



COMPUTER CRIME: A STUDY ON DATA PROTECTION

BY

MR. APICHET SUNTARACHUN

AN INDEPENDENT RESEARCH PAPER SUBMITTED IN PARTIAL
FULFILLMENT OF THE REQUIREMENT
FOR THE DEGREE OF MASTER OF LAWS
(IN BUSINESS LAW)

GRADUATE SCHOOL OF LAW
ASSUMPTION UNIVERSITY

SEPTEMBER 2005

COMPUTER CRIME: A STUDY ON DATA PROTECTION

BY
MR. APICHET SUNTARACHUN

**AN INDEPENDENT RESEARCH PAPER SUBMITTED IN
PARTIAL FULFILLMENT OF THE REQUIREMENT FOR THE
DEGREE OF MASTER OF LAWS
(IN BUSINESS LAW)**

**GRADUATE SCHOOL OF LAW
ASSUMPTION UNIVERSITY
SEPTEMBER 2005**


Research Title: The Problems on Computer Crime: Study on the Data Protection

Author: Mr. Apichet Suntarachun


Major: Business Law (International Program)


Advisor: A. Kiarttiporn Umpai
A. Pongsaton Sestathavorn

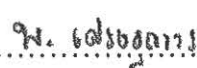
Faculty of Law, Assumption University approves this Independent Research Paper as the partial fulfillment of the requirement for the Degree Master of Laws.


..... Director of the Graduate School of Laws.
(Assoc.Prof. Nattapong Posakabutra)

Committees.


..... Chairman.
(Dr. Poom Moolsilpa)


..... Advisor and Committee.
(A. Kiarttiporn Umpai)


..... Advisor and Committee.
(A. Pongsaton Sestathavorn)

Independent Research Title: The Problems on Computer Crime: Study on the Data Protection

Student Name: Mr. Apichet Suntarachun

Degree: Master of Laws (International Program)

Academic: 2005

Advisor: A. Kiarttiporn Umpai
A. Pongsaton Sestathavong

ABSTRACT

The development of computer technology which is an important kind of communication system in the present world is very rapid. It is a world without border. This development brings forth the ability to transfer and access data inside computers throughout the world. However, it also can be used for committing many kinds of computer crime like using computers to access unauthorized data in other computers.

The purpose of this research is to focus on finding out whether the laws with criminal punishments currently enforced in Thailand can cover the computer crime committed through information technology, and to focus on the offences and liability that are resulted from computer crime.

The result obtained from this research is that, Thailand does not yet have specific legal provision applied to place punishment on computer crime and the present legal provision which has been brought to enforce is also not sufficient. Whenever computer crime is committed, the government agencies involved try to consider it as a criminal case under the Criminal Code or as other offenses stipulated in other similar Acts. However, there are lots of problems in interpretation, for example, when data is not interpreted as property, the criminals who steal data cannot be punished with the charge of steal under the

Article 334 of Criminal Code. So it should be provided the special legal provision on computer crime.

The United States of America have legislated the Computer Crime Acts to take legal action against the computer criminals since 1984 (The Counterfeit Access Device and Computer Fraud and Abuse Act of 1984). The aim of these laws is to crack down the computer crime. In this Act, three major offences are stipulated: Unauthorized Access, Alteration and Damage or Destruction of data.



ACKNOWLEDGEMENT

I would like to express profound the gratitude to Assoc. Prof. Nattapong Posakabutra, Director of Master of Laws Program and chairperson of the Master of Laws Program in Business Law (International Program), for his invaluable support, encouragement, supervision and useful suggestions throughout this independence research paper. His moral support and continuous guidance enabled me to complete my work successfully. I am also highly thankful to Ajarn Kiarttiporn Umpai, Ajarn Pongsaton Sestathavorn, Dr.Poom Moolsilpa, Ajarn Artit Pinpak for their valuable suggestions throughout this study.

I am ever, especially indebted to my parents for their love, suggestions, encouragement and support everything throughout my life. Moreover, my sincere thanks given to my LL.M. friends, who shared their cares and experiences with me. Finally, I wish to express my appreciation once again to everyone as above, who helped me overcome all the doubts in doing this Research.

Apichet Suntarachun

Table of Contents

	Pages
Abstract	iii
Acknowledgement	v
Table of Contents	vi
Chapter 1 : Introduction	
1.1 Historical and Background of the Problems	1
1.2 Hypothesis	1
1.3 The Objective of the Study	2
1.4 Methodology	2
1.5 Scope of the research	2
1.6 Expectation of the research	3
Chapter 2: Computer Crime in Data Protection	
2.1 Introduction	
2.1.1 Information Technology: IT	4
2.1.2 Defining of Computer	4
2.1.3 Historical Development	5
2.2 Computer Crime	
2.2.1 Defining of Computer Crime	7
2.2.2 The Nature of Computer Crime	9
2.3 Categories of Computer Crime	
2.3.1 Fraud by Computer Manipulation	11
2.3.2 Computer Forgery	13
2.3.3 Damage to or Modifications of Computer Data or Programs	13
2.3.4 Unauthorized Access to Computer Systems and Service ...	18
2.3.5 Computer Espionage	20

Pages**Chapter 3: Computer Crime Related Data Protection**

3.1	Computer Crime Related Data Protection	
3.1.1	Unauthorized Access and Use Computer Data.....	23
3.1.2	Duplicate Computer Data	27
3.1.3	Alteration Computer Data	30
3.1.4	Damage or Destruction Computer Data	32
3.2	The Problem of Data Protection in the Thailand	
3.2.1	Legal Problem	36
3.2.2	Impact to Economic	39
3.2.3	Impact to Society	42

Chapter 4: Computer Crime Relate with Data Protection in US and Thailand

4.1	The US Computer Crime Law: Relate with Data Protection	
4.1.1	Statutes of US Computer Crime	44
4.1.2	Liability of Computer Crime-Relate Data Protection of US	47
4.2	The Law and Security Measure of Computer Data in Thailand	
4.2.1	Nature of Thai Law	51
4.2.2	Penal Code	52
4.3	The Problem of Computer Crime: Related Data Protection in Criminal Law	
4.3.1	Offence of Theft	52
4.3.2	Offence of Criminal Misappropriation	54
4.3.3	Offence Relating to Counterfeiting and Alteration	54
4.3.4	Offence of Mischief	55

Pages**Chapter 5: Conclusion and Recommendation**

5.1 Conclusion and Recommendation	56
---	----

Bibliography	62
--------------------	----



Chapter 1

Introduction

1.1 Introduction and Problems Identification

At present, the growth of technology is rapidly emerging, especially, the growth of computer technologies and the internet that are bringing the centers of information exchange, transfer or communication of data. Therefore, the computer system, data and computer networks are essential components in this time; since computer systems are concerned with the economy, government and everybody who lives in the society.

The rapid development of computer technology is bringing advantages such as easy use and comfort for overseas communication, multimedia, personal entertainment etc., however, the rapid development is also bringing disadvantages. The problems that occurred by the rapid development of computer technology is computer crime. These problems are troubling the society and economy; for example, virus attacks, hackers, frauds, insults on internet. Those offences may occur because of the loophole of law, like the law does not empower to arrest the offenders for punishing or it is difficult to arrest them.

Currently in Thailand, this problem has been increasing so we ought to find the measure or protection to stop the cyber criminals. This is why the researcher has claimed that the law does not cover cyber crime and does not provide direct enforcement to offenders. There are only comparative laws to enforce that, however, impose fewer penalties and do not provide justice for injured persons.

1.2 Hypothesis

In general, the crimes that occur in the present time are severe and it is complex and difficult to suppress since many countries are developing new technologies to benefit ways of life and businesses, but the criminals also improve themselves to use the new

technologies to commit offences. Therefore, it's very difficult to prove an offence and there is not a measure to secure data that are earned from new technologies.

Especially, the measure for Data Protection by the criminal law which is being adapted now is not sufficient. There are problems in interpreting and enforcing the law, so it is a cause of the legal problem. Therefore, there must be a clear measure for protection of innocent people and suppression of computer crimes. So, Thailand should have a specialized legislation for computer crime.

1.3 Research Objective

- 1.3.1 To study computer crime causes damages and danger in the systems of the country.
- 1.3.2 To study laws, rules and regulations that other countries used to handle computer crime-Related data protection.
- 1.3.3 To Study problems of computer crime related data protection.
- 1.3.4 To study about the cause and measure for data protection in the United States of America and Thailand also about the specialized legislation for protect the computer data.

1.4 Research Methodology

This research paper uses documentary research in the research methodology and compiles the documents in both Thai and English languages in the text book, journal, article, thesis, and research.

1.5 The Scope of Research

This research is to study about the meaning, nature and damage incurred from computer crime. There are many types of computer crime so the researcher would like to concentrate on the computer crime-related data protection by studying the existing law of Thailand and the US computer crime law.

1.6 Expectation on the Research

- 1.6.1 Identify the problems of the computer crime.
- 1.6.2 To realize the history and the development of computer crime- related data protection the meaning of computer crime and types of computer crime.
- 1.6.3 To realize the damages that is incurred from unauthorized access, alteration and damage or destruction the data of computer.
- 1.6.4 To realize the concept of criminal enforcement from unauthorized access, alteration and damage or destruction the data of computer.
- 1.6.5 To realize the concept of criminal enforcement of United Stage of America from unauthorized access, alteration and damage or destruction the data of computer.
- 1.6.6 To realize the way to rectify or raise a criminal statute for securing the computer data.

Chapter 2

Computer Crime in Data Protection

2.1 Introduction

2.1.1 Information Technology: IT

Information Technology is the technologies that store, process, retrieve, distribute, disperse, communicate data in electronic form, it includes radio, television, telephone, computer etc. therefore, the Information technologies can be divided into 2 parts. The first is Computer and the second is Data Communication.

2.1.2 Defining of Computer

A computer is a device or machine for making calculation or controlling operations that are expressible in numerical or logical terms. Computers are constructed from components that perform simple well-defined functions. The complex interactions of these components endow computers with the ability to process data and information. If correctly configured (usually by, programming) a computer can be made to represent some aspects of a problem or parts of a system¹.

US Federal Computer Crime and Abuse Act²

Computer means an electronic, magnetic, optical, electromagnetic, or other high speed data processing devices performing logical, arithmetic, or storage function and includes any data storage facility or

¹ HyperText Transfer Protocol, Wikipedia, the free encyclopedia, 2005. In <http://en.wikipedia.org/wiki/>, Access date 04/27/2005.

