5-1-2004

Cybercrime

Karissa Ayala
University of Georgia School of Law

CYBERCRIME: INTELLECTUAL PROPERTY CRIMEUSING

THE INTERNET AS A TOOL

by

KARISSA AYALA

UNDER THE DIRECTION OF PROF. ROBERT BRUSSACK

ABSTRACT

As the new information age develops and grows in all areas of communication technologies, it imposes new challenges to the legal system in protecting individuals and companies. These new challenges are the result of the Internet increase in scope and complexity. While society is receiving great benefits from the Internet, they are also confronting a new type of crime, cyber crime. Cyber crime includes a wide variety of illegal acts committed using the computer, and because of the continuous technology developments is impossible to create an exhaustive list of all actions considered a cyber crime. In order to facilitate the investigation of cyber crime the U. S. Department of Justice has classified them in three broad categories: when the computer is used as a target or the medium or its use is incidental to other criminal offenses.

Crimes using a computer as a target or victim of an offense include actions that intrude the confidentiality, integrity or availability of the information or services. The second category includes actions where the computer is used as the tool to commit traditional criminal conduct. This category includes those crimes that have been occurring in the physical world, but now we are seeing with increasing frequency on the Internet. Examples of this type include child pornography, fraud and intellectual property violations. In the third category, the computer is

used to store data, which contains evidence of fraud, white collars crimes and viruses for example, and therefore its use is considered to be incidental to the criminal act.

In this thesis, I will study primarily the intellectual property crimes committed using the Internet as a tool or medium. This classification includes criminal activity that can be performed by other means, but the criminal has chosen to use the computer as the mechanism. I will also discuss the international dimensions and dilemmas of this crime and as Janet Reno said, *"how critical is to create treaties for international cooperation to reduce the threat". "One of the biggest challenges has been to implement an effective matrix of bilateral mutual legal assistance and extradition treaties."* Janet Reno, Conference held on September 2000.

Chapter 2 discusses the impact of cybercrime against Intellectual Property Rights in the evolution and creation of new intellectual property legislation. Specifically, the absence of a legal scheme that can effectively address the prosecution of cybercriminals. The second part of this chapter contains some of the most significant legislation to prosecute cybercrime, follow by a brief discussion and application of each one.

Further, Chapter 3 focus in the challenges this crime create in the conduction of the criminal investigation, how the FBI surveillance works and it impact on private citizens and businesses. The controversies Carnivore has created. Including a discussion on how this type of crime endangers citizens and legitimate businesses causing them multi-millionaire losses. And what Congress should do to combat the crime as well as what we can do to cooperate.

Chapter 4 discusses the jurisdictional problems confronted in the prosecution of cybercrime due to the nature of the World Wide Web and the lack of assistance from other countries. The second part contains some of the most controversial constitutional problems arising from the use of Carnivore.

INDEX WORDS: Cybercrime, Computer crimes, Copyright Infringement, Carnivore, Prosecution of Intellectual Property Rights Infringement, Internet.

CYBERCRIME: INTELLECTUAL PROPERTY CRIME USING THE INTERNET AS A TOOL

BY

KARISSA AYALA

B.A., The University of Puerto Rico, 1995
J.D., University of Puerto Rico School of Law, 1997

A Thesis Submitted to the Graduate Faculty of the University of Georgia in

Partial Fulfillment of the Requirements for the Degree of

MASTER IN LAW

ATHENS, GEORGIA

2004

CYBERCRIME: INTELLECTUAL PROPERTY

CRIME USING THE INTERNET AS A TOOL

by

KARISSA AYALA

Major Professor: Robert Brussack

Committee: Gabriel Wilner

Electronic Version Approved:

Maureen Grasso
Dean of the Graduate School
The University of Georgia
May 2004

DEDICATION

I wish to dedicate this Thesis to my parents, Ismael and Lydia for all their support and efforts to make my dreams come true. And to my lovely husband, Jose and our beautiful daughter Bianca Isabelle. I love you, both.

TABLE OF CONTENTS

Page

CHAPTER 1

NATURE OF INTELLECTUAL PROPERTY RIGHTS SUBJECT TO PROTECTION

This chapter is an introduction to the subject matter of the intellectual property rights; copyright law, trade secrets, trademark and patent law. The creation of the intellectual property rights emerged as a result of the legal response to the new technologies' creation and open ending revolution of the human expression.[1] Legislators sought for the protection of these new ways of expression and created three bodies of federal law: Copyright, Patent, Trade Secrets and Trademark. Copyright gives authors protection to their original works of authorship for limited times to reward them for new invention and advances, and to promote the "Progress of Science".[2] Patent gives protection to new inventions, process or useful improvement. Trademark protects the commercial identity created to identify a product or service from being use by other to confuse the public regarding the source of the good or service. Trade Secret is another form of protection for new inventions, which includes almost anything used by a company to obtain advantage over its competitors. In sum, it includes any formula, pattern, device or compilation of information. All these different legal regimes have been created to promote the creation of knowledge by giving authors and inventors the right to exclude other from their intangible property.[3]

---

[1] Craig Joyce, William Patry, Marshall Leaffer and Peter Jaszi, Copyright Law, Fifth Edition (2000) at page 1: *"Our post-industrial era is marked by rapid technological change in which our ability to reproduce and receive information grows exponentially".*

[2] Art. I, §8, cl.8 of the Constitution of United States of America.

I. Copyright Law[4]

A. Subject Matter and Requirements

Copyright has its origin in the power vested in the Congress by the Constitution of the United States of America, Art. I, §8, cl.8, which states:

> *"Congress shall have the power to Promote the Progress of Science and Useful Arts, by securing for Limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries."*[5]

This clause contained three important policies; the promotion of learning, the protection of the public domain, and the right of public access. Copyright Law gives authors a proprietary monopoly over their work by giving them the *'exclusive right to their respective writings and discoveries'*. *'For Limited Times'* means that Congress need to establish a period of time for the existence of that monopoly that once expires, the copyrighted work goes to the public domain. The promotion of learning is achieved by giving the authors exclusive rights as an incentive.[6]

Pursuant to this constitutional authority vested in the Congress, the first federal copyright act was passed in 1790 and gave authors protection for a term of 14 years and right of renewal for the same term. This protection was followed by the 1909 Act. Between 1909 and 1976, different

---

[3] Craig Joyce, supra page 19

[4] 17 U.S.C. §101 et seq.

[5] Art. I, §8, cl.8 of the Constitution of United States of America

[6] See Scott K. Pomeroy, Promoting the Progress of Science and the Useful Arts in the Digital Domain: Copyright Computer Bulletin Boards, and Liability for Infringement by Others, 45 Emory L.J. 1035 (1996). See also Mazer v. Stein, 347 U.S. 201, 219 (1954)("The economic philosophy behind the clause empowering Congress to grant patents and copyrights is the conviction that encouragement of individual effort by personal gain is the best way to advance public welfare through the talents of authors and inventors in 'Science and Useful Arts'."); and Craig Joyce, William Patry, Marshall Leaffer and Peter Jaszi, Copyright Law, Fifth Edition (2000) at Chapter 7, §7.01, page 489.

advances and technical changes forced legislators to amend copyright law to include those changes. Among the amendments is the extension of protection to motion pictures and the right of performance for nondramatic literary works. By 1955, Congress was convinced that the 1909 Act has become obsolete and new legislation should replace it. Nonetheless, it took Congress twenty one years to enact the Copyright Act of 1976[7]. The current copyright law was enacted in 1976 and all others laws regarding copyright are preempted by this act.

Since the 1976 Act, protection of copyright starts when *"an original work of authorship is fixed in any tangible medium of expression, now know or later developed, from which they can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device"*.[8] Copyright gives authors the legal right to exclude others from copy, distribute, create derivative works, performance or display of their works without authorization. This statute established two important requisites; originality and fixation. Originality means that the work was created independently with a modicum of creativity and does not extend to words, symbols, or as stated by title 17 USCA§102(b)[9]. Section 102(b) of Title 17 was discussed in Feist Publications v. Rural Telephone Services, 499 US 340[10], when the court stated that facts are not copyrightable and no author may copyright his ideas or the facts he is narrating. This case explains that facts cannot be copyrightable, because the *sine qua non* of copyright is originality. The threshold for creativity has been described as "very slight," "minimal," "modest".[11] 'Original

---

[7] Pub. L. No. 94-553, Title I, §101, Oct. 19, 1976, 90 Stat 2541

[8] 17 U.S.C. §102(a).

[9] 17 U.S.C. §102(b): *"In no case does copyright protection for an original work of authorship extend to any idea, procedure, process, system, method of operation, concept, principle, or discovery regardless of the form in which it is described, explained, illustrated, or embodies in such a work".*

[10] See also Alfred Bell & Co. v. Catalda Fine Arts, 191 F. 2d. 99 (1951)(" 'Original' in reference to a copyrighted work means that the particular work 'owes its origin' to the 'author' citing Burrow-Giles Lithographic Co. v. Sarony, 111 U.S. 53, 57-58(1884); Bleinstein v. Donaldson Lithographing Co., 188 U.S. 239 (1903).

[11] See West Publishing Co. v. Mead Data Central, 799 F. 2d 1219, 1223 (8th Circuit 1986).

Works of authorship'[12] includes, without limitation, literacy works, pictorial, graphic, and sculptural works, architectural works, dramatic, pantomime, and choreographic works, musical works and sound recordings, motion pictures and other audiovisual works, derivative works and compilations. In 1978 the Commission on New Technological Uses of Copyrighted Works (CONTU) submitted a final report concluding that copyright protection should be given to computer software.[13] In 1980 Congress amended the copyright legislation to extend protection to the original works of authorship embodies in computer software taking in consideration that the list of original works of authorship in section 102 is illustrative and not exhaustive. The protection given to computer software includes the program's code and object codes, but does not include any element containing an idea, method, procedure, process or any other subject matter not protected by copyright law. This imposes several limitations to the software protection that sometimes can be protected under the patent law or cannot be protected at all.

'Fixation' occurs when the original work of art is embodied in a tangible medium of expression. 'Fixed'[14] means that the original work has been embodied in a copy that is *"sufficiently permanent or stable to permit it to be perceived, reproduced, or otherwise communicated for a period of more than transitory duration"*. This requirement is necessary to make a distinction between transient ideas or thoughts, which are not protectable, and tangibles. Copyright protects the author's creation of an original work and not the idea itself to maintain the balance of the public interests in knowledge and

---

[12] 17 U.S.C. §102 and §103.

[13] Merges, Robert P., Peter S. Menell and Mark A. Lemley, Intellectual Property in the New Technological Age, Chapter 7 Copyright Law, Subsection C at page 911 (2nd Edition 2000). See also Apple Computer v. Franklin Computer, 714 F. 2d 1240 (3rd Cir. 1983).

[14] The fixation requirement has been derived from the Constitutional requirement "Writings', which has been construed by the Supreme Court as 'any physical rendering of the fruits of the author's creativity'. See Goldstein v. California, 412 U.S. 546 (1973), and White-Smith Music Publishing Co. v. Apollo Co., 209 U.S. 1(1908). Fixed is defined by 17 U.S.C. §101: *"A work is "fixed" in a tangible medium of expression when its embodies in a copy or phonorecords, by or under the authority of the author, is sufficiently permanent or stable to permit it to be perceived, reproduced, or otherwise communicated for a period of more than transitory duration. A work consisting of sounds, images, or both, that are being transmitted, is "fixed" for purposes of this title if a fixation of the work is being made simultaneously with its transmission".*

the proprietary interest of the author in his original work of authorship. Ideas are left in the public domain to motivate others to create original works and as a restriction to grant a monopoly over ideas that can just be expressed in a limited number of ways.[15]

A tangible medium of expression means to embody the work in a physical object in written, printed, photographical, etc., or any other sufficiently permanent or stable, and not transient reproductions. A tangible medium has been extended to include floppy disks, hard drive and websites, among other new technology that can be utilized to create a large variety of inspirational works. The Supreme Court has held that the loading of copyrighted software into the hard drive constituted a fixation and can be considered a copy for purposes of copyright infringement.[16]

B. Exclusive Rights

Section §106 of Title 17[17] established five exclusive rights of the copyright owner; the right to reproduce the copyrighted work in copies or phonorecords[18], to prepare derivative works based on the copyrighted work, to distribute copies or phonorecords of the copyrighted work to the public for sale or other transfer of ownership, or by rental, lease or lending, in the case of literary, musical, dramatic, and choreographic works, pantomimes, and pictorial, graphic, or sculptural works, including the individual images of a motion picture or other audiovisual work, to display the copyrighted work publicly. These fundamental rights are subject to some limitations and restrictions in the subsequent sections of this title. For example, the right to reproduce extent to the copying by downloading a copy from the internet in a floppy disk, but also is broaden to include the making of exact or substantially

---

[15] See Baker v. Selden, 101 U.S. 99 (1880) (for a full discussion of the idea-expression dichotomy theory). See also CCC Information Services, Inc. v. MacLean Hunter Market Reports, Inc. 44 F. 3d 61 (1994)(about the 'merger doctrine')

[16] See MAI Systems Corp. v. Peak Computer Inc., 991 F. 2d 511(1993).

[17] 17 U.S.C. §106

[18] See Arnstein v. Porter, 154 F. 2d 464 (2d Cir. 1946)

similar reproductions.[19] Also, the right to distribute is limited to the first sale doctrine, which means that his right is in force until the copy of his work of authorship is sold. Once the copy of a computer program, for example, is sold, the owner of the copyrighted work cannot exercise this right to distribute over that copy, but still has the right to be protected from infringement of any of the other exclusive rights.

C. Limitations on Exclusive Rights

Generally these exclusive rights further the purposes of providing a public benefit, but this is not always the case. There exist some situations in which those exclusive rights need some limitations to comply with this legislative intent. In those cases, it is necessary to carefully consider and balance of the authors exclusive rights and the public's right to have access to knowledge. For that reason, Congress has sought to balance those interests in its legislation of section 107 through 118, where this is achieved by establishing a limited monopoly to the author's rights.

1. Fair Use and Personal Use

Section 107 states that *"notwithstanding the provisions of section 106, the fair use of a copyrighted work, including such use by reproduction in copies or phonorecords or any other means specified by that section, for purposes such as criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship, or research, is not an infringement of copyright".* There exist a four factor test to determine whether the use of a copyrighted work constitutes fair use; the purpose and character of the use, the nature of the copyrighted work, the amount and substantiality of the portion used in relation to the copyrighted work as a whole and the effect upon the potential market. In Harper & Row v. Nation, 471 US 539 the court applied those

[19] Merges, supra note 13 at page 4, Chapter 4 Copyright Law, Subsection E at page 433.

four factors and decided that under the particular circumstances of this case the publication was commercial and Nation took what was essentially the heart of the book what constitutes a copyright infringement.[20]

2. Other Limitations

Other limitations exist, like for example the idea/expression dichotomy or the merger doctrine which restricts the material that can be protected by granting a monopoly and what cannot be taken from the public domain. The first sale doctrine is another limitation to the author's control of his work of authorship. This doctrine establish that once the author gave permission to reproduce certain amount of copies of his paint or any other work of authorship and sale them, he does not have any control over the physical object that embodies the art. The new owner can sell the copy to anybody or dispose it without the author's authorization. Nevertheless, the author still has protection under the exclusive rights on that particular copy, meaning that the new owner is banned from reproducing or creating derivative works, because what the author sales is the physical object that embodies his creation, but not his exclusive rights. All these limitations and exceptions are concerns of the legislators regarding the balance between the author's right and the public access right that is the underlying purpose of the Constitution.

