officer had authorization to use the data base, so there were not any actions that could be considered hacking.

In the aforementioned case of Lund v. Commonwealth of Virginia 217 Va. 688 (1977), had the crime taken place in present day, the prosecution would have surely charged him with unauthorized access as a minimum, and may well have been successful. He clearly did not have any authorization to use the computer for his personal purposes, and since the access only requires that he use the computer or its resources in some way, this could very well fall into the category of an unauthorized access crime. Also in the afore mentioned case of United States v. Seidlitz 589 F.2d 152 (1978), the use of a spy program to monitor and retrieve data would be a blatant violation of unauthorized access statutes in today's courts. Within these unauthorized accesses statute, not only do they state that "without authorization" is needed for the crime to occur, they also state that the exceeding of authorization can also constitute unauthorized access. This phrasing has the potential of drastically changing the outcome of two court cases from the mid 1980's. In the State of Indiana v. McGraw 480 N.E.sd 552 (1985), the defendant's use of the cities computer system for his own private business venture would clearly have violated the unauthorized access statutes. Without such statutes, the court found that no theft had occurred since the media that he used to store his data could simple be erased. In the

case of the State of Washington v. Olsen 735 P.2d 1362 (1987), a police officer was prosecuted under the computer trespass statue and was found not guilty. The courts determined that even though the officer had used the university police department computer for his own purpose of seeking out coeds, he had authority to use the computer. Under modern statutes, the inclusion of exceeding authorized access would have meant that this individual may well have been convicted of computer trespass.

It can be seen that unauthorized access has a place within the legislative web that is developing with the ever more present personal computer. This research only sought to examine the criminal aspects of the unauthorized access crimes. The civil aspects and litigation are also present and can have an effect on the criminal aspects of the laws. As it was alluded to earlier, Kerr's (2003) work has already begun to examine the civil side of the unauthorized access coin. Within his research there is already the growing possibility of unauthorized access also covering the breach of contracts that arise from ignoring, intentionally or unintentionally, the terms of service on web pages and services. These civil aspects could be further explored in future research. Civil cases such as American Online v. National Health Care Discount, Inc. 121 F. Supp. 2d 1255 (2000), have expanded the definition of access to include the violation of terms of service for gather AOL customer emails and sending spam email.

The sheer amount of case law that exists also means that not every case with some relevance to computer crime and unauthorized access could be covered fully (See Appendix B for court cases covered in this research). There are many other emerging computer related crimes that also could be examined for their effect and usefulness within the legal system. Crimes such as denial of services attacks, spam email, and virus

dissemination have all garnered national attention and have caused the enacting of legislation specifically targeted at these crimes. Many problems that exist now in the legal system as they relate to computer crime did not exist a mere decade ago. This research was limited in scope to only that of unauthorized access, but there are many more emerging crimes that can also be examined such as denial of service attacks, or bulk email. With the constant introduction of newer, smaller, faster and always connected computers, computer crimes may begin to spill into the realm of other devices such as smart phones and digital media players. This constant evolution of computer technology and the increasing dependence on it for routine corporate and everyday activities means that computer legislation will be a topic rife for debate for many years to come.

Chapter Summary

In this final chapter, the research conducted is brought together to show t purpose and usefulness of unauthorized access. The case law is covered to show that with current legislation, the cases that were decided in the absence of computer crime laws could garner much different rulings. These examples provide some evidence that the unauthorized access crimes that have been passed into legislation are useful, and will continue to be developed in the future.

BIBLIOGRAPHY

Brenner, S. W. (2004). U.S. Cybercrime Law: Defining Offenses. *Information Systems Frontiers, 6*(2), 115-132.

Draper, J. (2007). The origins of Captain Crunch... Retrieved December 3rd 2008 http://www.webcrunchers.com/crunch/origins.html

Fugarino v. State 531 S.E.2d 187(2000).

Kerr, O. (2003). Cybercrimes Scope: Interpreting "Access" and "Unauthorized" in Computer Misuse Statutes. *New York University Law Review, Nov. 2003*.

Knetzer, M., Muraski, J. (2008). Investigating High Tech Crime. Pearson Prentence Hall. Upper Saddle River, NJ.

Lund v. Commonwealth of Virginia 217 Va. 688 (1977).

Merriam-Websters Dictionary. (2009). Retrieved July 6th 2009. http://www.merriam-webster.com/dictionary

Michalowski, R. J., & Pfuhl, H. (1991). Technology, property, and law. *Crime, Law and Social Change, 15*(3), 255 - 275.

Minnesota Rate Cases (230 U.S. 352, 1913).

National conference of State Legislatures (2009). Computer Hacking and Unauthorized Access Laws Retrieved April 14th 2009 http://www.ncsl.org/IssuesResearch/TelecommunicationsInformationTechnology/ComputerHackingandUnauthorizedAccessLaws/tabid/13494/Default.aspx

Office of Legal Education, Prosecuting Computer Crime February 2007 http://www.usdoj.gov/criminal/cybercrime/ccmanual/ccmanual.pdf

Oxford Compact Dictionary. Retrieved July 6th 2009. http://www.askoxford.com/concise_oed/

Sommer, P. (2006). Criminalising hacking tools. *Digital Investigation, 3*(2), 68-72.

State of Indiana v. McGraw 480 N.E.sd 552 (1985).

State of Kansas v. Allen 260 Kan. 107 (1996).

State of Oregon v. Schwartz 173 Ore. App. 301 (2001).

State of Ohio v. Moning 2002 Ohio 5097 (2002).

State of Washington v. Olsen 735 P.2d 1362 (1987).

State v. Riley 846 P.2d 1365 (1993).