² US Federal Computer Crime and Abuse Act (FCAA)

communication facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator or similar device;

Singapore Computer Misuse Act³

"Computer" means an electronic, magnetic, optical, electrochemical, or other data processing device, or group of such interconnected or related devices, performing logical, arithmetic, or storage functions, and includes any data storage facility, communications facility directly related to or operating in conjunction with such device or group of such interconnected or related devices, but not include

- 1) An automated typewriter or typesetter;
- 2) A portable hand held calculator;
- 3) A similar device which is non-programmable or which does not contain data storage facility; or
- 4) Such other devices as the Minister may, by notification in the Gazette, prescribe;

2.1.3 Historical Development

It is difficult to determine when the first crime involving a computer actually occurred. The computer has been around in some form since the abacus, which is known to have existed in 3500 B.C. in Japan, China and India. In 1801 profit motives encouraged Joseph Jacquard, a textile manufacturer in France, to design the forerunner of the computer card. This device allowed the repetition of a series of steps in the weaving of special fabrics. So concerned were Jacquard's

³ Singapore Computer Misuse Act cited in Buncha Lertbunnapong, "Thailand Computer Crime Bill" (Master's Thesis , Chulalongkorn University, 2004), p.8.

employees with the threat to their traditional employment and livelihood that Acts of sabotage were committed to discourage Mr. Jacquard from further use of the new technology. A computer crime had been committed.

The history of “computer crime” dates back to the 1960 when the first articles on the cases called “computer crime” or computer-related crime” was published to the public in the public press and in scientific literature⁴. These cases primarily included computer manipulation, computer sabotage, computer espionage and the illegal use of computer system. However, due to the fact that most reports were based on newspaper clipping, it was controversially discussed whether or not this new phenomenon of computer crime had any plausible reasons.⁵

In 1983 a group of experts of the Organization for Economic Corporation and Development⁶ (OECD) defined the term “computer crime” (or “computer-related crime”) as any illegal unethical or unauthorized behavior involving autonomic data proceeding and/or transmission of data⁷. Later studies went even further in developing broader concepts on “data and/or information crime”⁸. The breadth of these definitions proved to be advantageous as it allowed the use of the same working hypothesis for all kinds of criminological,

⁴ Ulrich Sieber, Legal Aspect of Computer –Relate Crime in the information Society- COMCRIME-student vol. 1(1998).

⁵ Tiber, A survey of computer crime studies, (computer and law journal, 1980), p.275.

⁶ Computer-Related Crime: Analysis of legal policy, (OECD:PARIS ,1986)

⁷ Ulrich Sieber, The international Handbook on Computer Crime (1986), p. 1.

⁸ Ulrich Sieber, The international Emergence of Criminal InformationLaw(1992), pp. 11-13.

criminality, economic, preventive and legal studies from only dealing with the phenomena of computer crime which cause computer-specific problems in their own discipline. The present study follows this definition and methodology: it is based in the broad concept of computer crime, as defined by the OECD. However, the legal part of the study will focus on computer-related criminal law creating computer-specific legal problems.

2.2 Computer Crime

2.2.1 Defining of Computer Crime

Computer crimes are broad groups of crime that involve computers as the object of the crime, as the instrumentality of the criminal or as the locus of the crime⁹. So Computer crime requiring knowledge of computer technology, such as sabotaging or stealing computer data or using a computer to commit some other crime. Therefore, the computer is implemented for the people who use to do the criminal offenses. The commission of an offence by using the computer may be in computer system, computer network and data system. The computer crime is related with the technology because the new technologies of computer are appealing the people to use for comfortable, modern and speedy life style. So the computers are important for the business or work to store and manage business data; for example, the business data that have a lot of value such as trade secret or secret information. If these data are disclosed to the public or adversary, it will bring damage to the business. So the crime has impact on the people who live in the society. The nature of computer crime can be of many kinds and occur in the same way by using computer such as using computer to destroy or change data of other people, to transfer money, to counterfeit ATM

⁹ Carl Benson, "Computer Crime" (Master's Thesis ,Indiana University,1997), p. 409.

card and account number for embezzlement or using computer to control and follow to do the crime – like stir of sex, defamation to persons or organ trading by internet are some examples of computer crime.

In general, the lawyer or organizations will use the words that concern with computer crime such as ‘computer abuse’, ‘computer fraud’, ‘computer-related crime’, and ‘computer-assisted crime’ and ‘computer crime’. However, there are many academics defining computer crime as the following:

Broadly defined, computer crime is any criminal offense, activity or issue that involves computers. There are two categories of computer crimes: any criminal activity that involves using a computer to commit a crime or any crime that has a computer as a target. Jones Telecommunication and Multimedia Encyclopedia define types of computer crimes. It is often difficult to classify a crime into one of these categories; many computer crimes fall into both.¹⁰

Loosely defined, the terms "computer crime" and "technology misuse" pertain to any intentional or unintentional harm done to or with information and/or hardware that may result in losses of or injury to, property, services, and people. For our operational purposes, we have used the term "computer crime" to refer specifically to actions which are against the local, state or federal laws. We have used the term "technology misuse" for situations where the legalities are unclear (e.g.

¹⁰ Broadly, “Computer Crime-Laws, Regulations, & Today’s Issues” (2002). In <http://www.personal.psu.edu/users/a/a/aaw136/ist432/>, Access date June 20, 2005.

remote examination of others' data or records without their specific permission as discussed in the Computer Hacking section).¹¹

Bowen, Mace define it as, Criminal activity directly related to the use of computers, specifically illegal trespass into the computer system or database of another, manipulation or theft of stored or on-line data, or sabotage of equipment and data.¹²

2.2.2 The Nature of Computer Crime

Computer Crime is one of Economic Crimes. Computer Crime occurs when the people or a body of persons commit a criminal offence or violate some rules by using computer (equipment) to commit an offence and people receive damages from invading in the computer system as well. Unauthorized access to information system for stealth that is the cause of damages to the data owners and sometimes the impact spreads to economic system of country or the world.

1) Computer crime can be divided into 4 types

- (1) Computer is the target of the crime including unauthorized access to the computer system, interception of non-public computer data, intentional damaging of computer data including spreading of viruses, Trojan horse, logic bombs, malicious codes and other harmful programs

¹¹ Karen Eder, "Defining Computer Crime and Technology Misuse". In <http://lrs.ed.uiuc.edu/wp/crime/definition.htm> ,Access date August 20, 2005.

¹² Bowen Mace, "Compute Crime". In <http://www.wowessays.com> , Access date August 25, 2005.

and intentional interference with computer system, computer espionage.

- (2) Computer is an instrument of the crime including forgery of electronic documents, and fraudulent computer alteration for personal benefit.
- (3) Computer-related crime including money laundering and transferring of illegal money through electronic transaction, pornography, and copyright infringement
- (4) Computer network malfeasance and coercion.¹³

2.3 Categories of Computer Crime

All stages of computer operations are susceptible to criminal activity, either as the target of the crime or the instrument of the crime or both. Input operations, data processing, output operations and communications have all been utilized for illicit purposes.

According to Prof. Dr. Sieber, a more comprehensive six fold classification is adopted: (1) fraud by computer manipulation, (2) computer espionage and software theft, (3) computer sabotage, (4) theft of services, (5) unauthorized access to data processing system, and (6) traditional business offences assisted by data processing.

However Prof. Dr. Wasik¹⁴ said that, the substantive criminal law which is or may become relevant to computer misuse is considered under the following broad heading: (a) Unauthorized access and

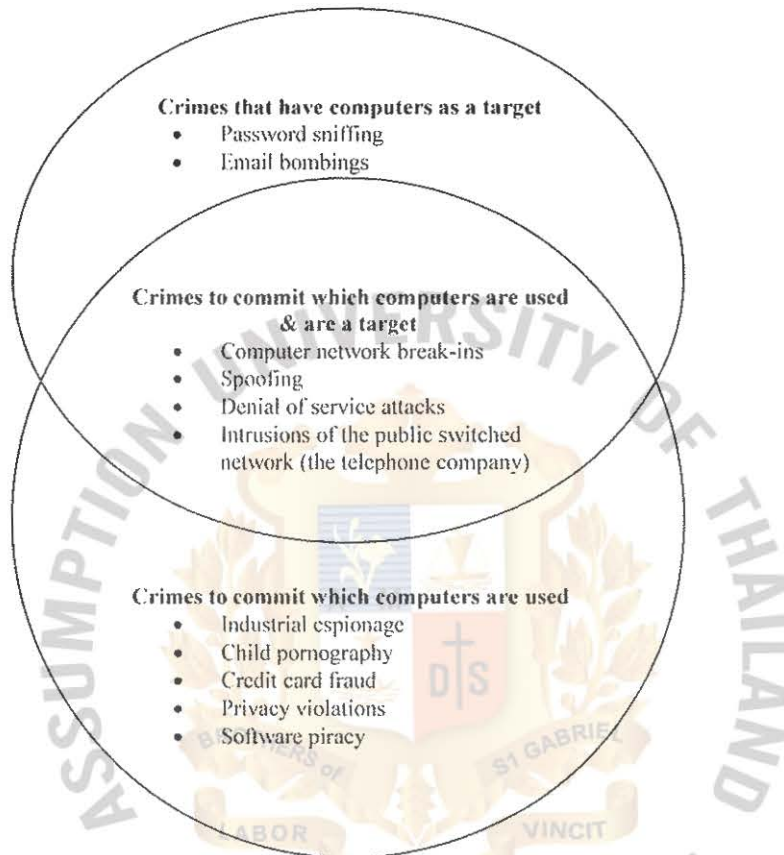
¹³ Buncha Lertbunnapong, "Thailand Computer Crime Bill" (Master's Thesis, Chulalongkorn University, 2004), p.1.

¹⁴ Martin Wasik, Crime and the Computer (Clarendon Press:Oxford,1987),p.

unauthorized use, (b) fraud and information theft, and (c) associated offences.

4084 e-4

An example of a classification of typical computer crimes



The more common types of computer-related crime and categorized next.