---

[20] See also American Geophysical v. Texaco, 60 F. 3d 913 as en example of an application of the 4 factors; and Campbell v. Acuff-Rose Music, 510 U.S. 569, about the four factor test application to parody. Also The statute opens with the proposition that, notwithstanding the exclusive rights of the copyright owner, "fair use of a copyrighted work ... for purposes such as criticism, ***1500** comment, news reporting, teaching, scholarship or research, is not an infringement." 17 USC §107. The statute then sets forth a short nonexclusive list of factors to be considered "in determining whether the use made ... is a fair use...." The factors are:

"(1) the purpose and character of the use [including consideration of commercial or nonprofit purpose];
(2) the nature of the copyrighted work;
(3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and
(4) the effect of the use upon the potential market price or value of the copyrighted work."

17 USC §107; see Harper & Row Publishers v. Nation Enterprises, 471 US 539, (1985).

D. Infringement

A copyrighted work may be illegally infringed by exercising any of the exclusive rights, like for example copy and sell an unauthorized copy of a computer program. Computer software and recording piracy involves infringement of copyright and trademark protection afforded to intellectual property, including software for programming computers and connected devices, and audio and video recordings. Because many recordings have been digitized, they can be easily uploaded via computer onto the Internet and then downloaded for playing, copying, or bootlegging.

Other examples include any unauthorized uploading, downloading, or digitalizing of performance or phonogram as acts of reproduction that would infringe the exclusive rights of the copyright holder, make available for downloads illegal copies of copyrighted software, and unlawful uploading and scriber downloading of copyrighted products. Criminal infringement of Intellectual Property and its legislation will be discussed throughout the next chapter.

II. Trade Secrets (18 US § 1839- Definition)

A. Subject Matter and Requirements

Trade secret laws were enacted to prevent unfair means of competition among businesses. It gives protection to its creators by establishing contractual limitations or building legal fences.[21] In 1996, Congress enacted a federal legislation called the Economic Espionage Act (hereinafter EEA) to criminalize the misappropriation of trade secrets and to enable federal courts to prosecute the theft of trade secrets. The EEA is codified at 18 U.S.C. §1831 et seq. and will be fully discussed in the next chapter as well as all the criminal legislation to protect intellectual property from infringement in the

[21] Merges, supra note 13 at page 4, Chapter 1 Introduction, Subsection B, 1 at page 22.

Internet. The definition of subject matter eligible for protection is broad and was first defined by the First Restatement of Torts[22] as: *"any formula, pattern, device, or compilation of information which is used in one's business, which gives [that person] an opportunity to obtain an advantage over competitors who do not know or use it. [A trade secret] may be a formula for a chemical compound; a process of manufacturing' treating or preserving materials; a pattern for a machine or other device; or a list of customers"*[23].

This definition was constructed broader by the Uniform Trade Secret Act[24] by adding any *"information, including a formula, pattern, compilation, program, device, method, technique, or process, that: (1) derives independent economic value, actual or potential from not being generally known to and not being readily ascertainable by proper means by other persons who can obtain economic value from its disclosure or use, and (2) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy"*[25]. Further, the Restatement (Third) of Unfair Competition[26] was enacted, but it seems uncertain whether this will have an effect on the states that apply the Uniform Trade Secret Act and about the one's that still have the Restatement (First) of Torts and have not a adopted it yet.[27]

Trade Secret Laws and its interpretative jurisprudence have established the requirements for certain information to be considered subject matter protected by trade secret laws. The first requirement is the secrecy of the information.[28] This requirement has been interpreted by the courts in several cases and they have concluded that the trade secret laws do not require it to be absolute.

---

[22] Restatement (First) of Torts. This statute was applicable for about 40 years before the Uniform Trade Secrets Act was enacted. Today, about 40 states follow the Uniform Trade Secrets, the rest of the states have either adopted the Restatement (Third) of Torts or still applying the Restatement (First) of Torts. See Gale R. Peterson, Recent Developments in Trade Secret Law in an Information Age, 507 PLI/Pat. 351 (1998).

[23] First Restatement of Torts §757, Comment b (1939).

[24] Uniform Trade Secret Act §1 (4)

[25] *Id*

[26] Restatement (Third) of Unfair Competition §39, Comment b (1995)

[27] Peterson, *supra.*

[28] Phillip Morris v. Reilly, 113 F. Supp. 2d 129, 133-137 (2000)

Meaning that the holder of a trade secret can disclose it *"to a limited extent without destroying its status as a trade secret…if the disclosure to others is made to further the holder's economic interests, it should, in appropriate circumstances, be considered a limited disclosure that does not destroy the requisite of secrecy…"*[29] Meaning that the employer can disclose the company's trade secret to employees that are involve in its use or the disclosure is necessary to perform their work at the company. But Courts have established that the disclosure need to be limited and the employer needs to take reasonable precautions to protect the trade secret as a valuable asset of his company and to avoid becoming generally known[30]. Other companies might have and use a similar or even the same trade secret, discovered by independent creation[31], without destroying the secrecy.

Secondly, the information does not need to be novel as is required in patent law, but it need to possess a *'modicum of originality'* to separate it from general knowledge.[32] Not generally known has been defined as information that it is not everyday knowledge and it is not known to be a customarily information used in an industry. Also, it need to show that the particular trade secret gives the holder commercial advantage over his competitors.[33] Third, the courts have established that the trade secret's holder has the burden of proving the company's reasonable efforts[34] to keep the secrecy of the information and protect it as a valuable property.[35] Courts has suggested that this requirement is necessary to make people aware of the existence of a right and it serve to proof the worth of the trade secret. In determining the reasonable efforts courts will balance between the costs of taking

---

[29] Metallurgical Industries Inc. v. Fourtek, Inc., 790 F.2d 1195 (5th Cir. 1986)

[30] Comprehensive Technologies International, Incorporated v. Software Artisans, Incorporated, 3 F. 3d 730 (1993)

[31] Restatement (Third) of Unfair Competition §43 (about the independent discovery and publicly available products or information); See also Restatement of Torts, Section 757, Comment (f).

[32] Kewanee Oil Company v. Bicron Corporation, 478 F. 2d 1074 (1973)

[33] Metallurgical, *supra.*

[34] E. I. duPont deNemours & Co. v. Rolfe Christopher et al. 431 F. 2d 1012 (5th Cir. 1970)

[35] See Rockwell Graphic System., Inc. v. DEV Industries, 925 F.2d 174 (about reasonable efforts to maintain secrecy).

precautions versus the benefits that might result from it[36]. If the trade secret's holder meets all these requirements, he will be protected not for a certain period of time, but rather as long as the information is kept secret. Once that information becomes public the protection ends.

B. Disclosure of trade secrets

According with Robert P. Merges, Peter S. Menell and Mark A. Lemley in their book Intellectual Property in the New Technological Age[37], a trade secret can be disclosed mainly in five ways. The owner may publish the secret; disclose the secret by selling a commercial product that embodies the secret; publicly disclosed by someone other than the trade secret owner; disclosed inadvertently' or if a government agency require the disclosure of the trade secret by private parties to serve some other social purpose.[38] If any of these actions take place, the trade secret will be infused into the public and the trade secret's owner losses protection for that particular information, process, or any other form of information protected by the trade secret laws.

C. Misappropriation of Trade Secrets

A trade secret is misappropriated when the trade secret is obtained by another party's breach of confidential relationship or through improper means such as physical or electronic theft, espionage or misrepresentation.[39] In a civil case, plaintiff must prove three elements to prevail. First, he or she is the owner of a trade secret. Second, that defendant improperly acquired his trade secret and last, that

---

[36] E. I duPont deNemours, *supra* note 34 at page 11.

[37] Merges, *supra* note 13 at page 4, Chapter 2 Trade Secret Protection, Subsection B: Subject Matter, 3 at page 62.

[38] *Id.*

[39] Boggild v. Kenner Products, 576 F. Supp. 533 (1983)

the defendant knew or should have known that the trade secret was acquired by improper means.[40] The Restatement of Torts[41] guides courts with a list of factors that can be considered to establish whether a trade secret exists; the extent to which the information is known outside the business; the extent to which it is known to those inside the business; the precautions taken by the holder of the trade secret to guard the secrecy of the information; the savings effected and the value to the holder in having the information as against competitors; the amount of effort or money expended in obtaining and developing the information; and the amount of time and expense it would take for other to acquire and duplicate the information.[42]

It has been estimated that corporate espionage costs U.S. businesses about $100 billion annually. For example, on August 16, 2001, a grand jury of the U.S. District Court indicted Aleksey Ivanov for allegedly intruded and threaten to damage computer systems owned by different companies in the United States. Similarly, on August 20, 2001, Geoffrey Osowski and Wilson Tang plead guilty to one count of computer fraud violation for exceeding their authorized access to the computer systems of Cisco Systems and illegally issued stocks to themselves.

III. Trademarks (Lanham Act §45, 15 USC §1127)

A. Subject matter and Requirements

Trademarks are protected under the Lanham Act, 15 U.S.C. §1051, which awards protection to those who were the first to use *'a distinctive mark'* in commerce. Trademark has its origin in the necessity to protect customers from deceptive marks or unfair competition and give them certainty

---

[40] See Sims v. Mack Truck Corp, 488 F. Supp. 592 (1980)(about trade secret requirement and the four factors to prevail in an misappropriation case)

[41] Restatement of Torts, Section 757.

that all products with the same trademark are linked to or have the same origin. Trademark has been defined as a distinctive mark used to differentiate a good or service from others. "It is what makes a product identifiable and distinct, and a customer chose one product over the other, identify it source or origin."[43] The Restatement (Third) of Unfair Competition defines trademark as an *"arbitrary or fanciful mark that could be protected without additional evidence that consumers understand it to identify the source or sponsor of goods or services"*[44]. Further, the Lanham Act[45] defines it as including *"any word, name, symbol or device, or any combination thereof" used by a person "to identify and distinguish his or her goods, including a unique product, from those manufactured or sold by others and to indicate the source of the goods, even if that source is unknown"*[46]. Trademark includes a wide variety of service marks, trade names, certification marks, collective marks and the like.

Callman has identified four characteristics in trademarks that help sellers and customers to communicate more efficiently. First, he identifies the figurative quality of the mark, which translate as the reaction the customer has when in contact with the product; the intangibility and transcendence that he interprets as the reputation a business or its product enjoys; third, is the motivating; and the public acceptability and recognition.[47] He also considers trademarks to poses three important characteristics that fulfill its purpose. A trademark serves to inform the buyer about the origin or source, ownership and quality of the goods and services. It also performs an important and key

---

[42] Phillip Morris, *supra* note 28 at page 9.

[43] See 3 Rudolf Callman, The Law of Unfair Competition, Trademarks and Monopolies §17.01 (4th ed. 1993)(about the utility and function of the trademarks).

[44] Restatement (Third) of Unfair Competition xvi (1995).

[45] 15 U.S.C. §1051

[46] 15 U.S.C. §1127 (1988).

[47] 3 Rudolf , supra .

function on the market and the most powerful tool in the advertisement campaign.[48] All three characteristics share the same goal; to establish in the community a reputation of excellence, quality and sometimes even exclusivity in the goods and services of a company that the law protects from unauthorized use or unfair competition. The right over a distinctive trademark is obtained when a company is the first to continuously use a particular symbol or mark, and people identify and attach that symbol to the company's product, store or service. Once a person identifies the product by looking at the symbol that symbol becomes a trademark protected from infringement.

B. Trade Dress

Trade dress is also protected under the trademark laws and the right to be protected from infringement attaches similarly to the trademarks. The purposes behind these protected trademarks are to protect consumers from product confusion, to make possible the identification of the source of the goods and services and to provide information regarding the goods quality, price and reputation.

C. Infringement

The two fundamental principals are the tort of misappropriation of the goodwill of the trademark owner also known as dilution, and the tort of deception or confusion to the consumer. If there is a likelihood of consumer confusion, the marks are similar and the products compete, the judge in an infringement action will only look at the marks. But if the products are related but do not compete, the judge should assess a multi-factored test that includes the strength of the mark, the proximity of the goods, similarity of the marks, evidence of actual confusion, marketing channels used, type of goods and the degree of care likely to be exercised by the purchaser, the defendant's intent in

---

[48] *Id.* See also James L. Robertson, 15 Miss. C. L. Rev. 331, 332, (Spring 1995) The Law of Business Torts in Mississippi (citing and discussing these important characteristics established by Callman)

selecting the mark and likelihood of expansion.[49] Another new cause of action for trademark infringement is called dilution and does not require the likelihood of confusion. Dilution is defined in section 43(c) of the Lanham Act as "the lessening of the capacity of a famous mark to identify and distinguish goods or services, regardless of the presence or absence of (a) competition between the parties, or (b) likelihood of confusion, mistakes, or deception". This cause of action applies when the trademark is used by a unauthorized users and as result it reduces the consumer's perception of the uniqueness of a famous mark. Trademark can be infringed by selling a good with a counterfeit mark, or by using other company's trademark to identify a product or service, or by tarnishing the image of an original product.[50] There also exists am prohibition against false or misleading advertising.

---

[49] Merges, *supra* note 13 at page 4, Chapter 5 Trademarks and Trade Dress, Section D. Infringement, pages 682-689.

[50] See *Id* at pages 711-712.

CHAPTER 2

THE IMPACT OF THE INTERNET IN THE EVOLUTION OF THE INTELLECTUAL PROPERTY LEGISLATION

I. New Legal Challenges Created by Cyberspace

Although intellectual property crimes have been in existence for a long period of time, the law enforcement and the prosecutors are now confronted with other challenges, in particular, the absence of a legal scheme that can address efficiently the prosecution of cyber crime. Due to the rapid pace of computer and Internet developments, most of the statutes regarding cyber crime fall behind leaving prosecutors without guidance to punish and deter this type of crime. With the fast advances in technology most of the existing laws concerning computer crime lag behind this unfolding making difficult for the prosecutors to have laws applicable to the deterrence and punishment of computer crimes.

As any other advances in science and technology, computers have had an exponentially impact in our society with great advantages, but also disadvantages. Computers and the Internet have dramatically changed how people conduct their lives and businesses. Its use and capacity has added new dimensions to individuals and corporations. Nevertheless, just as people use the Internet to communicate with family and friends, or to conduct their business matters, criminals use it to appropriate trade secrets, steal money from banks accounts, theft of identities, unauthorized use of other's people credit cards accounts, to infringe intellectual property rights, etc. Although civil

remedies provided enough compensation to misappropriation of intellectual property rights in the past, today criminal sanctions are completely necessary for the punishment and deterrence of that illegal activity, or otherwise a chaos could be possible. Unfortunately, computers allow criminals to commit crimes in new ways that legislation had never contemplated before, creating the necessity of new legislation to bring criminals to justice. Congress has been working hard creating laws to provide protection to the intellectual property owners and fight these new crimes for the last 11 years. Many states have also taken the initiative by implementing new legislation to prosecute cyber criminals. Nevertheless, there exist a great variety of misuses and infringements of intellectual property or actions not yet included in any criminal legislation nor (e.g. patent law infringement) contemplated in the new legislation. For example, infringement of a patent is not a criminal violation, but the use of the internet to access the confidential information regarding the patented product formula could be.

Even though criminal legislation for intellectual property crimes has been in existence since 1897 when the first copyright law came to existence it's today, due to the invention of internet and therefore an enormous increase in violations of intellectual property, that Congress and States have seen the necessity to use those laws actively, not only in the prosecution to deter cyber criminals, but also in the construction of new legislation to adapt those laws to the new technological era.