Thomas, J. (2005). The moral ambiguity of social control in cyberspace: a retro-assessment of the 'golden age' of hacking. *New Media & Society, 7*(5), 599-624.

United States v. Czubinski 106 F.3d 1069 (1997).

United States v. Morris 928 F.2d 504 (1991).

United States v. Seidlitz 589 F.2d 152 (1978).

Walden, I. (2004). Harmonising Computer Crime Laws in Europe. *European Journal of Crime, Criminal Law and Criminal Justice*, *12*(4), 321-336.

Walton, R. (2006). The Computer Misuse Act. *Information Security Technical Report*, *11*(1), 39-45.

Wang, W. (2006). Steal This Computer Book 4.0. No Starch Press, Inc. San Fransisco, CA

APPENDIX A
Current Unauthorized Access Statute Research Chart

State Name	Statute	Crime Name	Attempt	Access	Access W/ Intent	Affirmative Defenses	Monetary Damages
Alabama	13A-8-100	Offense Against Intellectual property	1	1			
Alaska	11.46.740	Criminal Use of a Computer			1		
Arizona	13-2316	Computer Tampering		1			
Arkansas	5-41-104	Computer Trespass			1		
California	Penal Code 502	Unauthorized Access		1			
Colorado	18-5.5-102	Computer Crime		1			
Connecticut	15-451(14)(b)	Unauthorized Use of a Computer			1		1
Delaware	11 §932	Unauthorized Access		1			
Florida	815.06	Offenses Against Computer Users		1			1
Georgia	16-9-93 (a)	Computer Theft			1		
Hawaii	708-895.5 - 7	Unauthorized Computer Access & Degrees		1			1
Idaho	18-2202	Computer Crime	1	1			
Illinois	720 ILCS 5/16D-3	Computer Tampering & Aggravated		1			
Indiana	IC 35-43-1-4	Computer Tampering		1			
Iowa	714.1	Unauthorized Computer Access		1			
Kansas	21-3755 (b) (1) (A)	Computer Trespass	1		1		

State Name	Statute	Crime Name	Attempt	Access	Access W/ Intent	Affirmative Defenses	Monetary Damages
Kentucky	434.845	Unlawful access to a Computer & Degrees	1	1			1
Louisiana	15:13.5	Computer Fraud			1		1
Maine	17-A §432	Crim. Invasion of Comp. Privacy & Aggravated		1			
Maryland	§7-302 (c) (1) (i)	Unauthorized Access to Computers	1	1			1
Massachusetts	266 § 120F	Unauthorized Access to Computer Systems		1			
Michigan	752.796	Fraudulent Access to Computers			1		
Minnesota	609.891	Unauthorized Computer Access	1	1			1
Mississippi	97-45-3	Computer Fraud		1			1
Missouri	569.099	Tampering with computer Users		1			1
Montana	45-6-311	Unlawful Use of a Computer		1			1
Nebraska	28-1343.01	Unauthorized Computer Access		1			
Nevada	205.477	Unlawful Use or Access of a Computer	1	1		1	
New Hampshire	638:17 I	Unauthorized Access		1		1	
New Jersey	2C:20-25	Wrongful Access	1	1			
New Mexico	30-45-5	Unauthorized Computer Use			1		1
New York	156.05	Unauthorized Use Of Comp.		1			1

State Name	Statute	Crime Name	Attempt	Access	Access W/ Intent	Affirmative Defenses	Monetary Damages
North Carolina	14-454	Accessing Computers		1			
North Dakota	12.1-06.1-08	Computer Crime	1	1			
Ohio	2913.04 (B)	Unauthorized Use of Property	1	1			
Oklahoma	21-1952 (A) (4)	Computer Crimes Act	1	1			
Oregon	164.377 (2)	Computer Crime	1		1		
Pennsylvania	18 §7611	Wrongful Use of a Computer		1			
Road Island	11-52-4.1	Computer Trespass			1		1
South Carolina	16-16-20	Computer Crimes Act			1		1
South Dakota	43-43B-2	Unlawful Use of a Computer System		1			
Tennessee	39-14-602	Personal and Commercial Computer Act	1	1			
Texas	33.02	Breach of Computer Security		1		1	1
Utah	76-6-703	Computer Crimes	1	1		1	1
Vermont	13 1402	Unauthorized Access		1			1
Virginia	18.2-152.4	Computer Trespass			1		1
Washington	9A.52.110 & 120	Computer Trespass		1			
West Virginia	61-3C-5	Unauthorized Access to Computer Services			1	1	
Wisconsin	943.70	Offenses Against Computer Data and Programs		1			1

State Name	Statute	Crime Name	Attempt	Access	Access W/ Intent	Affirmative Defenses	Monetary Damages
Wyoming	6-3-504	Computer crimes Against Users		1			
TOTALS			14	37	13	5	19

APPENDIX B
Referenced Court Cases
Arranged Alphabetically

Fugarino v. State 531 S.E.2d 187(2000)

Lund v. Commonwealth of Virginia 217 Va. 688 (1977)

Minnesota Rate Cases (230 U.S. 352, 1913)

State of Indiana v. McGraw 480 N.E.sd 552 (1985)

State of Kansas v. Allen 260 Kan. 107 (1996)

State of Ohio v. Moning 2002 Ohio 5097 (2002)

State of Oregon v. Schwartz 173 Ore. App. 301 (2001)

State of Washington v. Olsen 735 P.2d 1362 (1987)

State v. Riley 846 P.2d 1365 (1993)

United States v. Czubinski 106 F.3d 1069 (1997)

United States v. Morris 928 F.2d 504 (1991)

United States v. Seidlitz 589 F.2d 152 (1978)