2.3.1 Fraud by Computer Manipulation

Intangible assets represented in data format, such as money on deposit or hours of work, are the most common targets of computer-related fraud. Modern business is quickly replacing cash with deposits transacted on computer systems, creating an enormous potential for computer abuse. Credit card information, as well as personal and financial information on credit-card clients, has been frequently targeted by the organized criminal community. The sale of this information to counterfeiters of credit cards and travel documents has proven to be extremely lucrative. Assets represented in data format

often have a considerably higher value than traditionally targeted economic assets, resulting in potentially greater economic loss. In addition, improved remote access to databases allows the criminals the opportunities to commit various types of fraud without even physically entering the premises of the victims.

Computer fraud by input manipulation is the most common computer crime, as it is easily perpetrated and difficult to detect. Often referred to as “data diddling”, it does not require any sophisticated computer knowledge and can be committed by anyone having access to normal data processing function at the input stage.

Program manipulation, which is very difficult to discover and is frequently not recognized, requires the perpetrators to have computer-specific knowledge. It involves changing existing programs in the computer system or inserting new programs or routines. A common method used by persons with specialized knowledge of computer programming is the Trojan horse, whereby computer instructions are covertly placed in a computer program so that it will perform an unauthorized function concurrent with its normal functions. A Trojan horse can be programmed to self-destruct, leaving no evidence of its existence except the damage that it caused. Remote access capabilities today also allow the criminals to easily run modified routines concurrently with legitimate program.

Output manipulation is effected by targeting the output of the computer system. The obvious example is cash dispenser fraud by falsifying instructions to the computer in the input stage. Traditionally, such fraud involved the use of stolen bank cards. However, specialized computer hardware and software is now being widely used to encode falsified electronic information on the magnetic strips of bank cards and credit cards.

There is a particular species of fraud conducted by computer manipulation that takes advantage of the automatic repetitions of computer processes. Such manipulation is characteristic of the specialized “salami technique”, whereby nearly unnoticeable, “thin slice” of financial transactions are repeatedly removed and transferred to another account.

2.3.2 Computer Forgery

Where data are altered in respect of documents stored in computerized form, the crime is forgery. In this and the above examples, computer systems are the target of criminal activity. Computers, however, can also be used as instrument with which to commit forgery. They created a new library of tools with which to forge the documents used in commerce. A new generation of fraudulent alteration or counterfeiting emerged when computerized color laser copies became available. These copiers are capable of high-resolution copying, the modification of documents and even the creation of false documents without benefit of the original copyright holder, and they produce documents whose quality is indistinguishable from that of authentic documents even inspected by an expert.

2.3.2 Damages or Modifications of Computer Data or Programs

For the method, one can differentiate between methods causing physical damage and those causing logical damage. During the 1970s, the most frequently practiced methods of causing physical damages were igniting or bombing a building. These techniques were typically applied by “outsider” not employed or otherwise related with the owners of the facilities damaged.

For “insider” aiming to effect damages in the facilities within the company mainly in access of labors and other social conflicts; the following additional techniques of physical destruction were recommended by left-wing European underground magazines: gluing emery paper into the electronically readable parts of cards in order to destroy badge-or card readers; inserting iron-cuttings, paper clip, or small pieces of aluminum foil into computer devices in order to cause electrical shortcuts; pouring coffee, saline solution, and caustic cleaning agents into the operator console and other equipment; blowing smoke, hair-spray and other gases into sensible devices; putting a container of hydrochloric acid in front of the air-conditioner or by heating computer parts with a lit cigarette; inserting with the electric power station, switching office, or communication lines; and cutting cables or putting mice under a raised floor where they could gnaw through the insulation of electrical power-cords.

Today, the most popular method of causing logical damage is through the use of crash programs which can erase large volumes of data within a short period. These programs can be self-written utilities or “Trojan horse” routines built into application programs or into the operating system. Crash programs can also exploit hardware defects (“bug”).

This category of criminal activity involves either direct or covert unauthorized access to a computer system by the introduction of new programs known as 1.viruses¹⁵

¹⁵ A **virus** is a program that “infects” an executable file. After infection, the executable file functions in a different way than before: maybe only displaying a benign message on the monitor, maybe deleting some or all files on the user's hard drive, maybe altering data files. There are two key features of a computer virus:

2. Worms¹⁶ or 3. Logic bombs¹⁷. The unauthorized modification, suppression or erasure of computer data or functions with the internet to hinder normal functioning of the system is clearly criminal activity

1. The ability to propagate by attaching itself to executable files (e.g., application programs, operating system, macros, scripts, boot sector of a hard disk or floppy disk, etc.) Running the executable file may make new copies of the virus.

2. The virus causes harm only *after* it has infected an executable file and the executable file is run.

The word "virus" is also commonly used broadly to include computer viruses, worms, and Trojan Horse programs. For example, so-called "anti-virus software" will remove all three classes of these malicious programs.

Beginning with the Melissa virus in 1999, viruses could automatically send e-mail with the victim's name as the alleged source.

¹⁶ A **worm** is a program that copies itself. The distinction between a virus and worm is that a virus never copies itself – a virus is copied only when the infected executable file is run.

In the pure, original form, a worm neither deleted nor changed files on the victim's computer — the worm simply made multiple copies of itself and sent those copies from the victim's computer, thus clogging disk drives and the Internet with multiple copies of the worm. Releasing such a worm into the Internet will slow the legitimate traffic on the Internet, as continuously increasing amounts of traffic are mere copies of the worm.

Beginning with the Klez worm in early 2002, a worm could drop a virus into the victim's computer. This kind of worm became known as a *blended threat*, because it combined two different types of malicious code.

¹⁷ A **logic bomb** is a program that "detonates" when some event occurs. The detonated program might stop working (e.g., go into an infinite loop), crash the computer, release a virus, delete data files, or any of many other harmful possibilities. A **time bomb** is a type of logic bomb, in which the program detonates when the computer's clock reaches some target date.

and is commonly referred to as computer sabotage. Computer sabotage can be the vehicle for gaining economic advantage over a competitor, for promoting the illegal activities of ideologically motivated terrorists or for stealing data or programs (also referred to as “bit napping”) for extorting purposes. In one reported incident at London, Ontario, in 1987, a former employee of a company sought unsuccessfully to sabotage the computer system of the company by inserting a program into the system that would have wiped it out completely.

A virus is a series of program codes that has the ability to attach itself to legitimate programs and propagate itself to other computer programs. A virus can be introduced to a system by a legitimate piece of software that has been infected, as well as by the Trojan horse ¹⁸ method discussed above.

The potential purposes of viruses are many, ranging from the display of harmless messages on several computer terminals to the irreversible destruction of all data on a computer system. In 1990, Europe first experienced a computer virus, used to commit extortion in the medical research community. The virus threatened to destroy increasing

¹⁸ A **Trojan Horse** is a deceptively labeled program that contains at least one function that is unknown to the user and that harms the user. A Trojan Horse does *not* replicate, which distinguishes it from viruses and worms.

Some of the more serious Trojan horses allow a hacker to remotely control the victim's computer, perhaps to collect passwords and credit card numbers and send them to the hacker, or perhaps to launch denial of service attacks on websites.

Some Trojan Horses are installed on a victim's computer by an intruder, without any knowledge of the victim. Other Trojan Horses are downloaded (perhaps in an attachment in e-mail) and installed by the user, who intends to acquire a benefit that is quite different from the undisclosed true purpose of the Trojan Horse.

amounts of data if no ransom was paid for the “cure”. A significant amount of valuable medical research data was lost as a result.

A worm is similarly constructed to infect legitimate data-processing programs and to alter or destroy the data, but it differs from a virus in that it does not have the ability to replicate itself. In a medical analogy, the worm can be compared to a beginning tumor, the virus to malignant one. However, the consequences of a worm attack can be just as serious as those of a virus attack; for example, a bank computer can be instructed, by a worm program that subsequently destroys itself to continually transfer money to an illicit account.

A logic bomb, also known as a “time bomb”, is another technique by which computer sabotage can be perpetrated. The creation of logic bombs requires some specialized knowledge, as it involves programming the destruction or modification of data at a specific time in the future. Unlike viruses or worms, however, logic bombs are very difficult to detect before they blow up; thus, of all these computer crime schemes, they have the greatest potential for damage. Detonation can be timed to cause maximum damage and to take place long after the departure of the perpetrator. The logic bomb may also be used as a tool of extortion, with a ransom being demanded in exchange for disclosure of the location of the bomb.

Irrespective of motive, the fact remains that the use of viruses, worms and logic bombs constitutes unauthorized modification of legitimate computer data or programs and thus fall under the rubric computer sabotage, although the motive of the sabotage may be circumstantial to the alteration of the data.

An example of computer sabotage by using computer programs to erase data is demonstrated in the case involving a southern German

engineer. He erased the comments of a valuable computer program on the disc before leaving the company so that it could not be easily modified by other programmers due to which the company almost lost a contract worth about DM 1 million. The accused programmer declared that he had copied the comments onto another disc in order to save space on the original one, and that the second disc must have been lost after his dismissal.

2.3.3 Unauthorized Access to Computer Systems and Service

The desire to gain unauthorized access to computer system can be prompted by several motives, from simple curiosity, as exemplified by many hackers, to computer sabotage or espionage. International and unjustified access by a person not authorized by the owners or operators of a system may often constitute criminal behavior. Unauthorized access creates the opportunity to cause additional unintended damage to data, system crashes or impediments to legitimate system users by negligence.

Access is often accomplished from a remote location along a telecommunication network, by one of several means. The perpetrator may be able to take advantage of lax security measures to gain access or may find loopholes in existing security measures or system procedures. Frequently, hackers impersonate legitimate system users; this is especially common in systems where users can employ common passwords or maintenance passwords found in the system itself.

Password protection is often mischaracterized as a protective against unauthorized access. However, the modern hacker can easily circumvent this protection using one of there common methods. If a hacker is able to discover a password allowing access, then a Trojan horse program can be placed to capture the other passwords of

legitimate uses. This type of program can operate concurrently with the normal security function and is difficult to detect. The hacker can later retrieve the program containing the stolen passwords by remote access.