Intellectual property infringement was first considered a crime back in 1897 having its first revision in 1909 with the Copyright Act of 1909. According to the 1909 Copyright Act, willful copyright infringement with the intention to profit was classified as a misdemeanor. In 1976 the Copyright Act was revised and dramatically changed as a whole. For example, criminal infringement was modified by changing one of the elements, "for profit", to extent it to any "commercial advantage or private financial gain". A significant change occurred in 1982 when Congress, force by the demands of the motion picture and recording industries, enacted a new law to make criminal copyright

infringement a felony and establish its punishment. This amendment incorporated section 2319 to Title 18 and section 506 of the Copyright Act.

Another significant amendment in favor of intellectual property owners occurred in 1997 when Congress, pressured by the computer companies and the like, submitted a bill petitioning to make illegal the distribution of copyrighted material even though there was no profit motive. After an arduous debate the bill was passed by Congress. Congress has approached this legislative issue both ways, by amending existing laws to cover crimes committed in cyber space and enacting new laws and programs. Others provisions includes the enactment of the Economic Espionage Act (hereinafter EEA) for theft of trade and the counterfeit of trademarks contained in 18 U.S.C. §2320. EEA contains two provisions; section 1831 that requires that the theft of trade secret had been done for the benefit of a foreign country, and section 1832 which does not require that element.

Despite this new legislation and the cooperation of many states in the creation of their own computer laws, courts and prosecutors have frequently experienced difficulties in prosecuting or convicting cyber criminals under the traditional criminal prosecution.

II. New Legislation to Prosecute Cybercrime against Intellectual Property

Today some groups regard cyber crimes as any other traditional and ordinary crime with the difference that is committed using the advance technology now available. Those groups consider current legislation to be enough and efficient for the prosecution of cyber crime. There are others who deem cyber crime as a new type of crime requiring a different legal framework to address the never ending creation of new technology and the different challenges it imposes in the legal system by giving criminals new ways to violate the different proprietary rights that were not foreseeable in prior laws. Desperately seeking ways to prosecute cyber criminals, Congress and Prosecutor have approached computer crime in two ways as a traditional crime committed by new methods, or as

crime unique in character requiring new legal frame work. Proof of these approaches are the different amendments to existing laws, and the enacted of new legislation reflecting the changes in technology that can be adapted to future changes. These enacted laws were constructed broad enough to allow new type of crimes to fit under its definitions or to be added by means of amendment without further problem.

A. Copyright Protection

Copyright is protected by Title 17 of United States Code. Several amendments have been added to section 101 and the followings of Title 17 to include new definitions, amendments and treaties in an effort to conform copyright law to the internet and the computer technology developments. Section 506 of title 17 affords the copyright owner with criminal prosecution for infringement. This section set up that copyright infringement constitutes a crime when it is committed willfully, either for commercial advantage or private financial gain, by reproduction or distribution of one or more copyrighted works.[51] On the other hand, Title 18 U.S.C. §2319 provides for the punishment of criminal infringement of copyright.

(US v. Moghadam, 175 F.3d 1269 (1999)

1. Elements to configure the crime

There are four elements to a charge of felony copyright infringement. In order to file criminal charges against suspect, government must demonstrate; that a copyright exists and is protected (see Chapter One regarding protectable works of authorship; second, defendant infringed it by

[51] Title 17 U.S.C. §506. "Criminal Offenses, (a) Criminal Infringement-Any person who infringes a copyright will fully either (1) for purposes of commercial advantage or private financial gain, or, (2) by the reproduction, including by electronic means, during any 180-day period, of 1 or more copies or phonorecords of 1 or more copyrighted works,

reproduction or distribution of the copyrighted work; third, defendant acted willfully; and last, defendant infringed at least 10 copies of one or more copyrighted works with a total retail value of more than $2,500 within a 180 day period.

The first element of criminal copyright infringement includes all the necessary requirements for a protected work of authorship to be protected under the copyright laws. This element is proven by presenting a certificate of registration of the protected work of authorship. Also, a certificate of registration obtained within 5 years of its first publication is considered to be prima facie evidence of its validity.[52] Once the prosecutor proved the existence of a protected work the burden of proof shifts to the defendant to present evidence to the contrary.

The second element can be proved if the infringer copy, distributes, creates derivative work, performs or displays a copyrighted work without the owner's authorization; proving that he or she had access to the copyrighted work; and the copies or reproduction is substantially similar to the copyrighted work. Section 501(a) provides that *"anyone who violates any of the exclusive rights of the copyright owner"* is an infringer[53]. However, only two of those actions will constitute a felony infringement; if the accused has violated either the reproduction or distribution rights of the copyright owner[54]. Always keeping in mind that independent creation is also possible and does not constitute an infringement. See Columbia Pictures Industries, Inc. v. T&F Enterprises, Inc. aka T&P Enterprises, Inc. dba Four Star Video & Communications, 68 F. Supp. 2d 833 (1999).

Third, willful conduct for commercial advantage or private financial gain. United States v. Cross, 816 F. 2d (1987) explains that the word willfully *"as used in the statute means the act was committed by*

---

which have a retail value of more than $1,000, shall be punished as provided under section 2319 of title 18, United States Code"

[52] 17 U.S.C. §410(c).

[53] 17 U.S.C. §106

a defendant voluntarily, with knowledge that it was prohibited by law, and with the purpose of violating the law, and not by mistake, accident or in good faith". Prosecutor must present proof of defendant's intention to derive financial gain or benefit, but does not have to prove actual gain or benefit. Defendant's purpose to obtain gain and/or benefit, either as the master mind of the criminal conduct or conspirator, is sufficient evidence to configure this element and therefore, to secure a conviction. This statute does not require realization of actual benefit or gain as long as the action was conducted with that purpose or intention in mind. This element enhances the maximum penalty. If this is proven the maximum prison sentence can rise to 5 years and 10- years for second offenders.

In addition, the number of reproduced or distributed copies and its value will dictate whether that particular criminal violation constitutes a misdemeanor or a felony. If the criminal action involves 10 copies or more and the value exceeds $2,500 in a period of 180 days, it is consider a felony. However, if the copies are fewer or the value is lower than $2,500, it is a misdemeanor. In US v. Laracuente 952 F. 2d 672 (1992) defendant copied more than 2,500 tapes with a total value of $180,000. Julio Laracuente was only sentenced to 12 to 18 months in prison.

Misdemeanor copyright infringement[55] is another option for prosecutors. This classification is commonly used in cases where scale of the crime is difficult to prove with specificity. For misdemeanor violations, a defendant may be sentenced to up to one year imprisonment and fined up to $100,000. In United States v. Cross, supra, defendants were convicted for criminal infringement, but they appealed arguing that the evidence at trial did not support a conviction for a felony criminal infringement of a copyright[56]. Appellants contended that the government did not prove beyond reasonable doubt the rental of more than 10 copies within the 180 days. The evidence introduced at

---

[54] Purchase of pirated copies of motion pictures on video cassettes, dvds or any other instrument capable of transmission and offered them for distribution to the general public without the copyright owner's permission, violates Title 17 §506.

[55] See 18 USC §2319(b)(3)

trial by the prosecution proved beyond reasonable doubt the rental of only six second-generation videos, out of the eleven, because they could not related or matched the control numbers on the rental invoice, the containers and on the videocassettes. Their sentences were vacated and remanded to the district court for re-sentence based on misdemeanor violations.

In 1999 due to the increasing number of infringements without profit motive, Congress decided to amend Section 506(a)(2) of Title 17 of the United States Code to provide for prosecution in the absence of profit motive. This amendment allows prosecution of large scale reproductions and distributions where even though the accused acted willfully, he or she did not have a profit motive.[57] And in May, 2000 a sentencing enhancement was made applicable to those individuals who uploaded copyrighted material with the intent to let others download such material.[58]

B. Digital Millennium Copyright Act of 1998

1. Scope of the Digital Millennium Copyright Act

The Digital Millennium Copyright Act was enacted to prosecute and sentence individuals that designed and offered to the public technologies to circumvent copyright protections. The act requires prosecutors to prove two key elements; (1) the use or dissemination of technology to circumvent protected copyrights, (2) with the purpose of obtaining commercial advantage or financial gain. DMCA prohibits the offer, dissemination or traffic in technologies created to circumvent measures

---

[56] 18 USC §2319(b)(2)(B)

[57] This amendment was done as part of the creation of No Electronic Theft Act of 1997, Pub.L.No. 105-147, 111 Stat. 2678. See also the U.S. Department of Justice website regarding prosecution of Intellectual Property Crimes.

[58] See U.S. Sentencing Commission, Guidelines Manual §2B5.3(b)(2)(Nov. 1998 & Supp. 2000).

that control access to copyrighted works. This is evident when an individual knowingly makes available to the public a circumvention technology with the intention to allow others to acquire it.[59]

17 U.S.C. §1201 addresses circumvention of technological measures intended to protect copyrighted works. The statute states that: *"to circumvent a technological measure means to descramble a scrambled work,...decrypt an encrypted work or otherwise... avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner"*. Section 1201(a)(2) specifically prohibits *"offering to the public, providing, or otherwise trafficking in any technology designed to circumvent a technological measure that controls access to a copyrighted work"*. This section was interpreted in Universal City Studios, Inc. v. Reimeders, 111 F.Supp.2d 294 (2000)[60] when the Court stated that this section includes as prohibited conduct, when one presents, holds out, or makes available a circumvention technology or device, knowing its nature, for the purpose of allowing others to acquire it. Furthermore, discusses that when the owner of a website posts links to another websites to automatically download computer software that decrypts digitally encrypted movies on DVD, contains code for decryption software or offers user choice of downloading decryption software, the owner is violating the Digital Millennium Copyright Act by providing and offering technology designed to circumvent access to copyrighted work.[61]

17 USC §1202 provides protection for the integrity of copyright management information. Copyright management information is defined as any of eight specific kinds of information conveyed in connection with copies of a work, such as the title of the work, the name of the author, and the terms and conditions for the use of the work. In July, 2001 a Russian man was charged in California under the Digital Millennium Copyright Act for circumventing Adobe eBook Reader. Adobe eBook Reader is a software that consumers can download into their computers to purchase electronic books.

---

[59] 17 U.S.C.1201(a)(2)

[60] Universal City Studios, Inc. v. Reimerdes, 111 F.Supp.2d 294(2000) Headnote 10.

[61] *Id.*

eBook reader allows that person to download the encrypted book and read it in that particular personal computer without affecting the copyright holder's interest.[62] According with this release Mr. Sklyarov is allegedly the author of a program called "Advanced eBook Processor" that decrypts Adobe eBook Reader allowing users to open an eBook in any portable document format (PDF) without paying the fee to the bookseller or restrictions on editing, copying or printing.

Section §1204 of the 17 U.S.C. states the penalty imposed for any infringement of Sections 1201 or 1202:

> *"(a) In General.- Any person who violates section 1201 or 1202 willfully and for purposes of commercial advantage or private financial gain-*
> *(1) shall be fined not more than $500,00 or imprisoned for not more than 5 years, or both, for the first offense; and*
> *(2) shall be fined not more than $1,000,000 or imprisoned for not more than 10 years, or both, for any subsequent offense.*
> *(b) Limitation for Nonprofit Library, Archives, Educational Institution, or Public Broadcasting Entity.- Subsection (a) shall not apply to a nonprofit library, archives, educational institution, or public broadcasting entity (as defined under section 118(g)).*
> *(c) Statute of Limitations.-No criminal proceeding shall be brought under this section unless such proceeding is commenced within five years after the cause of action arose."*

The first indictment was announced in August 28, 2001, when the U.S. Attorney's Office of the Northern District of California filed charges against Elcom, Ltd. and Demitry Sklyarov[63], both from Russia, on five counts of copyright violations. According to the U.S. Department of Justice Press Release of August 28, 2002, defendants were indicted with one count of conspiracy to traffic in technology designed and marketed to circumvent protected copyrights in violation of Title 18 § 371, two counts of trafficking with technology created primarily to circumvent technology that protects a rights of a copyright owner in violation of Title 17 §1201(b)(1)(A), and two counts of trafficking in

---

[62] Russian Man Charged in California under Digital Millennium Copyright Act with Circumventing Adobe eBook Reader, July17, 2001, Press Release, U.S. Department of Justice, United States Attorney, Northern District of California. www.usdoj.gov/criminal/cybercrime/Skylyarov.htm.

[63] *Id.*

technology marketed for use in circumventing technology that protects a right of a copyright owner, no under Title 17 §1201(b)(1)(C).

2. Defenses

A person who acquires or discovers information through the reverse engineering[64] exception is allowed to share that information with others without violating the rights of the copyright owner. In Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, the court, after consideration of all facts, held that this exception applies only to the dissemination intended to achieve interoperability (OS) as defined in the statute, and did not apply to public dissemination of a means of circumvention, and defendants knew that decryption software would run under other OS and could therefore be used to decrypt media files copies onto computer hard drives violating copyrighted movies.[65]

The encryption research defense does not apply where software was disseminated to facilitate copyright infringement, rather than to advance the general knowledge of encryption technology. In Universal, supra, there was no evidence that defendants made any effort to provide results of the research to copyright holders, instead defendants posted computer software program that decrypted movies on DVD in the Internet.

C. Economic Espionage Act of 1996

1. Protection of Trade Secrets

Economic Espionage Act 1996 (Theft or Misappropriation) is also known as the "Protection of Trade Secrets" and it became Public Law 104-294 on October 11, 1996. This statute was created in

[64] 17 U.S.C. A..§1201(f)

response to the corporate increasing loses on stolen corporate intellectual property and the absence of laws that could offer a remedy to target the problem.[66] This statute provides that theft of trade secrets from a company or individual can be convicted and punished with a fine of $5,000,000 for corporations or organizations, and fine and/or imprisonment for individuals not to exceed 10 years. The Act applies to theft of trade secrets that occurred within the United States and that of U.S. Citizens or U.S. corporations outside of United States and was enacted to cover the loopholes that federal and state law could not cover with existing state criminal statutes. For example, before the creation and enactment of this act, economic espionage was cover by the Trade Secrets Act, 18 U.S.C. §1905, which only prohibits disclosure of trade secret by a government employee, but does not apply to private or corporate employees. Other statutes protecting trade secrets were enacted even before the creation of computers.

2. Subject Matter and Requirements

A trade secret is defined at §1839 of Title 18 as *"all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing"*[67], if the owner has taken reasonable measures to keep that information secret, and the information protected derives independent economic value, actual or potential, and advantage over other companies. Prosecutor needs to prove that a trade secret exists; the owner has taken reasonable measures to keep it secret, the owner of the trade secret derives independent economic value and defendant misappropriated, either

---

[65] Universal City, *supra* note 60 at page 23.

[66] See United States v. Hsu, 155 F. 3d 189 (3rd Cir. 1998)

[67] 18 U.S.C.A. §1839, Definitions

by physical action or with the assistance of an electronic device or machine. However, the EEA has included a broader definition of a trade secret in an effort to protect technological and intangible information not as of that moment protected. In United States v. Hsu, *supra*, the Court states that a wider variety of information is now protected by the EEA, including programs and codes, whether tangible or intangible and whether or how stored.[68] Also the Court states that *"EEA contains a definition crafted to reach only illicit behavior"*[69].

3. Application of the Law[70]

The EEA contains two separate sections that penalize the theft of trade secrets. Under each section the government must prove beyond reasonable doubt that the defendant stole, or without authorization of the owner, obtained, destroyed, or conveyed information, that the defendant knew this information was proprietary and the information was in fact a trade secret. To establish a violation of the economic espionage provision, the government must also prove that the defendant knew the offense would benefit or was intended to benefit a foreign government, foreign instrumentality or foreign agent.

Section 1831 of Title 18 of the USCA divides economic espionage in three categories; when an individual (1) *"knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent, knowingly steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains a trade secret",* (2) *"without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys a trade*

---

[68] *Id.*

[69] *Id.*

[70] See 18 U.S.C.A. §1831-1839.

secret'"[71]. The drafters of this Act included as ways of misappropriation the interception of oral, wire and electronic communications used to obtain business secrets. And third (3) *"receives, buys, or possesses a trade secret, knowing the same to have been stolen or appropriated, obtained or converted without authorization"*[72]. In my interview with an Special FBI agent, he told me that it is really hard to find and hard to prove and prosecute under this section due to the difficult task of proving a government intervention. Sentence for this section is imprisonment for not more than 15 years and not more than $500,000 in fine, or both. For corporations the maximum fine allowed is $10,000,000.

Section 1832[73] classifies the criminal conduct in the same three categories, but this section particularly applies to *anybody* who knowingly intents to convert a trade secret of a product that is, either produce intestate or in foreign commerce, for the benefit of an individual other than the owner. If government cannot establish that the defendant acted with the intent to benefit a foreign entity, the government can still establish a violation under section 1832 if it can establish, in addition to the elements above-mentioned, three additional elements. First, defendant intended to convert the trade secret to the economic benefit of anyone other than the owner. Second, defendant knew or intended that the owner of the trade secret would be injured, and last, the trade secret was related or was included in a product that was produced or placed in interstate or foreign commerce. This crime carries imprisonment for not more than 10 years or a fine, or both, and a fine of not more than $5,000,000 for corporations.

---

[71] 18 U.S.C.A §1831

[72] *Id.*

[73] 18 U.S.C.A. §1832

D. Trademarks

1. Subject Matter and Requirements

Section 2320 of Title 18 penalize individuals who intentionally traffic or attempt to traffic counterfeit goods or services and knowingly use counterfeit mark. Traffic is defined by the statute as a *"means to transport, transfer, or otherwise dispose of, to another, as consideration for anything of value, or make or obtain control of with intent so to transport, transfer, or dispose of"*[74]. This law was created with two objectives in mind, first to protect consumers from buying and paying for a product that it is not authentic and to protect trademark owners' reputation and quality of products.

On the other hand, counterfeit mark is defined as "*a spurious mark that is used in connection with trafficking in goods and services; that is identical with, or substantially indistinguishable from, a mark registered for those goods or services on the principal register in the U.S. Patent an Trademark Office and in use…and the use of which is likely to cause confusion, to cause mistake, or to deceive; or spurious designation that is identical with, or substantially indistinguishable from, a designation as to which remedies of the Lanham Act are available…"* The test for likelihood of confusion has been repeatedly interpreted by the Courts as the confusion created in an ordinary person of the community when that person sees the counterfeit good or mark.

This Section also provides for severe punishment, imposing a fine for an individual of not more than $2,000,000 or imprisonment for not more than 10 years, or both. If it is a person other than an individual, he should be fined for not more than $5,000,000.

---

[74] 18 U.S.C.A. §2320

E. Other Statutes

1. Trafficking of Counterfeit Labels

Section 2318 of Title 18 prohibits the counterfeit labeling of copyrighted works. In particular this section states that *"whoever, …knowingly traffics in a counterfeit label affixed or designed to be affixed to a phonorecord, or a copy of a computer program or documentation or packaging for a computer program, or a copy of a motion picture or other audiovisual work…"* Counterfeit label is defined as an *"identifying label or container"* affixed to a particular product that seems to be original or genuine, but is not.

2. Trafficking in Recordings of Live Musical Performances

Section 2319A of Title 18[75] protects live musical performances from being fixated and trafficked without the authorization of the copyright owner. This section is divided in three subsections protecting different rights of the performing artist. First,*"whoever, without the consent of the performer or performers involved, knowingly and for purposes of commercial advantage or private financial gain (1) fixes the sounds or sounds and images of a live musical performance in a copy or phonorecord, or reproduce copies or phonorecords of such a performance from an unauthorized fixation…"*. This subsection prohibits the fixation of live musical performance without the performers' authorization.

Subsection 2 sanction *"whoever…(2) transmits or otherwise communicates to the public the sounds or sounds and images of a live musical performance…"*. This section prohibits the transmission of bootleg performances through the radio or television. And subsection 3 punish *"whoever…(3) distributes or offers to distribute, sells or offers to sell, rents, or offers to rent, or traffics in any copy or phonorecord fixed…"*. This last

[75] 18 U.S.C.A. §2319A, Pub. L. No. 103-465, 108 Stat. 4974 (1994).

subsection prohibits the distribution or trafficking to the public of any fixed recording of live musical performance without authorization from the performers.

CHAPTER 3

CRIMINAL INVESTIGATION OF INTELLECTUAL PROPERTY CYBERCRIMES

The criminal investigation is one of the biggest challenges imposed in the legal system and law enforcement by cyber crime against intellectual property, not only for the complexity of the subject matter, but also because of the technical, operational and legal challenges involved. The Department of Justice in conjunction with law enforcement has the operational challenges to ensure well-trained personnel, including investigators, specialized prosecutors and instructed judges. As part of the initiative to educate, investigate and prosecute cyber crime, the Department of Justice founded a division called Computer Crime Unit, which in 1996 became the Computer Crime and Intellectual Property Section (hereinafter CCIPS)[76]. This division works closely on computer crime cases with another section of the Assistant United States Attorneys, known as Computer and Telecommunications Coordinators (CTC) in each of the U.S. Attorneys' Office nationwide. They also work in conjunction with the other law enforcement agencies including the Federal Bureau of Investigations (FBI), Central Intelligence Agency (CIA), the U.S. Secret Service and U.S. Customs Service, in an effort to coordinate and create guidelines for the conduction of the investigation and

[76] This division started with only five attorneys and has grown to 22 attorneys by September 6, 2001. Today, the Computer Hacking and Intellectual Property Unit is extending its operation to 9 cities; San Francisco, Los Angeles, San Diego, Atlanta, Boston, New York (Brooklyn and Manhattan), Dallas, Seattle and Alexandria. There will be a total of 77 positions, including 48 prosecutors. (As announced in a Conference by Attorney General Ashcroft's in September 6, 2001).

federal prosecution in computer crimes[77]. Also other sections of the criminal division are involved such as the Fraud Section, the Child Exploitation and Obscenity Section and the Terrorism and Violent Crime Section. CCIPS is considered the central point of contact for investigators and prosecutors when they confront problems arising from the new technology developments. It is also a key component in enforcing the "Economic Espionage Act"[78], enacted in 1996 with the purpose to deter and punish theft of valuable trade secrets. Further, CCIPS attorneys have the responsibility to litigate computer crime and intellectual property cases and sometimes even lead the investigation.

On 1998, in response to the exponentially growing capacities of the Internet and it challenges, the National Infrastructure Protection Center (hereinafter NIPC) was created. This agency consists of investigators, computer scientists and analysts that devote their entire shift to work in the investigation of computer crimes. It is also in charge of the coordination of the FBI's investigation of computer crimes. On January 2001, the Department of Justice published a Manual for Prosecution of Intellectual Property Crimes[79] that supersedes a previous version published in May, 1997. This Manual contains the new developments in the law and practical procedures to better prosecute and pursue cases involving intellectual property crimes. Martha Stensell-Gamm, Chief of the Computer Crime and Intellectual Property Section of the Department of Justice said *"the insights and practical guidance in this new manual will help us tackle the complex issues in IP cases that we are seeing every day"*[80]. This 2001 Manual

---

[77] The CCIPS provides legal advice and technical instruction for exercises and seminars to senior personnel on information warfare, infrastructure protection, and other topics for the Department of Defense, the National Security Agency, the Central Intelligence Agency, and others. CCIPS is making efforts to train local, state, and federal agents and prosecutors on the laws governing cybercrime, and last year alone gave over 200 presentations to a wide variety of audiences. In addition, CTCs across the country are training prosecutors and agents in their districts. CCIPS has also coordinated an interagency working group consisting of all the federal law enforcement agencies, which developed guidance for law enforcement agents and prosecutors on the many problems of law, jurisdiction, and policy that arise in the online environment. See www.cybercrime.gov/ccips.html for more information about the CCIPS.

[78] 18 U.S.C. §1831 et seq.

[79] See www.usdoj.gov/criminal/cybercrime/ipmanual for more information about this manual.

[80] *Id.*

contains eight chapters discussing the subject matter of intellectual property and its protective rights, law protection given to trademark and copyright, how it can be criminally misappropriated, criminal copyright infringement, elements of the crime, and the defenses for misappropriation and copyright infringement. Further, it discusses the enforcement of intellectual property laws, penalties and novel issues related to the Internet. Also, the manual states other federal criminal laws that protect intellectual property and it provides guidance on whether to charge or not for intellectual property infringement and how to proceed, including an analysis of other charges that could be considered under other applicable laws. Finally, it states the sentencing guidelines and restitution, and the theft of commercial trade secrets under the Economic Espionage Act, 18 U.S.C. §1831 and §1832. This manual is just one example of the U.S. Department of Justice's response to the increasing concern for intellectual property infringement by promoting guidelines and educating its personnel in intellectual property rights.

I. Cyber crime

Cyber crime takes place in what most people refer to as the 'information superhighway' or "cyberspace". Anne M. Fulton in her remarks, *"Cyberspace and the Internet: Who will be the Privacy Police?"*[81], says that cyber crime takes place in cyberspace, which is a 'nonphysical place' where electronic communications happen and digital data are located. She defines cyberspace as *"an immense network of networks that connects an estimated twenty million computer users by telephone lines to thousands of electronic information storehouses worldwide"*[82]. Computer networks are considered systems of interconnected computers that allow an individual to exchange communication between computers, and the Internet

[81] Anne Meredith Fulton, Comment, *"Cyberspace and the Internet: Who Will be the Privacy Police?"*, 3 CommLaw Conspectus 63 (1995). See also Philip Elmer-DeWitt, *"Welcome to Cyberspace: What Is It? Where Is it? And How Do We Get There?"*, Time, Mar. 22, 1995, at 4, 6.
[82] *Id.*

is the largest computer network.[83] In cyberspace people are communicating with friends, conducting their private matters and business by creating or accessing data from any location and saving it in hard drives. Those hard drives are witnesses of private information transferred using the Internet, what makes possible for others to peek at almost any information. It is estimated that the Internet is growing at a pace of 10% monthly[84]. In a survey reported by the New York Times on May 29, 1995, the Internet has about 13.5 million users and 27.5 million e-mail users.[85] As the Internet makes possible to access confidential information by an authorized individual, that information can also be accessed by other unauthorized individuals or intruders with the skill and knowledge to violate the code, encryption or passwords that restrict the access to data without leaving any track.[86] Once that person has access to confidential or protected information, it can be used to commit a number of unimaginable crimes that includes a wide variety of copyright infringement, trade secret espionage, rapist looking for their preys, and child pornography.

A. Classification of the types of cyber crimes

In order to define and facilitate the investigation of cyber crime the U.S. Department of Justice has classified them in three broad categories: when the computer is used as a target (victim), medium (tool) or incidental to other criminal offenses.[87] Crimes using a computer as a target or victim of an

---

[83] See Edward Cavazos and Gavino Morin, *Cyberspace and the Law: Your Rights and Duties in the On-Line World,* 2-11 (1994).

[84] Edward Baig, *Ready to Cruise the Internet?*, Bus. Wk., Mar. 28, 1994, at 180, 180.

[85] Peter H. Lewis, *On the Net,* New York Times, May 29, 1995, at 39

[86] See Michael Adler, *"Cyberspace, General Searches, and Digital Contraband: The Fourth Amendment and the Net-wide Search",* 105 Yale L.J. 1093 (1996).

[87] Mark Sherman, *Introduction to Cyber Crime, "What is cyber crime?"* Special Needs Offenders Bulletin, No.5, August, 2000. Published by the Federal Judicial Center. In this article Mr. Sherman states that *"cyber crime is difficult to define because it ranges from crimes that cannot be committed without a computer to traditional crimes that are merely facilitated by computers or connected devices. In its March 2000 report, the President's Working Group on Unlawful Conduct on the Internet" provided helpful framework for thinking about cyber crime. According to the Working Group, cyber crime can be carried out in one of three ways:*

offense include actions that attack the confidentiality, integrity or availability of the information or services. The second type includes actions where the computer is used as the tool to commit traditional criminal conduct. This category includes those crimes that have been occurring in the physical world but now we are seeing with increasing frequency on the Internet. Examples of this type include child pornography, fraud and intellectual property violations. In the third category, the computer is used to store data, and can seized to obtain evidence of any crime, especially white collars crimes and viruses for example.

As early as 1985, Douglas M. Reimer wrote the article "The low side of high tech" discussing the advantages of the computers as well as the "dark side" which he synthesize as 'the criminal use of these computers'. He mentioned that Irving Sloan has also categorized the roles of a computer in four:

1. *"Object: includes the use of the computer to destroy others computers, data, programs, supportive facilities or resources that allow the computer to function.*
2. *Subject: when the computer is the site or environment of a crime or the source of unique forms and kinds if assets*
3. *Instrument: some types and methods of crime are complex enough to require a computer as a tool.*
4. *Symbol: a computer may be used as a symbol for intimidation or deception"*[88]

He further says that usually all computer crimes involve one or more of the above-mentioned roles. The scope of this paper is limited to intellectual property crimes committed using the computer as a tool and as a target.

In 1999 as part of President's Clinton initiative to combat cyber crime, his administration designated a group of technical experts to handle different issues brought by the computer crimes. The

---

· *Computer as object, victim, or target.*

· *Computer as subject or storage device*

· *Computer as instrument or tool."*

Mark Sherman is an Education Specialist for the Court Education Division, Federal Judicial Center in Washington, D.C.

[88] *Id.*

President's Working Group on Unlawful Conduct on the Internet published 'The Electronic Frontier: The Challenge of Unlawful Conduct Involving Use of the Internet"[89] which is a report on the policy framework and legal analysis of the nature of unlawful conduct with the use of computers and specially, the internet. It also discusses the needs and challenges created by the use and misuse of the Internet and the difficulties this bears on law enforcement.

B. Challenges

In May, 29, 2000 the International Computer Crime Conference titled "Internet as the Scene of Crime"[90] was held in Oslo, Norway with the participation of 33 nations. The Conference addressed primarily the new challenges the Internet poses on the law U.S. Department of Justice and law enforcement. Mr. James K. Robinson, former Assistant Attorney General for the Criminal Division at the United States Department of Justice during Mr. President Clinton Administration, spoke about the major challenges for law enforcement agencies in their fight against cyber crime. He divides those challenges into three major categories: *"Technical challenges that hinder law enforcement's ability to find and prosecute criminals operating online; legal challenges resulting from laws and legal tools needed to investigate cyber crime lagging behind technological structural, and social changes; and operational challenges to ensure that we have created a network of well-trained, well-equipped investigators and prosecutors who work together with unprecedented speed – even across national borders"*[91]. In this chapter, I will discuss the technical and operational challenges only, since the legal challenges were discussed in the prior chapter.

---

[89] The President's Working Group on Unlawful Conduct on the Internet, *'The Electronic Frontier: The Challenge of Unlawful Conduct Involving Use of the Internet"*, Washington, D.C.: U.S. Department of Justice (March 2000), www.cybercrime.gov.

[90] See James K. Robins, International Computer Crime Conference, "Internet as the Scene of Crime", Oslo, Norway, May 29-31, 2000. www.cybercrime.gov/roboslo.htm.