Password protection can also be bypassed successfully by utilizing password cracking routines. Most modern software effects password security by a process that converts a user's select password into a mathematical series, a process known as encryption disguises the actual password, which is then almost impossible to decrypt. Furthermore, legitimate security software has been developed that allows access to data only after it checks encrypted passwords against a dictionary of common passwords so as to alert system administrators of potential weakness in security. However, this same security process can be imitated for illegitimated purposes. Known as a "cracker" program when used for illegitimate purposes, these tools encrypt some or all of the data of the system. This creates a dictionary of data to compare with cracker software, for the purpose of identifying common passwords and gaining access to the system. A variety of these-specific encryption routines can be obtained from hacker bulletin boards around the world and are regularly updated by the criminal community as security technology develops.

The third method commonly used to access a system in the "trapdoor" method, whereby unauthorized access is achieved through access points, or trapdoor, created for legitimate purposes, such as maintenance of the system.

The international criminal hacker community uses electronic bulletin boards to communicate system infiltration incidents and methods. In one case, details of a Canadian attempt to access a system were found on suspects in an unrelated matter in England; they had removed the material from a bulletin board in Germany. This sharing of information

can facilitate multiple unauthorized infiltrations of a system from around the globe, resulting in staggering telecommunication charges to the victim.

With the development of modern telecommunications system, a new field for unauthorized infiltration is created; Personal telecommunications have been expanded with the advent of portable, cellular telecommunication devices. The criminal community has responded to these advances by duplicating the microchip technology.

Modern telecommunications systems are equally vulnerable to criminal activity. Office automation systems such as voice mail boxes and private business exchanges are, in effect computer systems, designed for the convenience of users. However, convenience features such as remote access and maintenance capabilities, call-forwarding and voice-messaging are easily infiltrated by computer criminals.

Modern telecommunication system, like other computer systems, is also susceptible to abuse by remote access. The integration of telecommunication systems means that once one system is accessed, a computer operator with sufficient skill could infiltrate telecommunication network of a city. The usual motive for telecommunication crime is to obtain free telecommunication services. However, more innovative telecommunication fraud has also been uncovered, and telecommunication systems have been used to disguise other forms of criminal activity.

2.3.4 Computer Espionage

Computer Espionage – only rarely appearing in official statistics constitutes a special danger compared with traditional economic espionage, because in computer systems, huge quantities of data are

stored in an extremely narrow space, and the data can be copied quickly and easily with the help of modern technology, also via data telecommunication. The objects of offence are especially computer programs, data of research and defense, data of commercial accounting as well as addresses of clients. As the *modus operandi*, the simple copying of data is predominant; the theft of data carries the evaluation of “remaining data” or the absorbing of electromagnetic are also effected. Besides young hackers and competing business enterprises, secret services increasingly appeared to be dealing with economic espionage in recent years.

The case of the KGB hacking presented above illustrates the close relation between hacking and computer espionage. A Japanese case from 1988 shows the possibility of using computer viruses for computer espionage: In this case, a computer virus penetrated a network of personal computers, collected secret numbers of other network users and then wrote these numbers down on an internal network “black board” in an encoded form usable only for the perpetrators.¹⁹

Giving an example for potential impact of such activities, reliable sources in Germany refer to the competition between the German company Siemens and a French competitor with respect to a huge contract deciding on a future high-speed train system in South Korea: French agents could intercept the satellite based fax transmission of the offer of the German company which was not encrypted so that the French company could undercut the German offer²⁰.

¹⁹ Yamaguchi, in Sieber(ed.), *Information Technology Crime*, 1994, p. 307.

²⁰ Ulrich Sieber, *Legal Aspect of Computer-Related Crime in the Information Society-COMCRIME study*, 1988, p.45.

The techniques of bugging telephones were used especially by the State Security Service of the former German Democratic Republic: the telephone numbers of politicians, of member of the secret service and of other important bearers of the Federal Republic of Germany were registered as target numbers, so that the telephone communications of these persons were automatically recorded.

Massive measures of listening in on telephone conversation are/were also carried out by the American National Security Agency (NSA). According to published reports, the NSA is said to run more than 2,000 installations for bugging telephones world-wide, which can supervise up to 54,000 telephone conversations at the same time.²¹

In 1982 an attempted espionage attack on IBM by twenty individuals working for Hitachi was thwarted by an FBI 'sting' operation. (Bloom Becker (1985)) In 1984 twenty-five computer disks containing instructions for glass-cutting machines went missing from Waterford Crystal in the Republic of Ireland. Although they were eventually recovered, it seems clear that they had already been copied by an industrial rival.

²¹ Cf. Garcia, UCLA Law (1991), pp. 1043-1055 cited in, Gristana Changgom. "Computer Crime in European Union"(Research , European University; 1999) ,p.33.

Chapter 3

Computer Crime Related Data Protection

3.1 Computer Crime Related Data Protection

The offences related with computer data is a one type of computer crime. There are many kinds of it depending on the objective and pattern. The importance of considering this offence is its impact because this offence is bringing a lot of damages to the data owners. Therefore, the method to solve this problem is by applying recent law to check this offence, but it is not sufficient or complete so. However, before we analyze this problem, we ought to know the nature and pattern of the committing computer- related crime.

3.1.1 Unauthorized Access and Use Computer Data

First, we start with analysing the word “Unauthorized Access” and use of computer data. We should understand the word of “Access”. Actually, this word is not important for computer scientists but it is very important for lawyers especially the criminal lawyers.

Since the penal code of Thailand does not providing the word of “Access” so we have to study the meaning from the foreign law.

The meaning of “Access” that the US law uses is that Access means approaching, instruct, communicate with, store data in, retrieve data from or make use of any resources.¹

At present, committing an offence by unauthorized access and use of computer data is easy to do because many organizations decide to use

¹ Phanu Rungsisahut, “Commit a criminal offence: related computer”
(Master’s thesis , Chulalongkorn University, 1990), p.53.

instant computer systems, so it is easy for unauthorized access. The new technology of telecommunication helps to access computer data, without entering the main computer, by just the offenders having only personal computers and internet modems so they can connect to the main computer. In some cases, the offence intent is not to espionage but just for challenging one's ability to pass a security system of computer programs.

Next we examine the problems of Unauthorized Access and use of computer data in penal code. If we would adjust the offence of unauthorized access and use of data to the offence in criminal law, it is comparable with offence of theft and offence of trespass. The problem does not occur, if this offence is done to computer or accessory of computer and it can be seen physically or the offender enters the place that the computer stays. But in fact, the data in computer cannot be seen physically so this is the problem to interpret whether a theft has been committed or not. Therefore, many countries should legislate a special law deal with such offence.

Case study of Unauthorized Access and use computer data

Chardon, Ohio Woman Sentenced for Computer Fraud via Unauthorized Access of Employer's Computer System

Emily M. Sweeney, United States Attorney for the Northern District of Ohio, today announced that on Monday, November 26, 2001, Melissa S. Brown, age 30, of 115 Tilden Avenue, Chardon, Ohio, and was sentenced by U.S. District Judge Dan A. Polster in U.S. District Court in Akron, Ohio, in connection with her recent computer crime conviction. Brown was sentenced to three years probation, with a special condition that the first 7 months of her probation be served in home confinement with electronic monitoring. Brown was also ordered

to pay \$15,346.71 in restitution to Christian & Timbers, the victim of her offense.

On July 6, 2001, a federal grand jury in Cleveland, Ohio, returned a one count indictment charging Brown, with computer fraud in violation of Title 18, United States Code, Section 1030(a)(5)(A). The indictment charged that on or about April 14, 2001, Brown knowingly caused the transmission of a program, information, code or command, and as a result of such conduct, intentionally caused damage, without authorization, to a protected computer server owned and/or operated by Christian & Timbers, 25825 Science Park Drive, Beachwood, Ohio.

On September 14, 2001, Brown pleaded guilty to the one count indictment. According to Court documents filed in U.S. District Court. Brown admitted that between the hours of 4:04 a.m. and 5:09 a.m. on April 14, 2001, she remotely logged onto the computer system of her employer, Christian & Timbers, an executive recruitment firm located in Beachwood, Ohio, from a company laptop computer located at her residence in Chardon, Ohio. During the session, Brown logged onto the company's computer system using the user ID and password of a co-worker, without the knowledge or authorization of the co-worker, and transmitted certain computer codes, instructions and/or commands to change the password of the company's Chief Information Officer who was on vacation at the time, thus preventing the CIO from gaining log-on access to the company computer. As a result, the victim corporation was forced to conduct a thorough analysis of their entire computer network to see if any additional damage had been done, or if any data or information had been improperly obtained by Brown.

As a result of her actions, Brown admitted that she caused Christian & Timbers to incur losses in the amount of \$15,346.71.

This case was prosecuted by Assistant U.S. Attorney Robert W. Kern, following an investigation by the Cleveland Office of the Federal Bureau of Investigation².

San Francisco Man Pleads Guilty to Unauthorized Access of Catholic Healthcare West Computer Causing Damage

The United States Attorney's Office for the Northern District of California announced that Michael Logan pled guilty today in San Francisco to a charge of unauthorized access into a protected computer causing damage in violation of Title 18, United States Codes, Section 1030(a)(5)(C).

Mr. Logan, 34, of San Francisco, was indicted by a federal grand jury on September 25, 2001. He was charged in a three-count indictment with unauthorized access into a computer recklessly causing damage, unauthorized access into a computer causing damage, and utilizing a telecommunications device in interstate communications with intent to harass, in violation of Title 18, United States Code, Sections 1030(a)(5)(B) and (a)(5)(C), and Title 47, United States Code, Section 223(a)(1)(C). Under the plea agreement, Mr. Logan pled guilty to count two of the indictment.

In pleading guilty, Mr. Logan admitted that he intentionally and without authorization accessed a computer of Catholic Healthcare West ("CHW") without authorization on or about November 28, 1999. Specifically, he admitted that he committed the computer intrusion and then sent electronic mail to approximately 30,000 employees and

² U.S. Department of Justice.Chardon.Ohio Woman Sentenced for Computer Fraud via Unauthorized Access of Employer's Computer System, December 14, 2001. In <http://www.cybercrime.gov/brownSent.htm> , Access date May 25, 2005.

associates of CHW. The e-mail purported to be from a named employee of CHW and contained insulting statements about that named employee and other CHW employees. Mr. Logan further admitted that, as a result of his conduct, he caused damage of at least \$5,000 to CHW. According to public records in the case, Mr. Logan actually caused damage to CHW of more than \$25,000.