[91] *Id.*

1. Technical challenges: Identification of the suspect and the 'electronic trail'[92]

One of the biggest challenges is the identification of the suspect and the electronic trail. Usually, computer systems keep track of all authorized and unauthorized access attempts. Those records or computer logs provide useful and critical information about where to start the investigation and can only be perceived by a well trained agent or computer specialist who after identifying the starting point can trace the route from computer to computer through the World Wide Web (hereinafter WWW)[93]. Nevertheless, there are instances in which the nature of the Internet[94] allows criminals to hide their identity and trail by gaining unauthorized access, hide their Internet Protocol (hereinafter IP)[95] address, use different Internet Service Providers (hereinafter ISP) to hide their tracks, use third's party computer, or alter the victim's log, among others.[96] All computers with Internet service are assigned a different numeric Internet Protocol (IP) address while online, similar to a physical address for a house or building, key to start the investigation, but if the cyber criminal find the way to hide it, then it is more difficult to trace the starting point.[97]

If the cyber criminal uses multiple computers before reaching the victim computer to hide his/her current location, it would be necessary to identify all locations used by the hacker to reach the

---

[92] See Daniel A. Morris, "Tracking a Computer Hacker" updated page July 10, 2001 at www.cybercrime.gov. Daniel A. Morris is an Assistant United States Attorney and Computer and Telecommunications Coordinator in the District of Nebraska.

[93] World Wide Web means all the resources and users on the Internet that are using the Hypertext Transfer Protocol (http). HTTP is an application protocol which is the basis for information exchange on the Internet.

[94] Internet has been defined as the worldwide network of computer networks providing file transfer, remote log-in, electronic mail, news, and other services.

[95] Internet Protocol is the most important of the protocols on which the Internet is based. IP allow a packet of data to travel through different networks on its route to the final destination.

[96] Morris, *supra.*

[97] *Id.*

local point. It would be necessary to obtain subpoenas and court orders for each point to identify the primary source of the communication.[98]

Cyber criminals can also choose to commit crimes in other international jurisdictions that do not criminalize those acts or in areas of the world where sometimes government cooperation is minimal or nonexistent. Therefore, even crimes that seem local in nature might require international assistance and cooperation. This would happen if the hacker routes his communications through multiple providers in different international places before accessing the victim's computer. In that case, international cooperation is crucial not only from the country the cyber criminal was located and at the place the crime has its results, but also in all other countries through where the track of communication took place. The fact that cyber criminals could choose to use international ISP to hide, establishes great difficulties in particular because of the necessity of international cooperation and the non existent computer legislation in some countries. The U.S. Government has been working in international negotiations to obtain mutual assistance in the borderless nature of computer crime. The CCIPS[99] chairs the G-8 Subgroup on High Tech Crime that has established mutual assistance in computer crime with 15 countries. This assistance has established points of contact 24 hours a day, seven days a week.

The involvement of private entities, such as ISP companies, is crucial to gain access to the log files. But sometimes law enforcement does not have records from the ISP's, either because they do not keep records for a long time or do not keep them at all.[100]

---

[98] *Id.*

[99] CCIPS also plays a leadership role in the Council of Europe Experts' Committee on Cyber crime, and in a new cyber crime project at the Organization of American States.

2. Operational challenges

The operational challenges have brought a series of important issues that need prompt attention. A well trained personnel with expertise in high technology, computers and telecommunications with the capacity to investigate and prosecute these sophisticated crimes that change and become more complex every day is imperative. The CCIPS is focused on hiring attorneys with computer, engineering or technical backgrounds that enable them to prosecute this type of technically complex criminal cases. Since the internet does not recognize barriers, international cooperation is key in order to have a well-trained personnel around the world. But a question remains without answer, what about the judges? Who is in charge of providing technical legal instruction to the Judiciary Brach. As I mentioned before, the Department of Justice has been very active in the creation of new divisions with the purpose of hiring high tech experts to work close with computer crimes. Among the most recent creation is the National Infrastructure Protection Center[101] created in 1998 that is in charge of the coordination of the FBI's investigation.

It is also important to mentioned the relevancy of the private sector involvement and sometimes lead in an investigation. Private corporations have the power to protect private computer networks by security measures and to give information and cooperate with government agencies to fight against this crime that causes millionaire loses to companies and private individuals. Most of the companies have resources, technical ability, and trained personnel to ensure that they continue to develop and change as the same pace of the Internet.

Another problem that creates obstacles is the fact that while America is having a productive day in some other locations in the world, people are sleeping and not vigilant to cyber crime. This

---

[100] Morris, *supra* note 92 at page 38.

[101] National Infrastructure Protection Center was created in 1998 to coordinate with the FBI the investigation of computer crimes. By September, 2000, it approximately had about 100 investigators, computer scientists and analysts working with computer cases.

impose a difficult situation to United States in the case of countries that do not have a 24/7 days contact agency[102] that in case of an computer break originated at one of those nations during the night could help United States track, investigate and preserve the evidence. United States has taken steps to establish international mutual assistance and fifteen countries have joined the G-8 Subgroup on High Tech Crime to have personnel 24 hours a day, 7 days a week to deal with computer crime.

C. How to Identify the Suspect

In the cyber space it is really difficult to prove that somebody was actually at the computer desk, because a neighbor could be walking over every day while the alleged suspect is at work, or to keep track of a cyber criminal when different ISP's have been used to reach the target. The Internet does not provide a specific mechanism to identify the primary source used, which means that in order to find their path, the investigators need to contact each provider in the chain when the hacker bounced the communication using different ISP's locally or internationally in order to obtain the starting point. In the physical world is more viable to find direct evidence that will lead the officer to the suspect than it is in cyber space. In my interview with a FBI Supervisory Special Agent in Atlanta, he indicated how difficult is to track a suspect that has been using multiple Internet providers before committing the crime. He explained how they conduct the investigation by contacting each provider in the chain in order to track the suspect of the investigation.

Another problem is that a person could reconfigure his/her own e-mail system to use somebody else's e-mail address and impersonate them to send out e-mails making difficult the identification of the actual cyber criminal as discussed below.[103]

---

[102] The CCIPS[102] chairs the G-8 Subgroup on High Tech Crime that has established mutual assistance in computer crime with 15 countries.

[103] The Internet False Identification Prevention Act of 2000 (114 Stat 3075) and 18 U.S.C. §1028 were enacted to strengthen the enforcement of Federal statutes relating to false identification.

II. How to Conduct the Criminal Investigation

Due to the nature of this type of crime was necessary to create new investigative tools to trace the route of the cyber criminals in addition to the traditional criminal investigative tools. Enabling technological tools to find and prosecute cyber criminals. Twenty years ago, a law enforcement agent needed a gun and a notebook to write about the investigation in the physical world. When they suspected or had reasonable suspicion that a criminal action took place or was taking place, they chased the individual or went to the place where the criminal activity was taking place, or looked for an arrest or/and search order. Today, law enforcement agents are fighting new and old types of crime[104], but what makes the distinction is the mechanism or 'modus operandi' used to commit it. Now they use the computer to commit crimes that were considered almost impossible in the past, but with the advances in technology with click of a button the crime is done, or to commit crimes that usually takes place in the physical worlds like steal of information or copyright infringement. For example, before the Internet was invented if a person wanted to steal a company's trade secret, it was necessary to physically infiltrate in the company and actually take into his possession, by either written information or becoming aware of it, the company's trade secret. But today, they can steal a company's trade secret through the manipulation of protected codes or encryption of protective software[105]. Significantly the work for the law enforcement agents has changed and so has the scope of the world. The scope of

---

[104] Law Enforcement and legal commentators are divided on whether cyber crime is an ordinary crime or is a new category of crime. Sinrod, Eric J. and William P. Reilly, *Cyber-Crimes: A Practical Approach to the Application of Federal Computer Crime Laws*, 16 Computer & High Tech. L. J. 177, 179 stated: *"What is cyber-crime? Law enforcement experts and legal commentators are divided. Some experts believe that computer crime is nothing more than ordinary crime committed by the high-tech computers and that current criminal laws on the books should be applied to the various laws broken, such as trespass, larceny, and conspiracy. Others view cyber-crime as a new category of crime requiring a comprehensive new legal framework to address the unique nature of the emerging technologies and the unique set of challenges that traditional crimes do not deal with; such as jurisdiction, international cooperation, intent, and the difficulty of identifying the perpetrator."*

[105] James X. Depsey, *"Communications Privacy",* 8 Alb. L.J. Sci. & Tech 65, 105-107 (1997)(about how the "inherent vulnerabilities" of the Internet has "widespread use of encryption to protect communications and stored data is essential to prevent fraud and other forms of crime in the digital age".)

this new mechanism does not recognize jurisdiction and agents should be more familiarize with it to efficiently fight against. They need to know the world of the enemy before even try to go to combat.

A. Criminal Investigation

1. Electronic Surveillance

Organized crime groups rely on telecommunications to plan and execute criminal activity.[106] One of the most important ways law enforcement agencies acquire evidence to prosecute these criminal organizations is thru lawful electronic surveillance of their communications. Since electronic surveillance evidence provides factual information about the defendant, it is usually not subject to being discredited or impeached during a jury trial, although objections based on the chain of custody might be raised.

Under the necessity for innovative mechanism to investigate cyber crime, law enforcement started to develop a new way of electronic surveillance to be utilized in the Internet, Carnivore. It was given this name because according with the FBI, this programmed computer can rapidly identified the 'meat' and captures it with precision[107]. Due to the absence of new legislation in which to base this new type of surveillance, a stretching of the existing legal framework has taken place to allow law enforcement to have access to communications and stored electronic data. Nonetheless, the absence of a legal framework has produce challenges with the proper balance between the constitutional right to privacy and law enforcement's criminal investigation that I will discuss later in this paper. Among the laws that have been used to support the use of electronic surveillance are the 1968 Title III of the

---

[106] *Id* at pages 104-105 (1997)*("Illegal electronic intrusion into computer networks is a rapidly escalating crime problem. White collar criminals, economic espionage agents, organized crime groups, foreign intelligence agents, and terrorist groups have been identified as "electronic intruders" responsible for penetrations of American computer networks.")*

[107] This topic will be discussed further in this chapter.

Omnibus Crime Control and Safe Streets Act[108], the 1986 Electronic Communications Privacy Act[109] and the 1994 CALEA.[110]

2. Title III, 18 U.S.C. §2510 et seq.

The 'Wiretap Statute' or Title III is govern by 18 U.S.C. §2510 et seq. This statute was a response to the decision in Katz v. United States,[111] 389 U.S. 347 (1967) and Berger v. State of New York, 388 U.S. 41[112]. In Berger the court held that lengthy, continuous or indiscriminate electronic surveillances were not acceptable, but in Katz, the court stated that a short and narrow surveillance was constitutionally acceptable upon showing to a judge the need to do so.[113]

The enactment of this statute had a dual purpose on mind; first, to establish the judicial procedure by which the law enforcement could obtain an authorization order to intercept communication[114], and second, to prohibit the use of interception devices by private citizens[115].

---

[108] Pub. L. No. 90-351, Tit. III, 82 Stat. 212 (18 U.S.C. 2510-22 (1996)).

[109] Pub. L. No. 99-508, 100 Stat. 1848 (18 U.S.C. 2510-21, 2701-10, 3121-26).

[110] Pub. L. No. 103-414, 108 Stat. 4279 (1994) (47 U.S.C. 1001-1010 and scattered sections of 18 U.S.C. and 47 U.S.C.)

[111] In this case the Supreme Court, Mr. Justice Stewart, held that *"government's activities in electronically listening to and recording defendant's words spoken into telephone receiver in public telephone booth violated the privacy upon which defendant justifiably relied while using the telephone booth and thus constituted a 'search and seizure' within Fourth Amendment, and fact that electronic device employed to achieve that end did not happen to penetrate the wall of the booth could have no constitutional significance. The Court further held that the search and seizure, without prior judicial sanction and attendant safeguards, did not comply with constitutional standards, although, accepting account of government's actions as accurate, magistrate could constitutionally have authorized with appropriate safeguards the very limited search and seizure that government asserted in fact took place and although it was apparent that agents had acted with restraint."* See also Camara V. Municipal Court, 387 U.S. 523 (1967) and Terry v. Ohio, 392 U.S. 1 (1968).

[112] *"Statute authorizing any justice of Supreme Court or judge of county court or of court of general sessions of New York county to issue ex parte order for eavesdropping upon oath or affirmation of district attorney or of attorney general or officer above rank of sergeant of any police department that there is reasonable ground to believe that evidence of crime may be thus obtained, containing no requirement for particularity as to what specific crime has been or is being committed or place to be searched or conversations sought as required by Fourth Amendment and requiring no showing of exigent circumstances, is too broad in its sweep, resulting in trespassory intrusion into constitutionally protected area and is violative of Fourth and Fourteenth Amendments. Code Cr.Proc.N.Y. § 813-a; USCA Const Amend 4, 14."* Berger v. State of New York, 388 U.S. 41, 46.

[113] See Robert S. Steere, 33 Val. U.L. Rev. 231, 234-246(1998*) "Keeping "Private E-mail" Private: A Proposal to Modify the Electronic Communications Privacy Act".*

[114] 18 U.S.C. §2516

Congress wanted to regulate the government use of wiretaps and other electronic surveillance devices on communications. The regulations of this statute not only apply to government, but also to private individuals and corporations. Section 2511 states that anybody who willfully[116] intercepts, endeavors to intercept, procures other person to intercept by means of electronic, mechanical or other device to intercept another person's communication will be *"fined not more than $10,000 or imprisoned not more than five years, or both"*[117]. It also states that when a person *"willfully discloses, or endeavors to disclose to any other person"*, or uses, or endeavors to use, *"the contents of any wire or oral communication*[118]*, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication",* that action constitutes a violation of this legislation.[119] This statute also contains in section 2516[120] whose are the persons with the power to request and signed a petition for authorization for interception of wire, oral or electronic communication.[121] Further section 2520 of Title III provides to any person *"whose wire, oral or electronic communication is intercepted, disclosed, or intentionally used"*[122], the right to sue for any of the violation of §2511 in order to recover civil damages.[123] According with Thomas R.

---

[115] 18 U.S.C. §2511

[116] Public Law 99-508 §101(f)(1) substituted "intentionally" for "willfully".

[117] *Id* at §101(d)(1) substituted "shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5)" for "shall be fined not more than $10,000 or imprisoned not more than five years, or both".

[118] *Id* at §101(c)(1)(A), substituted *"wire, oral, or electronic communication"* for *"wire or oral communication"*.

[119] 18 U.S.C. §2510 contains definitions applicable to this statute. It defined for example, "wire communication" as *"any communication made in whole or in part through the use of [common carrier] facilities for the [interstate or foreign] transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception."* Also defines "oral communication" as *"any oral communication uttered by a person exhibiting an expectation [of privacy]." "Interception" is defined as an "aural acquisition of the contents of any wire or oral communication through the use of any electronic, mechanical, or other device."*

[120] 18 U.S.C. §2516

[121] See Marjorie A. Shields, J.D, *"Who may apply or authorize application for order to intercept wire or oral communications under Title III of Omnibus Crime Control and Safe Streets Act of 1968 (18 U.S.C.A. §2510 ET SEQ.)"* 169 A.L.R. Fed. 169 (2001)(discusses in detail who can apply or authorize for an order to intercept wire or oral communication under 18 U.S.C. §2510 et seq.)

[122] 18 U.S.C. §2520

[123] William G. Phelps, *"Construction and Application of 18 U.S.C.A. § 2511(1) and (B), Providing Criminal Penalty for Intercepting,*

Greenberg[124] the federal courts in an effort to define the language of this section, have came to different opinions.[125]

3. Electronic Communication Protection Act[126]

New methods of communications emerged by 1986, forcing Congress to study these new technological changes by appointing the Office of Technology Assessment to review this matter. The Office of Technology Assessment reported about how the latest technological developments in communication have made Title III obsolete[127] and therefore new legislation coping with these new challenges was necessary to regulate the electronic surveillance more efficiently. As a result, the Electronic Communications Privacy Act (hereinafter ECPA) was enacted to clarify how existing wiretap laws apply to cyberspace and other computer and technological developments that fell out of the scope of prior laws, and at the same time set the boundaries on how much the government can invade our on-line privacy. It was necessary to redefine the boundaries between privacy and the law enforcement. ECPA made it a crime to knowingly intercept wireless communications and e-mail.[128]

One of the most important changes is the addition of "electronic communication" to section 2510 and it broadly definition to includes any communication not included in Title III, as the Internet. This term was inserted throughout the statute to substitute wire and oral communication for wire, oral,

---

Endeavoring to Intercept, or Procuring Another to Intercept Wire, or Oral, or Electronic Communication", 122 A.L.R. Fed. 597 (1994).

[124] Thomas R. Greenberg, *"E-mail and Voice Mail: Employee Privacy and the Federal Wiretap Statute"*, 44 Am. U. L. Rev. 219 (1994).

[125] See United v. Christman, 375 F. Supp. 1354 (N.D. Cal. 1974) (controversy includes whether Title III's protection applied to communications transmitted via a private phone system).

[126] Pub. L. No. 99-508, 100 Stat. 1848

[127] Greenberg, *supra.* Title III was considered obsolete because most of the new methods of communication were not under the definition "aurally acquired.

[128] See Robert S. Steere, *Keeping "Private E-mail" Private: A Proposal to Modify the Electronic Communications Privacy Act,* 33 Val. U.L. Rev. 231, 249(1998).

and electronic communication. To cope this amendment with the content of the following provisions, Congress expanded the scope of intercepting devices to include those able to intercept electronic communications. ECPA also amended the meaning of "intercept" in order to extent the aural acquisition of a wire or oral communication to any non-voice electronic or wire communication, such as a communication through the Internet. Further, Congress expanded ECPA by adding a new title, §2701 to protect any "stored communication" and added the concept of "electronic storage". This section states that any person who *"intentionally accesses without authorization… or exceeds an authorization to access a facility through which an electronic communication is provided and it is in electronic storage"* may be subject to both fines and imprisonment as provided in s 2701(b).[129] In sum, ECPA amendments' purpose can be divided in three major concerns: first that the interceptions be conducted with none or just a minimum of interference with the services of the person whose communications are being intercepted and secondly, that the interception does not access more than is authorized. And lastly, to give law enforcement the authority to use electronic surveillance with new telecommunications technologies and services such as electronic mail, cellular telephones, and paging devices.

4. CALEA

As result of the fast moving technological advances, Congress amended title 18 of the United States Code by enacting the Communications Assistance for Law Enforcement Act[130] in October 25, 1994. With this amendment all telecommunication carrier have the duty to cooperate with the law enforcement in the interception of communications or for other purposes. CALEA impose the duty of telecommunications carriers to provide to the law enforcement with adequate equipment and

---

[129] Greenberg, *supra* note 124 at page 46.

[130] PL 103-414 (HR 4922), 108 Stat. 4279, October 25, 1994.

facilities that enable them to perform lawfully-authorized electronic surveillance. This law also assigned some responsibilities to the Attorney General of the United States as follows:

> *"* Consulting with industry associations, standard-setting organizations, representatives of users, and state utility commissions to facilitate implementation of the assistance capability requirements;*
>
> ** Providing telecommunications carriers, telecommunications industry associations, and standard-setting organizations with an estimate of the number of interceptions, pen registers, and trap and trace devices that government agencies may conduct;*
>
> ** Establishing regulations to facilitate timely and cost-efficient reimbursement to telecommunications carriers as authorized under CALEA;*
>
> ** Allocating funds appropriated for reimbursement in a manner consistent with law enforcement priorities; and*
>
> ** Reporting to Congress, annually, the total amount of payments made to telecommunications carriers during the preceding year, and the projected expenditures for the current year."*[131]

Section 102 defines all the basic terms of this statute such as, "call-identifying information", "electronic messaging services", and "telecommunications carrier". According with CALEA Implementation Section (hereinafter CIS), section 103 has four "assistance capability requirements that can be summarize in the telecommunications carrier duty to ensure "that they are capable of expeditiously isolating and enabling the government to access pursuant to appropriate legal authorization" to all interception of communications content, access to call-identifying information[132], delivery of communications content and call identifying information, and protection of privacy and security of communications.

---

131 CALEA Implementation Section (CIS) was established in 1995 in response to the delegation of implementation responsibilities to the Federal Bureau of Investigation (FBI) by the Attorney General

132 Section 102 of CALEA defines call-identifying information as *". . . dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber by means of any equipment, facility, or service of a telecommunications carrier."*

In addition Section 105 of CALEA takes care of the security and integrity by requiring that a *"telecommunications carrier shall ensure that any interception of communications or access to call-identifying information effected within its switching premises can be activated only in accordance with a court order or other lawful authorization and with the affirmative intervention of an individual officer or employee of the carrier acting in accordance with regulations prescribed by the Commission".*[133] Further, section 108 established the grounds, time and limitations for the issuance of an order of electronic surveillance under this statute. It states that a *"court shall issue an order enforcing this title…only if the court finds that: (1) alternative technologies or capabilities or the facilities of another carrier are not reasonably available to law enforcement for implementing the interception of communications or access to call-identifying information; and (2) compliance with the requirements of this title is reasonably achievable through the application of available technology to the equipment, facility, or service at issue or would have been reasonably achievable if timely action had been taken."*[134] It also specifies that the court should state the time and conditions for the compliance of the order. In sum, it requires telephone carriers, including ISP's, to help with investigations and the court order usually comes in two parts, one authorizing the FBI to sniff, and the other obligating the ISP to help out

B. Carnivore

The FBI has long learned during criminal investigations about how crime organizations have been using the internet to communicate with each other and their victims. Since ISPs lack the ability to discriminate between communications related to criminal activity and those that are not, the FBI developed a diagnostic tool called *C a r n i v o r e* to help determine and distinguish criminal activity and to track the source of that criminal activity, which is operated under the permission or application of the above mentioned statutes. The FBI alleges that Carnivore has the ability to intercept and collect

---

133 47 U.S.C. A.§1005

134 47 U.S.C.A. §1008

communications that can be lawfully intercepted and to limit the information obtained to what the court has specially ordered.

1. What is Carnivore?

According to the FBI, Carnivore is a computer system created as a tool to investigate cyber crime. The FBI uses Carnivore in cooperation with ISP to collect information from a specific user suspect targeted in an investigation. The FBI assures that: "*Carnivore chews all the data on the network, but it only actually eats the information authorized by a court order*".[135]

This computer consists of a Pentium III Windows NT/2000 system with 128 megabytes of RAM; a commercial communications software application; a custom C++ application that works in conjunction with commercial program above to provide the packet sniffing and filtering; a type of physical lockout system that requires a special pass code to access the computer; a network isolation device that makes the carnivore system invisible to anything else on the network; a 2 gigabyte Iomega Jaz drive for storing the captures data.

2. How to obtain an authorization to use Carnivore?[136]

Applications for electronic surveillance and interceptions, as Carnivore, that target a full content wiretap, must be without capturing the content of the communication. The order for a full content wiretap can only be obtained if the law enforcement has demonstrated probable cause, stated the offense being committed, the telecommunications filed before a federal district judge. In contrast, a lower court can authorized a trap and trace wiretap that allow the law enforcement to obtain limited

---

[135] Carnivore FAQ, Version 0.1, September 7, 2000 by Robert Graham. (http:// www.robertgraham.com /pubs /carnivore-faq.html).

[136] See Marjorie A. Shields, *Who may apply or authorize application for order to intercept wire or oral communications under Title III OF Omnibus Crime Control and Safe Streets Act of 1968,* 169 A.L.R. Fed. 169 (18 U.S.C.A. § § 2510 ET SEQ.)

information such as e-mail headers, list of all servers, or to track everyone who accesses a specific web page, but facility for which the subject's communications are to be intercepted, the type of conversation to be intercepted and the identities of the individuals committing the offenses. In specific it is necessary to give details of who is the suspect (e-mail address), what lines will be tapped, and what kind of information is being seized. In addition, the application must indicate that other forms of investigation will not work or are too dangerous to pursue. If accepted, the order for surveillance is limited to 30 days, and may be ended sooner if the subjects are detained or extended for up to 60 days, if justified. The law enforcement is required to provide periodic reports to the Court. Once the petition is accepted, the order needs to specify, who is the suspect, the account information, the type of crime he or she is suspected of and what will be tapped. According with the FBI, the issuance of this order is held to a higher standard[137] and only can be contained from a Federal District Judge or Higher in the case of a full content wire tap. This controversy was addressed in United States Telecom Association v. Federal Communications Commission,[138] 2000 WL 1059852 (D.C.Cir.). In this case, the Court of Appeals stated its concerns about extending the scope of the Pen Register Statutes to "digits" that convey "content". This decision indicated that the government needs to show a higher standard to have access to an e-mail address under the Pen Register Statutes.[139] Carnivore is only used when the ISP cannot satisfy the search warrant by their own means.[140]

---

[137] Some controversy exists with regard to this "high standard". Some legal commentators believe that the standard use under the Pen Register Statutes to authorize the access to information is too low to be approved in the access of e-mail addresses. They came to that conclusion because the standard of "reasonable indicia" established by the Guidelines in order to initiate an FBI investigation is higher than that established by the pen register statutes that is limited to the relevancy to "an ongoing investigation". This controversy was addressed recently in

[138] See United States Telecom Association v. Federal Communications Commission, *2000 WL 1059852* (D.C.Cir.).

[139] Paul Taylor, *Issues Raised by the Application of the Pen Register Statutes to Authorize Government Collection of Information on Packet-Switched Networks*, 6 Va.J.L. & Tech 4 (2000)

[140] See Testimony of Dr. Donald Kerr, Hearing of House Subcommittee on the Constitution on Fourth Amendment Issues Raised by the FBI's Carnivore Program (July 24, 2000) provided to Congress by Dr. Donald Kerr. (about the increasing use

3. How Carnivore works?

After the issuance of the court order, the FBI configures Carnivore's software with the IP address of the suspect to capture all packets from the suspect particular location for a full content-wiretap or a trap and trace wiretap of e-mails. A content-wiretap will cover all information in the e-mail while a trace wiretap only saves the e-mail addresses. This has brought some controversy because some analysts say that a trace wiretap or pen register cannot exist in the Internet due to the way the e-mails are constructed. I will discuss this issue later in this paper in the Constitutional Issues section. This software works as a packet sniffer that spy on packets contained in the internet traffic while they are traveling to their destination and makes a copy of the suspicious ones. All Internet traffic is fragmented into packets, so it could be possible that it could miss packets, or collect unrelated packets as being part of an e-mail message. However, according with Robert Graham in his website, "Carnivore can detect these problems and clearly mark them" he says that *"rather than capturing the e-mail message itself, it instead captures the raw packets that transported the e-mail. These packets have 'check sums' and 'sequence numbers' to guard against corruption. Therefore if Carnivore misses a packet that was in the middle of an e-mail message, this hole is clearly marked within the packet."*[141] Nonetheless, this can create problems with the 'best evidence rule' at the time of the admission into evidence of these packets.

Carnivore copies all of the packets without impeding the flow of the network traffic, or altering, stopping or modifying the original e-mail and its route. Carnivore makes copies of all e-mails targeted in the investigation and the original just continue its final destination. The copies go through a process of filtration to only keep the e-mail packets targeted and save them into the Jaz cartridge.

---

of Carnivore, "indicates that Carnivore has been used by the federal government at least 16 times in 2000, including instances in which it has been applied pursuant solely to authority under the Pen Register Statutes).

[141] 17 U.S.C. §102(a).

The information saved is kept in the ISP and is collected everyday or two by an FBI agent and swaps out the Jaz cartridge. In order to secure and preserve the evidence and establish the chain of custody, the agent takes the retrieved cartridge and puts it in a container that is dated and sealed as any other evidence that can be altered or contaminated in a criminal case. The captured data is later processed using two software called Packeteer and Coolminer.

The FBI assures that Carnivore system is very well monitored and there are significant penalties for misuse. However, that is not the way private citizens and the media perceive the use of Carnivore. Here is an example of a publication in the Atlanta Journal Constitution:

> "*Carnivore" is a laptop computer with highly sophisticated software that is connected to the mail servers at an Internet service provider such as CompuServe. Once connected it looks to all e-mail, incoming and outgoing, searching for messages involving the target of probe. This is not at all the way a tap on a telephone works. In that case, law enforcement sees only the calls of the person who is under surveillance; in the e-mail case, it sees everything sent or received by everyone."*
> *"Net is different technologically from old media such as telephones and mail, some argue, they need new rules, laws and techniques to find the bad guys and track what they are doing".*[142]

This and other constitutional issues will be discussed in Chapter 4 of this paper.

It is the FBI opinion that electronic surveillance has been very effective in securing the conviction of thousand of criminals in the past through it use with telephone and other devices, and with all possibilities will be an excellent tool in the criminal investigation of computer crimes.

4. Legislation that authorize the use of Carnivore

Carnivore has been operated mostly under the authority given to the law enforcement under the Pen register, trap and trace and full content statutes above mentioned. However, those statues were enacted having other type of technology in mind and to address some other issues that were

---

[142] "Who's peeking at your e-mail? The Atlanta Journal-Constitution. Sunday, July 23, 2000. John Walter, Managing Editor; Cynthia Tucker, Page editor; Jim Wooten, Page Editor; Ron Martin, Editor.). Related web-sites: www.whithouse.gov, www.epic.org/privacy/wiretap, www.aclu.org/news/2000, www.whitehouse.gov/judiciary.

completely different in scope to those presented today with the World Wide Web. Most of these statutes protecting privacy were enacted in times when the telephone was the dominant mean to intrude privacy and therefore, those statutes are not broad enough to include the new digital communication, such as e-mail and other forms of digital communication and to extent protection against violations to privacy or to deter their use. Among other statutes there is also the 1986 Computer Fraud and Abuse Act, which makes breaking into federal computers and trafficking in stolen passwords felonies and the 1998 roving wiretaps that allows the FBI to tap lots of people's communication as long as it only keeps records of the suspect's communications.

C. Search and Seizure

Another tool to investigate the criminal activity could be through search and seizure of computer hardware, software, or connected devices like DVD's, CD's or diskettes. This procedure requires forensic investigative knowledge and training because is legally and technically complex. If this procedure is not carried out correctly, it can cause several problems like the risk for the government and its agents to be sue, either by individuals or by companies in the case of losses as result of the investigation. A mishandled search or seizure can cause significant problems for officer and agencies like for example: risk exposure to civil liability if a search or seizure of networked devices is alleged to have contributed to a company's financial loss. In addition, if the law enforcement does not follow the guidelines to search and seize computers, computers hardware or software or any other connected devices as zips, the evidence collected might be considered a fruit of the poisonous forbidden tree or the result of an illegal search and therefore, not able to present that evidence at trial.