The sentencing of Mr. Logan is scheduled for April 26, 2002, at 11 a.m. before Judge Susan Illston in San Francisco. The maximum statutory penalty for a violation of Title 18 United States Code, Section 1030(a)(5)(C) is one year in prison and a fine of \$100,000, plus restitution. However, the actual sentence will be dictated by the Federal Sentencing Guidelines, which take into account a number of factors, and will be imposed in the discretion of the Court.

This prosecution is the result of an investigation by agents of the Federal Bureau of Investigation's Computer Intrusion Squad. Ross W. Nadel, Chief of the U.S. Attorney's Office's Computer Hacking and Intellectual Property ("CHIP") Unit, is the Assistant U.S. Attorney who prosecuted the case.³

3.1.2 Duplicate of Computer Data

Duplicate of computer data can be divided into 2 types. The first is Copying and the second is Extracting, both of them are easy for the offenders to do by accessing to the computer data. Exempt in some cases where it requires special knowledge for committing this crime.

³ U.S. Department of Justice, Chardon, "San Francisco Man Pleads Guilty to Unauthorized Access of Catholic Healthcare West Computer Causing Damage", July 6, 2001. In <http://www.cybercrime.gov/loganPlea.html>, Access date June 12, 2005.

Further, there is one more offence besides duplicate of computer data; it is an Unauthorized Interception (stealthily bringing other's data); for example, hiding an intercept, using the camera that can zoom in faraway or using the accessory to connect for interception.

Next are the impacts incurred from duplicates of computer data or unauthorized Interception. It will affect the economy because the most of data that is stolen by the offenders are commercial data; they are valuable data for the business such as account data, industry data or trade secret. There are many causes for espionage such as fraudulent, cheating or infiltrating to enemy companies by use of employees. Especially, a new technology is good instrument for the offenders to commit offences.

Case study of Duplicate computer data

Three Men Indicted for Hacking into Lowe's Companies' Computers with Intent to Steal Credit Card Information

CHARLOTTE, N.C. -- United States Attorney Robert J. Conrad, Jr. and Chris Swecker, Special Agent in Charge of the FBI in North Carolina, announced that BRIAN A. SALCEDO, ADAM W. BOTBYL, and PAUL G. TIMMINS were indicted November 19, 2003 by a federal grand jury on sixteen counts alleging conspiracy, wire fraud, computer fraud, unauthorized computer access, intentional transmission of computer code, and attempted possession of unauthorized access devices.

According to the indictment, from October 2003 through November 9, 2003, SALCEDO, BOTBYL, and TIMMINS conspired and schemed to gain unauthorized access to the nationwide computer system used by

Lowe's Companies, Inc. and, after gaining access, to download and steal credit card account numbers from that computer system. In order to carry out this scheme, the defendants secretly compromised the wireless network at a Lowe's retail store in Southfield, Michigan, and thereby gained unauthorized access to Lowe's Companies, Inc.'s central computer system in North Wilkesboro, North Carolina and, ultimately, to computer systems located in Lowe's retail stores around the United States. Having gained this unauthorized access, the defendants then attempted to install and installed a computer program on the computer system of several Lowe's retail stores, which program was designed to capture the credit card information of customers conducting transactions with those stores.

SALCEDO, BOTBYL, and TIMMINS face maximum sentences of 170 years in prison if convicted on all counts. However, it is important to note that any sentence received upon conviction will be determined by the federal Sentencing Guidelines. Under the federal Sentencing Guidelines, the Court determines each defendant's actual sentence based upon a formula that takes into account the severity and characteristics of the offense and each defendant's criminal history, if any. Of course, defendants in criminal cases are entitled to a presumption of innocence, and the Government has the burden of proving all charges beyond a reasonable doubt.

U.S. Attorney Conrad credits the Charlotte office of the Federal Bureau of Investigation ("FBI") with leading the investigation that resulted in the filing of these charges. In addition, U.S. Attorney Conrad credits the Detroit, Michigan field office of the FBI for assisting in this investigation. The Government is represented in this

matter by Assistant U.S. Attorney Matthew T. Martens of the U.S. Attorney's Criminal Division in Charlotte.⁴

3.1.3 Alteration of Computer Data

Alteration of computer data is the part of unauthorized access because the actor will be doing something concerned with data in computer such as data rising, data abridge or data limit. The most data subject to alteration are important data or main data. Generally, the aim of alteration of data is computer fraud such as fraud by ATM (Automatic Teller Machine).

The important reason of computer fraud is the actor alters data to get an asset such as a bank officer altering salary, balance sheet or transfer money by electronic means.

The important reason of computer fraud is the actor will be altering data to get an asset such as a bank officer is alteration a salary, balance sheet or transfer money by electronic

Case study of computer fraud by credit card

Naim Hamud, a former graduate student in Florida has been charged with trying to fraudulently obtain credit cards on the Internet. He was released on \$25,000 bond.

⁴ U.S. Department of Justice, "Three Men Indicted for Hacking into Lowe's Companies' Computers with Intent to Steal Credit Card Information", November 20, 2003. In <http://www.cybercrime.gov/salcedoIndict.htm> , Access date June 19, 2005.

Hamud allegedly applied for 174 credit cards through the Internet using names of students at Nova Southeastern University that he had pulled from the computer system at the college, where he was studying at the time. Law enforcement officers were tipped off when several banking institutions realized the applications were all being sent to a post office box in Fort Lauderdale. No cards were issued.

If convicted, he faces a maximum penalty of up to five years in prison and a fine of up to \$250,000 US.⁵

San Jose Man Indicted for Theft of Trade Secrets and Computer Fraud

The United States Attorney's Office for the Northern District of California announced that Patrick J. Murphy, 43, of San Jose, California, was indicted today by a federal grand jury on six counts of Theft of Trade Secrets in violation of 18 U.S.C. § 1832, and one count of Computer Fraud in violation of 18 U.S.C. § 1030.

According to the indictment, Mr. Murphy stole trade secrets relating to computer code for designing computer chip features, and wireless computer networks specifications, from his former employers, Jasmine Networks, Inc., San Jose, California, and Silicon Wave Corporation, San Diego, California.

The maximum statutory penalty for each count in violation of 18 U.S.C. § 1832 is 10 years imprisonment and a fine of \$250,000. The maximum statutory penalty for the count in violation of 18 U.S.C. §

⁵ Patrick Meikle, "Ex-student charged with Net fraud", September 3, 1997. In <http://www.monitor.ca/monitor/issues/vol5iss1/netbytes.html>, Access date June 19, 2005.

1030 is 5 years imprisonment and a fine of \$250,000. However, any sentence following conviction would be dictated by the Federal Sentencing Guidelines, which take into account a number of factors, and would be imposed in the discretion of the Court. An indictment simply contains allegations against an individual and, as with all defendants, Mr. Murphy must be presumed innocent unless and until convicted.

The prosecution is the result of a investigation by agents of the Federal Bureau of Investigation. The investigation was overseen by the Computer Hacking and Intellectual Property (CHIP) Unit of the U.S. Attorney's Office. Matt Parrella is the Assistant U.S. Attorney in the CHIP Unit who is prosecuting the case. Both Jasmine Networks and Silicon Wave cooperated with the FBI in the investigation.⁶

3.1.4 Damage or Destruction Computer Data

Damage or destruction to computer data is one part of unauthorized access as well. The damage can occur by the data owner's ignorance or negligence so it's very important for the owners to set up a security standard of computer data. Although, it can't protect all the damages because the damages of computer data can be caused in many situations; for example, in some case, it's caused by officer exasperation or the causes of political, economic factors; however the most frequent cause is computer fraud. The damage or destruction of data is components of computer fraud. There are many ways to conduct it beginning with stopping the computer system or crashing the system, for unauthorized access of data to cause damage or

⁶ U.S. Department of Justice, "San Jose Man Indicted for Theft of Trade Secrets and Computer Fraud", April 2, 2003. In <http://www.cybercrime.gov/murphyIndict.htm>, Access date June 19, 2005.

destruction of computer data such as the data of creditor. In some case, the offenders' use some programs that are able to destroy a lot of money in short time, some programs can set up the time or condition to destroy data after the offenders get out of the computer system.

In some case, damage or destruction of computer data will cause damage to other assets such as computer, computer system or computer network. It's like a damage of physical asset so the criminal law can be applied on this offence because this is an Offence of Mischief under the Penal Code Section 358-360 of Thailand.⁷

Case study of Damage or destruction computer data

Former Employee of Viewsonic Sentenced to One Year for Hacking into Company's Computer, Destroying Data

A man previously employed at the Walnut office of the Viewsonic Corporation was sentenced today to one year in prison for hacking into the company's computer system and wiping out critical data, an act that shut down a computer server that was central to the company's foreign operations.

Andrew Garcia, a 39-year-old Montebello resident, was sentenced by United States District Judge John F. Walter. Garcia, who was the network administrator at Viewsonic's Walnut office where he was in charge of several computer servers and had access to system passwords, pleaded guilty in October to one count of accessing a protected computer and recklessly causing damage.

⁷ Phanu Rungsrisahut, "Commit a criminal offence: related computer", p.127.

On April 14, 2002, approximately two weeks after Garcia was terminated by Viewsonic, Garcia accessed the company's computer system and deleted critical files on one of the servers that he had maintained. The loss of these files rendered the server inoperative, and Viewsonic's Taiwan office was unable to access important data for several days. Viewsonic Corporation is a manufacturer of computer monitors that generates more than \$1 billion a year in revenues. The case against Garcia was investigated by the FBI.⁸

Former Employee of American Eagle Outfitters Indicted on Charges of Password Trafficking and Computer Damage

United States Attorney Mary Beth Buchanan announced today, February 26, 2003, that a resident of Greensburg, Pennsylvania, has been indicted by a federal grand jury in Pittsburgh on charges of Password Trafficking and Computer Damage.

The two-count indictment named Kenneth Patterson, age 38, of 615 Cherry Street, Greensburg, Pennsylvania, 15601.

According to the indictment presented to the court, Patterson, a former employee of American Eagle Outfitters, was charged with trafficking in passwords and similar information that would have permitted others to gain unauthorized access to the American Eagle Outfitters computer network, when Patterson posted and maintained at a Yahoo hacker group posting board the username and password combinations of certain legitimate American Eagle Outfitters users together with

⁸ U.S. Department of Justice, "Former Employee of Viewsonic Sentenced to One Year for Hacking into Company's Computer, Destroying Data", February 23, 2004. In <http://www.cybercrime.gov/garciaSent.htm>, Access date June 20, 2005.

detailed instructions on how to hack into the wide area network of American Eagle Outfitters using those passwords.

Patterson was also charged with a series of computer intrusions into the American Eagle Outfitters computer network from November 27, 2002 through December 1, 2002. These intrusions were attempts to deny computer services to American Eagle Outfitters stores in the United States and Canada during the beginning of the Christmas shopping season. These denials of service attempts were quickly identified by American Eagle personnel and corrective actions were implemented that limited their intended economic impact.

Assistant United States Attorneys Paul E. Hull and Luke E. Dembosky, who presented the case to the grand jury, indicated that the law provides for a maximum total sentence of 11 years in prison, a fine of \$350,000, or both. Under the Federal Sentencing Guidelines, the actual sentence imposed would be based upon the seriousness of the offenses and the prior criminal history, if any, of the defendant.

Agents from the High Technology Crimes Task Force conducted the investigation leading to the indictment in this case together with the invaluable cooperation and assistance of American Eagle Outfitters' staff and employees.

An indictment is only a charge and is not evidence of guilt. A defendant is presumed innocent and is entitled to a fair trial at which the government must prove guilt beyond a reasonable doubt.⁹

⁹ U.S. Department of Justice, "Former Employee of American Eagle Outfitters Indicted on Charges of Password Trafficking and Computer Damage", February 26, 2003. In <http://www.cybercrime.gov/pattersonIndict.htm> , Access date June 20, 2005.

3.2 The Problem of Data Protection in Thailand

3.2.1 Legal Problems

The existing laws cannot handle Computer Crime because Thai Criminal Code focuses on protecting the corporeal objects but most of the targets of computer crime are incorporeal objects combined with electromagnetic impulse, which are beyond the scope of the law. At present, the age of industry is changing to the age of Information Technology so the value of data is increasing. This is the important reason why the criminal law should be changed of paradigms from protecting only the corporal objects to protecting incorporeal objects as well.

Computer and Internet provide a new environment for the criminal to commit old crimes and also lead to new types of crimes through the new medium. Some existing laws may be able to be adapted to prosecute the criminals. However, the amendments and new law are necessary to clarify and strengthen the application. One of the principles of the criminal law is no punishment without law (*Nulla poena sine lege*)¹⁰.

The important problem for providing the law is a real scope of committing a criminal offence related with computer because it's very difficult to decide; there have 2 reasons as following;

- 1) The target of the crime does not dare to report that crime to the police because they are afraid of criticism of the public or afraid to disclose an insecurity of their own computer system
- 2) Public prosecutors hesitate to sue and the court as well, because the both groups are not experts or well versed with the

¹⁰ Kiatkajorn Watchanasawat, The Explanation of Criminal Law(Bangkok :Thamasart University Press, 1997),p.55.

information technology and it's very difficult to see the damages of the public from such offence.

Thai Law and Jurisdiction: The provisions on the jurisdiction in the Criminal Code can punish the criminals using the territorial principle, the universality principle, and the personality principle. In case that the computer-related crime was committed in the Kingdom, the criminals have Thai nationality or the offence is under the universality principle, there would not be a problem on the jurisdiction. However, as mentioned earlier, there are many cases that no country has a clear jurisdiction to the offences.

The above example about the unauthorized access that happens in one country but the affect happened in a company registered in another country while the victim or the injured party is in another different country. The section 5 of the Criminal Code focuses only on the affect of the offences occurred in the Kingdom or foreseeable that the affect of the offences would occur in the Kingdom. In many cases, it has no clear border that can determine the jurisdiction such as the offences of interfering or intercepting of the computer system¹¹, the target computer, in this case a server, although belonging to a Thai company, it can be in another country or a website that registered in another country.

The other law that can be applied is the Law of Civil Procedure section 4 ter. if the defendant has no domicile or resident in the Kingdom and the cause of the action is not arose within the Kingdom, the plaintiff that has Thai nationality or domicile within the Kingdom can submit the case to the Civil Court or the Court within the territorial jurisdiction of which the plaintiff is domiciled. With these provisions, I believe Thai law does not have many problems if Thailand has a

¹¹ Draft of Computer Crime in Thailand.

special law to enforce, but the actual concern is the difficulty of the investigation and obtaining of the evidences of the victims/injured parties of the crime.

As explained earlier, Computer crime exists in various forms. This research focuses on data security because nowadays the data have a lot of value especially the data of business and country. Most of them are secret data and are stored in computers because this is the age of information technology where every organization or country brings new technologies to facilitate their operations. Therefore, this is an opportunity and reason for the criminal to attack or hack in other's computers. Although, Thailand has criminal law to enforce but it's not sufficient to protect the public from computer crime, for example, the meaning of "Thing" (corporeal object) or "Property" (incorporeal object) are not provided in the Penal Code of Thailand therefore we must bring the meaning from Civil and Commercial Code sections 137,138. So this is the problem of interpretation because the Penal code use the word "Thing" it is a question whether the interpretation of the Penal code is combined with the meaning of Property or not, and this will be discussed in the next chapter.

However, Thailand has a draft of computer crime by the National Electronics and Computer Technology Center (NECTEC) which is now under the supervision of the Ministry of Information and Communication Technology (ICT). The office of the secretary of the National Information Technology Committee is now responsible for the draft. The draft is now under the consideration of the office of the Judicial Council and in the process of selecting the committee. There are some amendments to the first draft; the bill now has 17 sections instead of 13 and the definitions part is not yet finalized.

Moreover, the Minister of justice is concerned with the power of the police and authority to investigate the crime and on the international crime and terrorist issues. The law has to harmonize with the international law to prevent further problems.

3.2.2 Impacts to Economic

Most of businesses have used computer for storage and management of the general data, information, or secret information- trade secret. At the moment, the communication via computer is very popular because it can save cost and time. So, the internet is important for computer to transfer or communicate data between companies and organizations. Therefore, this is the opportunity for criminals to intervene by Stealing computer data, Computer sabotage, and Computer forgery etc. These offences are bringing lots of damage to the businesses and it has impact directly to the economy.

The damage incurred from theft of computer data is the first problem and very important because nowadays is the age of information technology the data inside computers, such as trade secret, balance sheet or personal information, have value. There are many kinds of theft, but every time of theft damage will be incurred and data owners will suffer from this offence. Many countries suffer from theft of computer data, especially, the data of banks it has occurred a lot of times in the society because of alteration or destruction of computer data. The crime is done directly on the cash, for example, the case study of US – Former Chase Financial Corp. employees sentenced for scheme to defraud Chase Manhattan Bank and Chase Financial Corporation; according to court document filed in the case, Turner and Williams each admitted that between approximately November 1999, and on or about December 12, 2000, in the Northern District of Ohio, Eastern Division, while employed by Chase Financial Corporation,

1500 W. 3rd Street, Cleveland, Ohio, they knowingly and with the intent to further a scheme to defraud Chase Manhattan Bank and Chase Financial Corporation, accessed one or more Chase Manhattan Bank and Chase Financial Corporation computer systems without authorization or in excess of their authorized access on said computer systems, thereby obtaining credit card account numbers and other customer account information pertaining to approximately sixty-eight (68) accounts, which they were not authorized to access in connection with their duties at Chase Financial Corporation. Turner and Williams admitted that the aggregate credit limits for the targeted accounts totaled approximately \$580,700.00. Turner and Williams further admitted that after fraudulently obtaining said credit card account numbers and customer account information, they distributed and transmitted said financial information to one or more individuals located in the Northern District of Georgia via facsimile transmission, who, in turn, used the credit card accounts and other financial information to fraudulently obtain goods and services valued at approximately \$99,636.08, without the knowledge or consent of the account holders, Chase Manhattan Bank or Chase Financial Corporation.

Next, case is Six Internet Fraudsters Indicted In International Conspiracy To Steal More Than \$10 Million From World's Largest Technology Distributor, Mateias began hacking into Ingram Micro's online ordering system in 1999. Using information obtained from his illegal hacking activity, Mateias bypassed Ingram's online security safeguards, posed as legitimate customers and ordered computer equipment to be sent to Romania. When Ingram Micro blocked all shipments to the Eastern European country in early 1999, Mateias recruited Tinubu, Crisovan, Long and Bailey from Internet chat rooms to provide him with United States addresses to use as "mail drops" for the fraudulently ordered equipment. Crisovan, Tinubu, Finley and

Long, in turn, recruited others, including high school students, to provide additional addresses and to accept the stolen merchandise.

Case Study

1) Case of “Thailand.com”¹²

In fact, the offender used the name “Sonya Lukthai” to commit an offence by the first, the offender send new information to Internet Network Information Center (InterNic) – organization of Network Solution Incorporation (NSI) in US for set up an IP for member, because the offender want to change phone number and address for cancel to call back and use old name. Next, the offender told to InterNic about them already to buy a domain name from owner so they want to change to a new name “Sonya Lukthai” and new address after that they set up a “Thailand.com” to the domain name. Therefore, the owner protested about this offence but the offender asserted to owner that the offender buy this domain name from owner so if the owner want this domain return they should be buy in 5 million baht.

Therefore, the owner must be close web-site around 1 month and show evidence to confirm with InterNic that they are owner so this offence is bringing damage to the owner.

2) Case of “Stolen Examination”¹³

In fact, the teacher in University saves textbook, Examination and answer in computer of him in private room. The problem occurred because he connects to the internet by use LAN

¹² Mana Savangjit and others, “Computer Crime” (Master’s Thesis, Assumption University, 2003), p. 3.

NETWORK of university so the offender hacking and stole any data of him.

3) Case of “Ebay.com”,¹⁴

Website ebay.com is a famous website that related with a bid. Every people can buy or sell the goods in this website. In case, Thai people want to buy a television that the American people are announce to buy. Next, Thai people is winner to bid this television and he transfers money 266,000 baht to pay television. After that, he receives parcel post from Fedex but it's not a television, it's just a big doll and glassware.

3.2.3 Impact on Society

Nowadays, most people own computer because computer is new technology. People can use the computer to search information, send/receive email, post picture/massage to the web board or chat. So, if some people use the computer to commission of an offence. It is very difficult to arrest the actor to penalty because it does not appear the actors and little evidence such as insult on internet, post obscene picture. It is very easy and speedy to do this offence. The important, it is spread speedy to the public.