The Fourth Amendment of the United States Constitution states that *"the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place*

to be searched, and the persons or things to be seized". This protection extends to each and every citizen while performing legally accepted actions. Once a citizen trespass that border, the law enforcement after presenting proof of their reasonable suspicion of illegal activity, can search persons, properties or houses. Today, the search has change from a physical search to a search that does not need to trespass walls or doors, it could simply be done in cyberspace.[143]

The Internet has been used to contraband illegal copies of copyrighted software, to steal trade secrets from companies, and the computer hard drive, diskettes or compact disks can be a crucial witness of those crimes providing important pieces of evidence to the law enforcement. Law enforcement agencies examination of those drives and removable artifacts is imperative in their search for evidence that may yield to important insights. The legal standard use to allow and order search and seizure of computer equipment is whether the police have reasonable suspicion to think that the computer was used to commit a crime and a search and seizure will provide them with evidence. An informant or agent can only save the content of an electronic communication in which he/she is active participant. However, when the law enforcement agent is observing a chat room in the Internet, the Fourth Amendment protection does not apply because the individuals participating in the chat have waived their privacy expectation when entered in the discussion.[144] It is also important to remember that the Fourth Amendment does not apply to private action, therefore the evidence collected or found by private individuals who are not working as agent of the government, is admissible in evidence.

---

[143] Paul Taylor in his article, *"Issues Raised by the Application of the Pen Register Statutes to Authorize Government Collection of Information on Packet-Switched Networks", 6 Va. J.L. & Tech. 4,* says *"Seventy years ago, Justice Brandeis, in his dissenting opinion in Olmstead v. United States predicted that ongoing technological developments would someday enable law enforcement to search people or their property without physical trespass. He also cautioned that courts should be alert to these changes in technology in determining the contours of privacy rights".* See also 277 U.S. 438, 474 (1928).

1.How specific the court order needs to be to be valid?

One of the most important reasons to allow the seize of a computer at the suspect's house is when they suspect the computer has been used in the commission of the crime and evidence could be hidden in said computer and could be lost or difficult to identify if the order for a seizure is not granted. Seizing the computer would give the law enforcement relevant and pertinent evidence that otherwise could be lost if the computer is not seized.

In United States v. Torch, 609 F. 2d 1088, the court approached this matter and held that *"unlike with murder weapons or drugs, when an offense concerns the use of hard copy or electronic files and documents a court cannot be sure which files will be relevant and the warrant may not be able to state as specifically what should be searched and seized. Therefore, courts have required less particularity in the warrant".*[145]

In terms of diskettes, CD's or DVD's the court have been threatening them under the 'containers doctrine'. Also in contrast with a physical search that gives the law enforcement the right to go to the particular place to be search and seize the evidence just one time and for a limited time, the electronic surveillance can continue for days looking for evidence. This type of search does not announce to the suspect the law enforcement presence as it is done by the physical or traditional search, because electronic surveillance operation is done secretly.

D. Evidence Issues

Will that information gathered be hearsay and therefore not admissible in Court? The evidence gathered by Carnivore or the IPS is hearsay and therefore not admissible in Court.

---

[144] See States v. Charbonneau, 979 F. Supp. 1177 (S.D. Ohio 1997), in which the court held that not to suppress the statements made in the chat rooms because the defendant could not have had a reasonable expectation of privacy in the chat room.

[145] United States v. Torch, 609 F. 2d 1088, 1090 (4th Cir. 1979)). See also United States v. Sassani, 1998 WL 89875 (4th Cir. Mar. 4, 1998) (per curiam) (unpublished decision), cert. denied, 119 S. Ct. 276 (1998)

Nonetheless, the Rules of Evidence allow this evidence to be admissible if, in this case the FBI can prove the evidence is accurate, reliable and trustworthy. FBI will have to present all evidence captured while Carnivore was running without consideration to non favorable evidence. The Court will also require the FBI to authenticate the evidence according with Rule 901 of the Federal Rules of Evidence. And finally, the evidence must meet the criteria for 'the best evidence rule'.

CHAPTER 4

CONSTITUTIONAL CONTROVERSIES

The legal system has been unable to keep proper and updated legislation for cyber crimes, because of the dynamic changes in technology, causing frustration to law enforcement and the prosecutors of these crimes. At the same time, lawmakers need to take into consideration the importance of keeping a balance between the government interest in prosecuting and punishing crimes, and the individual constitutional rights, such as privacy and free speech. There is also concern for the protection of the integrity of companies and the public in general.

Further complicating cyber-crime enforcement is the area of legal jurisdiction. This problem poses significant restrictions in what a country can do, because even though a country like the United States, can implement a comprehensive group of laws, those laws cannot address the computer crime problems outside its jurisdiction. Therefore, international cooperation is absolutely necessary to successfully address this problem. Even though some countries are taking action in organizing their law enforcement as well as cooperating with the United States, there are other countries that have not yet realize the necessity to legislate against this type of crime.

I. Jurisdictional Problems

Janet Reno, at the International Symposium on Intellectual Property held on September 12, 2000, gave a speech to government officials from 30 different countries and stated: *"One of our biggest challenges has been to implement an effective matrix of bilateral mutual legal assistance and extradition treaties. The*

transactional character of the crimes and the perpetrators poses special challenges and makes international cooperation critical to reduce the threat." Even though the Internet is world wide and does not recognize frontiers, United States must respect others countries boundaries and be abide by their internet regulations. This leaves America with the imperative necessity for cooperation in the investigation and prosecution of these crimes. Further, she said it is necessary that intellectual property crimes be extraditable offenses, otherwise, foreign countries should be prepared to conduct effective domestic prosecutions in lieu of extradition. When multinational enforcement efforts form a network to prosecute these crimes, intellectual property criminals will learn that there is no safe place to hide, she commented. She also mentioned that anonymous criminals find a haven in infringing intellectual property via Internet where the profits are sure and the possibility of getting caught is low or nonexistent.

II. Constitutional Concerns

A. Right to Privacy, Right to Freedom of Speech and Due Process of Law

There are three major concerns on how carnivore works. It is not clear whether carnivore could be misused to intrude private sectors in contravention with the Fourth and Fourteen Amendment. Second, whether the application of the pen register, trap and trace, and full content wire tap statutes should be applied to authorize the use of Carnivore, even though those statutes were enacted without contemplating this new technology. Lastly, there exists concern for the legality of the search and seizure of computers. *"There is a real danger that the cops will step over the line of legal surveillance of criminals and adopt methods that put everyone's communications under inspection". "This is not at all the way a tap on*

a telephone works. In that case, law enforcement sees only the calls of the person who is under surveillance; in the e-mail case, it sees everything sent and received by everyone".[146] (Atlanta Journal-Constitutional)

1. Fourth Amendment

"Carnivore" has raised unexpected problems in relation to the Constitutional Rights to Privacy and Freedom of Speech. The Fourth Amendment states that:

> *"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and a particularly describing the place to be searched, and the persons or things to be seized."*

This system is the equivalent to the controversial old method of surveillance and interception of mail and telephone used by law enforcement such as the FBI, but with a greater capacity. It is reasonable to expect that for this new technological type of crime, innovative procedures must be developed in order to track the cyber criminals and bring them to justice. Nevertheless, they must outweigh between the constitutional rights and the measures they take to combat cyber crimes. One of the problems this electronic surveillance has brought is the application of the same statutes that regulate the use of the old electronic surveillance that caused so much controversy in the past and were created with other type of communication in mind. James X. Dempsey in his article *"Communications privacy in the digital age: Revitalizing the federal wiretap laws to enhance privacy"*[147] says that not only opponents but also proponents of the electronic surveillance have recognized that the legal framework for wiretap is completely unsatisfactory and creates confusion that should be address promptly by Congress.[148]

---

[146] Taylor, *supra* note 143 at page 55.

[147] Dempsey, *supra* at note 105 page 42

[148] *Id a*t page 67.

The Electronic Frontier Foundation (a non profit organization dedicated to give support to the individual's rights) submitted its comments about the Fourth Amendment and other issues related to Carnivore to the United States House of Representatives on July 28, 2000.[149] It presented comments about the analogy between the use of pen registers in the telephone system and its use on the internet and the effect it could have on if it is used improperly by the FBI. The EFF offered its vision through Ms. Deborah S. Pierce, one of the Staff Attorneys at EFF. EFF argues that *"the use of packet analyzers on the Internet captures much more information from an individual than does the use of pen registers and trap and trace devices used on traditional land-line telephone systems"*[150]. A pen register is a device the FBI can use to intercept a particular telephone line after obtaining an order from a court of justice to record every telephone number is dialed. 'Trap and Trace' is a similar device with the difference that it records the caller id of everyone who called to the targeted phone instead of the dialed numbers. According to the EFF, pen registers or trace devices, which have been used to gather information like telephone numbers and the origin of the call, are strictly limited to obtain information targeted in an investigation. However, EFF says that pen registers, as the ones defined to be used in the telephone wiretap, does not exist in the Internet due to the form in which the information is displayed in an e-mail. In the Internet, the sender/receiver and the textual message are not displayed separately and that format gives law enforcement ample potential to collect information out of the scope of the court order. In the case of the telephone wiretap, a separation between the routing information and the call content exists, while in internet e-mails the message is divided into small packets that contain routing information and content information allowing the FBI to collect more information than permitted.

---

[149] EFF Statement of the Electronic Frontier Foundation before the Subcommittee on the Judiciary United States House of Representatives about the Fourth Amendment and Carnivore on July 28, 2000. EFF is a nonprofit organization founded in 1990 and it encourages and challenges industry and government to support free expression, privacy and openness in the information society.

[150]

After a careful study of Carnivore, EFF found it is a system that gathers pen register and trap and trace-like information by sniffing each packet as it goes along its final destination. Once the packets are gathered, it filters out "unwanted e-mail" from the information that has been targeted. EFF states that this process is controversial because in the case of traditional wire taps, pen registers and trap and trace devices, "they are attached to specific phone lines" and law enforcement is just able to collect the telephone numbers of the target, rather than having access to "all of the traffic going through a particular Internet Service Provider's network" and such process goes beyond the scope of the wiretap laws. It also found that the analogy between pen register information from a traditional land-line phone system to the Internet is incorrect, due to the fact that Carnivore can gather content as well as numbers. EFF stated that it is possible that with Carnivore in place the FBI can have access to more than e-mail addresses, in particular, in the subject line of the e-mail where the individual can summarize the content of the e-mail and therefore revealing its content.[151] EFF says that pen register statutes were enacted taking in consideration a 'physical connection' of the telephone, which uses circuit-switched networks[152], rather than the configuration of the Internet that uses "packet switched network"[153]. As a result this system combines call routing information with the content in the packets. For that reason, EFF believes that the use of pen registers or trap and trace devices in the Internet

---

[151] Taylor, supra note 143 at page 55, says that *"when the Supreme Court held that the retrieval of telephone numbers pursuant to a pen register request was not an "interception" of content - and that such numbers could therefore be obtained with the minimal showing of evidence required by the Pen Register Statutes - it made clear that "pen registers do not 'intercept' because they do not acquire the 'contents' of communications . . . They disclose only the telephone numbers that have been dialed a means of establishing communication. Neither the purport of any communication between the caller and the recipient of the call, their identities, nor whether the call was even completed is disclosed by pen registers." Because an e-mail address, unlike a phone number, may contain not only letters but also a person's name, such as "john.smith@home.com," and other descriptive elements that could be considered "content," such as "wild-and-crazyjohn.smith@home.com," e-mail addresses may not only be outside the clear terms of the Pen Register Statutes, but the low standard under which the government may be authorized to access information under the Pen Register Statutes may be too low to constitutionally authorize its access to e-mail addresses."*

[152] In the physical connection of a telephone call, once the connection is made the network will be dedicated to that sole connection.

[153] Packet-switched network means that the information sent is broken into small packets and sent through different routes at the same time, and finally, assembled together when it reach the receiver.

raises privacy concerns that were not present at the time the Supreme Court reached it decision about this matter, since those devices in the internet can reveal more private information than telephone numbers.[154] Pen registers do not tap the content of the communication, identities or other descriptive elements, but just routing information from calls received and dialed from a particular telephone line. Therefore, carnivore is out of the scope of the pen register laws.

In an effort to resolve this controversy, the FCC requested a report from the Telecommunications Industry Association that would address this issue and gave them until September 30, 2000 to deliver it. The Telecommunications Industry Association selected a group of experts to present their results of their Joint Expert Meetings on September 29, 2000. The JEM concentrated their report in the technical issues confronted with the packet-switched networks and the use of Carnivore. Their letter states that they are unable to conclude about the technical impact of the information available to law enforcement because a legal framework does not exist to be used as a guidance to know, for example what constitutes "call-identifying information" for packet data.[155] JEM reported that Carnivore *"…has not been proven effective, as yet, in cases where the subject's communications are part of a high bandwidth transmission"*. The JEM concluded that *"there is no reliable method for determining the Pen Register and Trap and Trace information when monitoring a packet stream."*[156]

Further, Carnivore can keep track of the URLs of web sites visited for purposes of obtaining routing information, but is can also give law enforcement content by knowing what is the web site

---

[154] It can also record content of a second party that is not suspect of any crime and in violation of his constitutional protection. *"Thus, if one person is under investigation, and that person sends an e-mail to a second person, law enforcement is likely to put a "cover" on all of the e-mail addresses going in and out of the second person's computer, even if such person is not involved in criminal activity, as the second person's communications would be "relevant" to the investigation insofar as law enforcement would like to know whether the second person is corresponding with other persons under investigation."* Paul Taylor, 6 Va. L.J. & Tech. 4, 6.

[155] See the Report to the Federal Communications Commission on Surveillance of Packet-Mode Technologies, Joint Experts, Committee TR 45, Telecommunications Industry Association (September 29, 2000) ("JEM Report").

[156] *Id* at 12, 13 and 16.

about. [157] Also, legal commentators have expressed their opinion about the privacy expectations while people make their connection to the World Wide Web, because they are using passwords to gain access to their e-mail boxes. Courts have held that in order to access an e-mail account it is necessary to use a password and that indicates the user's objective and expectation of privacy in the e-mail communication transmitted.[158]

As result of the multiple problems and controversies confronted, on July 31, 2000 President Clinton submitted a proposal called "Enhancement of Privacy and Public Safety in Cyberspace Act" to the Congress with some amendments to the federal electronic surveillance laws, which included a new broader definition for pen registers. The proposal will change the wording of the definition from *"a device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line"* to *"a device or process which records or decodes dialing routing, addressing, and signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted"*. Immediately after this announcement, legal commentators raised their voice to say that this amendment constitutes a broad definition and a deviation from the original legislative intent to limit the type of content recorded by these devices. Most of them are of the opinion that the phrase *"dialing, routing, addressing or signaling information"* is too broad and could expand the scope of information sought, making electronic devices more intrusive to legitimate businesses and individuals. The substitution of a term to adapt these statutes to the electronic communication has made the scope of those go beyond the limits established by the courts for the electronic surveillance.[159] Among the scope of that phrase a question is raised, whether this would include lines in the 'routing information' that include any content. Also

---

[157] *Supra* note 6 at page 11. Taylor, *supra* note 143 at page 55.

[158] See United States v. Maxwell, 42 M.J. 568, 576 (1995). See also Note, *Keeping Secrets in Cyberspace: Establishing Fourth Amendment Protection for Internet Communication*, *110 HARV. L. REV. 1591, 1603 (1997)* ("Cyberspace communication should be protected with a password to establish a reasonable expectation of privacy.").