Some personal information, the owner didn't want to disclose to the public but It's has some people want to know. So, this is the cause of hacking and thief of computer data because this data is benefit for criminal and if this information is disclose to the public, the reputation of data owner receive will be damaged. For example, medical record. Because the medical record is concern about the healthy of each person

¹³ Ibid., p.4.

¹⁴ Ibid., p.4.

so the doctor uses medical record when they come to the hospital. But the criminal want to disclose to the public because the criminal want to discredit of data owner such as if the owner has been a nervous and this data is disclosed to the public. This data will destroy a belief in Society.



Chapter 4

Computer Crime Relate with Data Protection in US and Thailand

4.1 The US Computer Crime Law

: Related with Data Protection

4.1.1 Statutes of US Computer CRIME

The computer crime of United States of America is very modern because America is a leader of technologies so the law must follow the crime. Therefore, Thailand adapts the computer crime of America as the pattern law. America has developed technologies before Thailand more than 10 years and America has adapted or changed throughout the law so the computer crime law of America is the most modern.

The United States of America have legislated a computer crime statute at the first time since 1984; there have been computer-related laws such as The Counterfeit Access Device and Computer Fraud and Abuse Act of 1984. The aim of these laws is to resolve the computer crime because the United States have suffered and lost a lot of money due to computer crime. Therefore, every state in the United States has passed a computer crime statute. These state statutes vary from each other of the states, and this research will focus on federal computer crime legislation.

At least 40 federal statutes impose criminal penalties for computer and internet frauds or other illegal activities. Several federal statutes have been passed in specific response to criminal activity on the Internet and by computers.

There are many federal statutes in the USA that can be used to prosecute computer criminals¹

State Statutes in USA

There is wide variation in state statutes² on computer crime in the USA: in the researcher's opinion, most state statutes are *not* adequate to punish computer criminals.

¹-15 USC § 1644, prohibiting fraudulent use of credit cards

- 18 USC § 1029, prohibiting fraudulent acquisition of telecommunications services
- 18 USC § 1030, prohibiting unauthorized access to any computer operated by the U.S. Government, financial institution insured by the U.S. Government, federally registered securities dealer, or foreign bank.
- 18 USC § 1343, prohibiting wire fraud
- 18 USC § 1361-2, prohibiting malicious mischief
- 18 USC § 1831, prohibiting stealing of trade secrets
- 18 USC § 2314, prohibiting interstate transport of stolen, converted, or fraudulently obtained material; does apply to computer data files *U.S. v. Riggs*, 739 F.Supp. 414 (N.D.Ill 1990).
- 18 USC § 2319 and 17 USC § 506(a), criminal violations of copyright law
- 18 USC § 2510-11, prohibiting interception of electronic communications
- 18 USC § 2701, prohibiting access to communications stored on a computer (i.e., privacy of e-mail)
- 47 USC § 223, prohibiting interstate harassing telephone calls

² California, Minnesota, and Maine are among the few states to prohibit explicitly release of a computer virus or other malicious program.

California Statutes, Title 13 (Penal Code), §§ 502(b)(10) and 502(c)(8).

Minnesota Statutes, §609.87(12) and §609.88(1)(c).

Maine Statutes, 17-A (Criminal Code), § 433(1)(C).

In states without an explicit statute, release of a malicious program would probably be

The primary federal statute applicable to hacking, cracking, and unauthorized computer use is the Computer Fraud and Abuse Act (CFAA). Congress amended CFAA several times as they came to grips with the extent of unauthorized electronic activity and technical change. Congress passed the original CFAA in 1984. In the legislative history, legislators expressed a strategy of regulating limited subject areas that were widely recognized as sensitive and essential matters for protection from intrusion. They did so in order to move cautiously in an area of law and technology that was just beginning to develop.

This approach is in line with the philosophy adopted later in the U.S. framework for Electronic Commerce. First, the legislation only protected “federal interest” computers and those banking computers covered under the 1978 Right to Financial Privacy Act and the Fair Credit Reporting Act.

The Act applied to three situations. It made it a felony (Subject to prison time) to knowingly access these computer in order to harm the interests of the United States. It was a misdemeanor (lesser crime) to knowingly access a financial file to obtain consumer information or to access a government computer in order to interface with its operation or change information. Because of its limited application, the law was ineffective. In 1986 the Act was amended and broadened to include any computer that is used in interstate commerce. Additional amendments were made in 1989, 1990, 1994, and again in the National

prosecuted as "malicious mischief".

California also provides for the forfeiture of computer systems used in the commission of a computer crime. If the defendant is a minor, the parents' computer system can be forfeited.

California Statutes, Title 13 (Penal Code), §§ 502(g) and 502.01(a)(1)

Information Infrastructure protection Act of 1996, resulting in any computer connected to the internet, whether in multiple state or not, being subject to the coverage of the Act.

In its present form, the CFAA prohibits the unauthorized access or access in excess of authorization to various government and nongovernmental protected computer. Criminal actions under the CFAA include:

- 1) Access to and transmission of government classified information
- 2) Access to computers used in interstate commerce
- 3) International access of a government nonpublic computer
- 4) Knowingly accessing and intentionally causing damage to a protected computer (through code, hacking, etc.)
- 5) Intentionally accessing a computer without authorization and causing damage (a \$5,000 minimum within 1 years for a felony conviction)

4.1.2 Liability of Computer Crime-Related Data Protection of United State of America

The Computer Fraud and Abuse Act of 1986 of United States has divided commit an offence that occur with computer data in 3 type

1) Unauthorized Access

Unauthorized access is emerging in many jurisdictions as the threshold offence in the field of computer crime. This is not at all surprising, since access is the fundamental factual predicate for anything else that can be done with a computer. In any event, unauthorized access appears to be the basic building

block of most other computer crimes. It is the "least included offense" in a hierarchical series of crimes that become progressively more serious as aggravating harms and culpability states are added to the base offense.

The Computer Fraud and Abuse Act of 1986 of United States are providing the offence of unauthorized access in Section 1030 (a)³. It is concerned about a computer fraud and the act

³ Computer Fraud and Abuse Act 1986 (US) 18 USC 1030(a). Fraud and related activity in connection with computers

(a) Whoever—

- (1) knowingly accesses a computer without authorization or exceeds authorized access, and by means of such conduct obtains information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph r. of section 11 of the Atomic Energy Act of 1954, with the intent or reason to believe that such information so obtained is to be used to the injury of the United States, or to the advantage of any foreign nation;
- (2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);
- (3) intentionally, without authorization to access any computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects the use of the Government's operation of such computer;
- (4) knowingly and with intent to defraud, accesses a Federal interest computer without authorization, or exceeds authorized access, and by means of such conduct

that is related with a computer. The main point is the actor has “act” and “Intent” to unauthorized- access or didn’t conduct the act within the scope of one’s authority.

3) Alteration

The term 'alteration' means the modification of existing data. The input of malicious codes, such as viruses and Trojan horses is, therefore, covered under this paragraph, as is the resulting modification of the data.

The US law is providing this offence:

Alteration offence is a one of criminal offences that the US law provides in the Computer Fraud and Abuse Act 1986. It covers the alteration of computer, computer system, computer network

further the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer;

(5) intentionally accesses a Federal interest computer without authorization and by means of one or more instances of such conduct alters, damages, or destroys information in any such Federal interest computer, or prevents authorized use of any such computer or information, and thereby—

(A) causes loss to one or more others of a value aggregating \$1,000 or more during any one year period; or

(B) modifies or impairs, or potentially modifies or impairs the medical examination, medical diagnosis, medical treatment, or medical care of one or more individuals; or

(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if—

(A) such trafficking affects interstate or foreign commerce; or (B) such computer is used by or for the Government of the United States;

shall be punished as provided in subsection (c) of this section.

and program/data of computer. The reason the US law provides the alteration offence separate from unauthorized access is that the alteration offence is concerned with the offence of document forge. Therefore, the US government provides this law to protect against all offences that involve with alteration

4) Damage or Destruction

Damage or destruction means some people making a damage or destruction in the program or data of computer; program or data of computer are intangible. There are object of damages that are resulted from this offence, they are computer hardware or accessory of computer. The US law holds that the offences of criminal offences related with computer, being separate from the offence of mischief, are provided in the Computer Fraud and Abuse Act 1986 Section 1030(a) (5) after that in 1994 was amended this Section in 2 parts.⁴

⁴ 5. Through use of a computer used in interstate commerce, knowingly causing the transmission of a program, information, code, or command to a computer system. There are two separate scenarios:

a. In this scenario, (i) the person causing the transmission intends it to damage the computer or deny use to it; and (ii) the transmission occurs without the authorization of the computer owners or operators, and causes \$1000 or more in loss or damage, or modifies or impairs, or potentially modifies or impairs, a medical treatment or examination.

The most common way someone gets into trouble with this part of the law is when trying to cover tracks after breaking into a computer. While editing or, worse yet, erasing various files, the intruder may accidentally erase something important. Or some command he or she gives may accidentally mess things up. Yeah, just try to prove it was an accident. Just ask any systems administrator about giving commands

4.2 The Law and Security Measure of Computer Data in Thailand

4.2.1 Nature of Thai Law

At present, Thailand has developed and accepted new technology because technologies are very important to develop the country. Technologies are directly concerned with business, government and sociality; especially, technologies of computer system and computer network. When people are interested in using computer, the developments of crime are occurring at the same time with the development of technologies. This is a new crime for Thailand so the law does not cover the computer crime.

as root. Even when you know a computer like the back of your hand it is too easy to mess up.

A simple email bomb attack, "killer ping," flood ping, syn flood, and those huge numbers of Windows NT exploits where sending simple commands to many of its ports causes a crash could also break this law. So even if you are a newbie hacker, some of the simplest exploits can land you in deep crap!

Penalty with intent to harm: Fine and/or up to 5 years in prison, up to 10 years if repeat offense.

b. In this scenario, (I) the person causing the transmission does not intend the damage but operates with reckless disregard of the risk that the transmission will cause damage to the computer owners or operators, and causes \$1000 or more in loss or damage, or modifies or impairs, or potentially modifies or impairs, a medical treatment or examination.

This means that even if you can prove you harmed the computer by accident, you still may go to prison.