[159] *Supra* note 6 at page 12.

the definition of addressing information could be constructed in a way that includes descriptive information from websites, like for example www.cybercrime.com, giving them with the exact information that the individual was researching. There are a number of cases in which the courts have held that devices to intercept pagers cannot be considered pen registers because a pager is capable of receiving not only numbers but combination of numbers used to transmit coded messages.[160]

Notwithstanding, FBI alleges that these devices can be set up to gather only the e-mail addresses and not any other content of the message, unless the court has authorized a full content wire-tap in which case Carnivore can save all the information contained in the e-mail target of the investigation. Robert Graham[161] wrote some answers to frequently asked questions over the Internet and he says that contrary to what EFF thinks, Carnivore is a protocol decoder that Carnivore "*follows the e-mail transfer protocols and only examines specific fields"*. Carnivore does not work as the regular search people can do over the Internet which is done by pattern matcher. Robert Graham says that when an e-mail is sent, it starts when the sender first send an envelope containing information about the sender and the receiver which is called 'SMTP', and then the message is sent. In response to the preoccupation about the tracking of more information than the 'SMTP', Mr. Graham says that if the court order specifies only the SMTP as the information to be gathered, Carnivore is set up to stop at the first blank line just right before the content is going to start. In this case Carnivore will be able to collect information about the subject of the communication and that has been considered content by the courts. Carnivore must have to remove that information in order to obey the court order

Another controversy exists with interception of information from other people not subjected to the investigation. Even though probable cause is necessary to request an order from the court, it is

---

[160] See Brown v. Waddell, 50 F.3d 285, 294 (4th Cir. 1995).

[161] *Supra*, note4 at page 3.

uncertain if Carnivore could capture data from innocent people, because they refused to disclose how carnivore works.

In sum, there are three general concerns: one is that the FBI's temporary use of Carnivore could interfere with the proper use of the ISP's network; second, whether Carnivore can capture more information that allowed by the court order and can transmit or alter data; and third, it can be misuse to invade privacy.

As a result of multiple critics to the use of Carnivore by individuals, corporations and the media, the IIT Research Institute and the Illinois Institute of Technology Chicago-Kent College of Law were hired by the Department of Justice to evaluate Carnivore. In the evaluation, ITT was asked to find whether Carnivore provides investigators with only the information that is allow by the court order or not; if it introduces material risks of operation or security impairment of an ISP; the risks of unauthorized acquisition of information, whether intentional or unintentional; if it provides protections commensurate with the level of the risks; as well as the corporations and private citizens concerns.[162] IITRI did not consider in its review of the Carnivore system any of the constitutional issues.

This evaluation was divided in four threads to facilitate the review: the process used to translate court orders into commands for Carnivore, implement the collection, and verify that only permitted information was gathered; the system architecture especially with respect to security; examined the Carnivore source code to determine what functions have been implemented and what limitations have been built in; and determine the system capabilities by installing it in the IITRI Information Technology Laboratory.

---

[162] Draft Report: Independent Technical Review of the Carnivore System, page 1,8.

Regarding the first thread, IITRI concluded that "when Carnivore is used *correctly* under a Title III order, it provides investigators with no more information than is permitted by a given court order. Nevertheless, it can be more effective in protecting privacy and enabling surveillance than can alternatives. Secondly, it concluded that the operation of Carnivore does not constitute any operational or security risks to the ISP network. In relation to the third thread, IITRI found that exist the risk of intentional and unintentional unauthorized used of Carnivore by the FBI personnel to obtain information not allow in the court order. Lastly, it concluded that Carnivore does not offer protection commensurate with the levels of the risks.

The IITRI found that contrary to what EFF thought, Carnivore can be used to gather content of communications ("broad swept") under Title 18 U.S.C.§2510-2522 and 50 U.S.C. §1801-1829 or only address information (pen register) under 18 U.S.C.§3121-3127 and 50 U.S.C. §1841-1846. In addition, IITRI reported that like in any other surveillance, Carnivore is operated under strict separation of responsibility between the case agents and the technically trained agents. The case agents investigate and gather the necessary evidence to proved probable cause to order the surveillance of the electronic communication, while the technically trained agents will be responsible for the installation and configuration of the system according with the court order to assure the evidence admissibility in court. Once Carnivore has been placed in the ISP, the collection of information is subject to filter settings made by the control computer operator, who is the responsible for set up and change filter setting, start and stop collection, and retrieve collected data. IITRI concluded that *"while the system was designed to, and can, perform fine-tuned searches, it is also capable of broad sweeps. Incorrectly configured, Carnivore can record any traffic it monitors".*

Among the deficiencies, IITRI reported one in the integrity of the information collected created by five factors: the difficulty to establish the process of setting up the filters, collecting data settings, and the rest of the investigation, the lack of access control constitutes a compromise of the

collection computer, the process to view, analyze and minimize raw output contain several material flaws, Carnivore does not consistently recover from power failures, and there is no synchronization within Carnivore.

ITT also concluded that Carnivore cannot: *"Alter or remove packets from the network or introduce new packets, block any traffic on the network, remove images, terms, etc. from communications, seize control of any portion of Internet traffic, shut down or shut off the communications of any person, web site, company or ISP".* It does not seems clear how Carnivore can be able to delete or erase the subject filed of an e-mail, but according to the FBI and the ITT is not able to alter or remove packets.

Another constitutional issue is regarding the charging both copyright and trademark violations arising from the same act or acts. In United States v. Dixon, 509 US 688 the court in its decision said that that does not violate the double jeopardy clause of the Fifth Amendment of the constitution because each offense contains an element not contained in the other.

CHAPTER 5

CONCLUSION

Congress and the Department of Justice's attention and action in the last decade, has certainly help in the enforcement and prosecution of cyber crime against intellectual property. Congress has been working hard creating laws to provide protection to the intellectual property owners and fight these new crimes for the last 11 years. The DOJ did not pay too much attention in the past to this type of crime. But in the last years, with the complexity of these crimes and with the new modalities, the DOJ has been taking affirmative action to combat this real and imminent threat to our society. Many states have also taken the initiative by implementing new legislation to prosecute cyber criminals. Nevertheless, there exist a great variety of misuses and infringements of intellectual property or actions not yet included in any criminal legislation nor infringement) contemplated in the new legislation.

It is important to remember that an increase in the amount of laws available to prosecute criminals alone, will not help us take control and successfully fight against cybercrime. A mutual effort to enforce and prosecute cyber criminals under this legislation is extremely important if not crucial. The criminal investigation is one of the biggest challenges imposed in the legal system and law enforcement by cyber crime against intellectual property, not only for the complexity of the subject matter, but also because of the technical, operational and legal challenges involved

Desperately seeking ways to prosecute cyber criminals, Congress and Prosecutor have approached computer crime in two ways as a traditional crime committed by new methods, or as crime unique in character requiring new legal frame work. Proof of these approaches are the different

amendments to existing laws, and the enacted of new legislation reflecting the changes in technology that can be adapted to future changes. These enacted laws were constructed broad enough to allow new type of crimes to fit under its definitions or to be added by means of amendment without further problem. In order to define and facilitate the investigation of cyber crime the U.S. Department of Justice has classified them in three broad categories: when the computer is used as a target (victim), medium (tool) or incidental to other criminal offenses. Crimes using a computer as a target or victim of an offense include actions that attack the confidentiality, integrity or availability of the information or services. The second type includes actions where the computer is used as the tool to commit traditional criminal conduct. This category includes those crimes that have been occurring in the physical world but now we are seeing with increasing frequency on the Internet. Examples of this type include child pornography, fraud and intellectual property violations. In the third category, the computer is used to store data, and can seized to obtain evidence of any crime, especially white collars crimes and viruses for example.

To effectively protect the creativity and ingenuity of our citizens, and the trade secrets they develop through research and development, we need to outmatch the criminals. That means integrating our federal resources with the resources of domestic industries that enjoy legal protection under intellectual property laws. Cyber criminals know no national boundaries, and the multi-jurisdictional nature of cyber crimes requires a new multilateral approach to investigations and prosecutions.

BIBLIOGRAPHY

I. United States Constitution

U.S. Const. art I, §8, cl. 8

U.S. Const. amend IV

II. Statutes

15 U.S.C. §1051 and §1127 (1988)

17 U.S.C. §410(c), § 506, §101, §102(a) and (b), §103, 106, 107, 1201(a)(2), 1201(f),(1976)

18 U.S.C. §1028, §1831-1839, §2319A, §2319(b)(3), 2319(b)(2)(B), §2320, 2510, 2511, 2516, 2520

47 U.S.C. §1005

Copyright Act of 1976, Pub. L. No. 94-553, 90 Stat. 2541

No Electronic Theft Act of 1997, Pub. L. No. 105-147, 111 Stat 2678.

Internet False Identification Prevention Act of 2000, 114 Stat 3075

Title III of the Omnibus Crime Control and Safe Streets Act of 1968, Pub. L.No. 90-351, 82 Stat. 212 (current version at 18 U.S.C. §2510-2522 (1996)).

Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat 1848 (current version at 18 U.S.C. §2510-2521, §2701-27110 and §3121-3126 (1996)).

Communications Assistance for Law Enforcement Act of 1994, Pub. L. No. 103-414, 108 Stat 4279 (codified in 47 U.S.C. §1001-1010 and scattered sections of 18 U.S.C. and 47 U.S.C.)

First Restatement of Torts, §757, Comment b and f(1939)

Restatement Third of Unfair Competition §39, Comment B and §43 (1995)

Uniform Trade Secret Act, §1(4)

III. Jurisprudence

Alfred Bell & Co. v. Catalda Fine Arts, 191 F. 2d 99, 102 (1951)

Apple Computer v. Franklin Computer, 714 F. 2d 1240 (3rd Cir. 1983)

Arnstein v. Porter, 154 F. 2d 464, 471 (2nd Cir. 1946)

Baker v. Selden, 101 U.S. 99 (1880)

Berger v. State of New York, 388 U.S. 41, 45 (1971)

Bleinstein v. Donaldson Lithographing Co,. 188 U.S. 239 (1903)

Boggild v. Kenner Products, 576 F. Supp 533, 539(1983)

Brown v. Waddell, 50 F. 3d 285, 294 (4th Cir. 1995)

Burrow-Giles Lithographic Co. v. Sarony, 111 U.S. 53, 57-58 (1884)

Columbia Pictures Industries, Inc. v. T&F Enterprises, Inc. dba Four Star Video & Communications, 68 F. Supp. 2d 833, 843 (1999)

Comprehensive Technologies International, Inc. v. Software Artisans, Inc., 3 F. 3d 730, 740 (1993)

E.I. duPont de Nemours & Co. v. Rolfe Christopher, 431 F. 2d 1012, 1018 (5th Cir. 1970)

Feist Publications v. Rural Telephone Services, 499 U.S. 340, 349 (1945)

Goldstein v. California, 412 U.S. 546, 552(1973)

Harper & Row Publishers v. Nation Enterprises, 417 U.S. 539 (1985)

Katz v. United States, 389 U.S. 347 (1967)

Kewanee Oil Company v. Bicron Corporation, 478 F. 2d 1074, 1077 (1973)

MAI Systems Corp. v. Peak Computer Inc,. 991 F. 2d 511 (1993)

Metallurgical Industries Inc. v. Fourtek, Inc,. 790 F. 2d 1195, 1199 (5th Cir. 1986)

Phillip Morris v. Reilly, 113 F. Supp 2d 129, 133-137 (2000)

Universal City Studios, Inc. v. Reimerdes, 111 F. Supp 2d 294 (Headnote 10)(2000)

United States v. Hsu, 155 F. 3d 189, 194 (3rd Cir. 1998)

United States Telecom Association v. Federal Communications Commission, 2000 WL 1059852 (D.C. Cir.)

United States v. Charbonneau, 979 F. Supp. 1177 (S.D. Ohio 1997)

United States v. Torch, 609 F. 2d 1088, 1090 (4th Cir. 1979)

United States v. Sassani, 1998 WL 89875 (4th Cir. 1998)

United States v. Maxwell, 42 M.J. 568, 576 (1995)

United States v. Cross, 816 F. 2d 203 (1987)

United States v. Laracuente, 952 F. 2d 672 (1992)

United States v. Riggs, 739 F. Supp. 414

West Publishing Co. v. Mead Data Central, 799 F. 2d 1219, 1223 (8th Cir. 1986)

White-Smith Music Publishing Co. v. Apollo Co., 209 U.S. 1, 7 (1908)

IV. Books

Callman, Rudolf, The Law of Unfair Competition, Trademarks and Monopolies, §17.01 (4th ed. 1993)

Cavazos and Gavino Morin, Cyberspace and the Law: Your Rights and Duties in the On-Line World, §2-11 (1994)

Craig, Joyce, William Patry, Marshall Leaffer and Peter Jaszi, Copyright Law, First Chapter, page 1, and Chapter 7, §7.01, page 489(5th ed. 2000)

Merges, Robert P., Peter S. Menell andMark A. Lemley, Intellectual Property in the New Technological Age, Chapter 1, Subsection B, 1, page 22; Chapter 2, Subsection B, 3, page 62; Chapter 4, Subsection E, page 433; Chapter 5, Section D, pages 682-689 and Chapter 7, Subsection C, page 911 (2nd ed. 2000)

V. Periodicals

Ann Meredith Fulton, *Cyberspace and the Internet; Who Will be the Privacy Police?,* 3 CommLaw Conspectus 63 (1995)

Edward Baig, *Ready to Cruise the Internet?,* Business Week, Mar 28, 1994, at 180-181.

Eric J. Sinrod and William P. Reilly, *Cybercrimes: A Practical Apporach to the Application of Federal Computer Crime Laws,* 16 Computer & High Tech L.J. 177, at 179.

James L Robertson, *The Law of Business Torts in Mississippi*, 15 Miss C.L. Rev. 331, 332 (Spring 1995)

James X. Depsey, *Communication Privacy Act in the Digital Age,* 8 Alb L.J. Sci & Tech 65, at 104-105 (1997)

Marjorie A Shields, *Who may apply or authorize application for order to intercept wire or oral communication under Title III of Omnibus Crime and Control and Safe Streets Act of 1968*, 169 A.L.R. Fed 169 (2001)

Mark Sherman, *Introduction to Cybercrime, What is cybercrime?*, Special Need Offender Bulletin No.5, August, 2000

Michael Adler, *Cyberspace, General Searches, and Digital Contraband: The Fourth Amendment and the Net-wide Search*, 105 Yale L.J. 1093 (1996)

Paul Taylor, *Issues Raised by the Application of the Pen Register Statutes to Authorize Government Collection of Information on Packet-Switched Networks*, 6 Va.J.L. & Tech 4 (2000)

Peter H. Lewis, *On the Net*, New York Times, May 29, 1995, at 39.

Philip Elmer-DeWitt, Welcome *to Cyberspace: What is it? Where is it? And How Do We Get There?*, Time, Mar. 22, 1995, at 4-6.

Robert S. Steere, *Keeping Private E-Mail Private: A Proposal to Modify the Electronic Communications Privacy Act*, 33 Val U.L. Rev. 231, 234-246 (1998)

Scott K. Pomeroy, *Promoting the Progress of Science and the Useful Arts in the Digital Domain; Copyright Computer Bulletin Boards, and Liability for Infringement by Others*, 45 Emory L.J. 1035(1996)

Thomas R. Greenberg, *E-Mail and Voice Mail: Employee Privacy and the Federal Wiretap Statute*, 44 Am. U.L. Rev 219 (1994)

John Walter, *Who is peeking at your e-mail?* The Atlanta Journal Constitutional, July 23, 2000.

Russian Man Charged in California under the Digital Millennium Copyright Act with Circumventing Adobe e Book Reader, Press Release, U.S. Department of Justice, United States Attorney, Northern District of California, (July 17, 2001)

U.S. Sentencing Commission, Guidelines Manual §2B5.3(b)(2)(Nov. 1998 & Supp. 2000)

www.cybercrime.gov/ccips.html