Penalty for acting with reckless disregard: Fine and/or up to 1 year in prison.

4.2.2 Penal Code

Basically, Thai criminal justice stems from the civil law oriented system. Therefore, all legislation is codified in the form of “Code” or “Act”.

In general, the criminal law is provided to enforce on the people who are against to the society. So, this law concentrates on any action such as larceny, offence of mischief, and offence against life or body. The criminal law is not provided to prosecute the offenders to use implement in criminal offense. For example, the law is not providing to enforce in the case of setting fire and criminal law does not provide to enforce in the case of stealing computer business data stored inside the computer. Therefore, Thailand has not the penalty to enforce on these offenders; especially, the criminal code does not provide to punish the offenders stealing computer data.

4.3 The Problem of Computer Crime in Criminal Law

4.3.1 Offence of Theft

Offences of theft, under the criminal law section 334⁵ there are two issues to consider. The first is meaning of “things” because in criminal code of Thailand there is not provided the meaning of things so when we adjudicate about *what is the things* we need to use the civil and commercial code of Thailand that provides the meaning as a corporeal object. Since the computer data are not corporeal objects so we cannot apply this word in criminal code. The second is the meaning of “take

⁵ Section 334 – whoever dishonestly takes away a thing belonging to another person or of which another person is a co-owner is said to commit theft, and shall be punished with imprisonment not exceeding three years and fine not exceeding six thousand baht.

away”, because the Supreme Court gives the standard of the Offences of theft in 2 ways. The first is disseisin and the second is moving of things.

However, the interpretation on problem of the word “Things” and “Property” in the criminal offence has been judged in the cases such as the decision of Supreme Court No. 887/2501 about that stealing the electricity is the offence of theft under the Penal Code section 334,335; but some lawyers don’t agree with this decision and they say that the electricity is an energy and incorporeal object. So, it is not a “Things” because electricity is moving through wire and it’s a source of energy such as heat, light or sound. Although, the energy have a weight but in physical science it is not referred about the electricity as a matter but it’s referred only as energy so the electricity isn’t a corporeal object.

Therefore, the decision of Supreme Court No. 887/2501 about the offence of stealing electricity as a part of the offence of theft under the Penal Code and it’s like a comparison with the law that is unfavorable to the defender. So, it’s in conflict with the general rule of criminal law.

After that, in the decision of Supreme Court No. 5354/2539 about the offence of stealing mobile phone wave, the plaintiff in this case sues the defendant in the offence of theft. The Court of first instance and appeal court are holding the Supreme Court No. 5354/2539 but the Supreme Court in this case does not agree with above decision and they decide a defendant to be exonerated from the offence of theft because they said that the act of defendant is only unauthorized use of mobile phone wave of other people and it is not a “take away dishonestly”; so, the act of defendant is not illegal in the offence of theft under the Penal Code section 334.

Although, the computer data can be moved by some instrument but the computer data can't be a thing or property. A thing or property has an exclusive right but computer data cannot be protected from disturbance and computer data can be moved by nature. Therefore, computer data are not things and cannot be stolen from a possession so we can't bring the criminal code (Offences of theft) to apply with computer data.

4.3.2 Offence of Criminal Misappropriation

Offence of Criminal Misappropriation, under section 352⁶ of criminal code of Thailand have two components to consider, the first is "Misappropriation" it has the same meaning as "take away" in Offence of theft. So, referring to the Offence of theft we can't bring this section to apply in charging of Offence of Criminal Misappropriation.

4.3.3 Offence Relating to Counterfeiting and Alteration

Offence Relating to Counterfeiting and Alteration, under the criminal code section 264⁷ states that Counterfeiting document means making

⁶ Section 352-Whoever, being in possession of a property belonging to the other person, or of which the other person is a co-owner, dishonestly converts such property to himself or a third person is said to commit misappropriation, and shall be punished with imprisonment not exceeding six thousand baht, or both.

If such property comes under the possession of the offence on account of being delivered to him by other person by mistake by any means whatever, or being a lost property found by him, the offence shall be liable to one half of the punishment.

⁷ Section 264-Whoever, in a manner likely to cause injury to another person or the public, fabricates a false document or part of a document, or adds to takes from or otherwise alters a genuine document by any means whatever, or puts a false seal or signature to a document, if it is committed in order to make any person to believe that it is a genuine document, is said to forge a document, and shall be punished with imprisonment not exceeding three years or fine not exceeding six thousand baht, or both.

addition or substance suppressing or amending in the genuine document. Although, counterfeiting and alteration of document can be done to computer data but the computer is not only object because of technologies in this time the actor can counterfeit and alterate data in transfer without amending anything directly to the data.

4.3.4 Offence of Mischief

Offence of Mischief, under section 358⁸ of the criminal code section 358 provides the Offence of Mischief to consider the computer data not an intangible property as immovable realty but their are some differences. It is that realty cannot be destroyed but computer data can be destroyed so this is the problem whether if the computer data can be destroyed it will be an Offence of Mischief or not.

Regarding this issue, there is no any Court decision; but if in future the Supreme Court decides that this act is not an Offence of Mischief, we cannot bring the Offence of Mischief to apply in the case of computer data offences. On the other hand, if the Court has decided that this act is an Offence of Mischief, it will be in conflict with intention of law and principle of criminal law.

Whoever fills in the contents on a sheet of paper or any other material bearing the signature of another person without the consent or by violating the order of such person, if it has committed in order to take such document for use in any activities which may cause injury to any person or the public' shall be deemed to forge a document, and shall be punished likewise.

⁸ Section 358-whoever damages, destroys, causes depreciation in value, or renders useless a property belonging to the other person, or of which the other person is a co-owner is said to commit mischief, and shall be punished with imprisonment not exceeding three years or fine not exceeding six thousand baht, or both.

Chapter 5

Conclusion and Recommendation

5.1 Conclusion and Recommendation

Thailand has entered the era of information technology society. Computer and Internet have become more and more important to our daily life. The dynamic nature of the computer technology can bring not only the benefit and convenience to the society but also can facilitate new crimes. It is important for the lawyers and the society to understand the problems that arise from the computer-related crimes and help preventing the possible problems.

Computer crime has many patterns so the committing of offences related to computer data is one of computer crimes. To find the measure to prevent such acts, it is necessary to have knowledge of Information Technology which consists of the process of computer, communication and information system. Therefore, we ought to understand the statutes or methods for committing offences with computers. The meaning of computer crime that I can conclude is the committing of offences by tort with criminal law; so if an offender has intent to commit offences to computer data, it will be deemed a crime and it is a one of Economic crime

The offences of computer data have many patterns and it can be divided as the following;

- 1) Unauthorized Access and Exceeding Authorized Access can be divided into 2 groups. The first is committing without vile intent, almost all of this offences are committed by students who want to show off or challenge their ability. The second is committing with vile intent because the aim is access to destroy the system, data or stop computer process.

2) Duplicate computer data

The aim of this offence is espionage of the data especially, for example, secret data, finance data or Industry data like making an unauthorized access to the computer data or copying a credit card number for selling or destroying a computer data.

3) Alteration computer data

The aim of this offence is fraud. The alteration can be done in each part of computer system. In some steps of this offence the criminals do not need computer knowledge; it's just having a chance to access to the data and alliterating them; but in some steps, the criminal must have special knowledge of computer to make alteration, for instance, they can create a program to alterate data or to access to the data.

4) Damage or destruction computer data

The main objective of this offence is to make damages to computer data and the cause is due to employee angry with the company, but the main cause is fraud. The virus is one cause of damage or destruction of computer data but it's different from virus because the virus can make a wide-ranging damage or even destroy all of system.

The Computer Fraud and Abuse Act (CFAA). Congress amended CFAA several times as they came to grips with the extent of unauthorized electronic activity and technical change. Congress passed the original CFAA in 1984. In the legislative history, legislators expressed a strategy of regulating limited subject areas that were widely recognized as sensitive and essential matters for protection from intrusion.

The Computer Fraud and Abuse Act (CFAA) has divided commit an offence that occur with computer data in 3 type

1) The offence of Unauthorized Access

The offence of unauthorized access is considered in many jurisdictions as the threshold offence in the field of computer crime. This is not at all surprising, since access is the fundamental factual predicate for anything else that can be done to or with a computer. In any event, unauthorized access appears to be the basic building block of most other computer crimes. It is the "least included offense" in a hierarchical series of crimes that become progressively more serious as aggravating harms and culpability states are added to the base offense.

2) The offence of alteration

Alteration means the modification of existing data, the input of malicious codes, such as viruses and Trojan horses is, therefore, covered under this paragraph, as they result in modification of data.

3) The offence of Damage or Destruction

Damage or destruction means some people make damages or destruction to the computer program or data and computer program or data that are intangible. There are objects that are involved in this offence; they are computer hardware or accessory of computer.

USA is a leader in information technology, so US are providing a Computer Crime Law to enforce in the area of computer crime rather than amending the existing law. For this reason, the USA has realized the problems and pay attention to this crime.

The criminal law of Thailand is not sufficient to protect and resolve the problems of computer crimes, for example the offence of theft, under the

criminal law section 334 does not provide the meaning of things that can be applied to the offence of theft; so we use the civil and commercial code of Thailand that provide “a thing” as a corporeal object. However, the computer data are not corporeal objects so we cannot bring this word of criminal code to apply in the case that occurred with computer data. Although the Supreme Court No. 887/2501 judgment that stealing the electricity is an offence of theft under the Penal Code section 334,335 but some lawyers don’t agree with that decision and they say that the electricity is energy and incorporeal object. So, it is not a “Thing” because electricity move by wire and it’s a source of energy such as heat, light or sound. Although the energy has weight but in physical science it is not stated that electricity is matter but it states only it is a kind of energy so the electricity isn’t a corporeal object. Therefore, the decision of Supreme Court No. 887/2501 about the Supreme Court’s deciding the offence of stealing electricity as a part of the offence of theft under the Penal Code. So, it’s in conflict with the general rule of criminal law.

After that, according to the decision of Supreme Court No. 5354/2539 about the offence of stealing mobile phone wave, the act of defendant is only unauthorized use of a mobile phone wave of other people and it is not a “take away by dishonestly”. So, the act of defendant is not illegal in the offence of theft under the Penal Code section 334.

Although, the computer data can move by using instruments but the computer data cannot be a thing or property because computer data is not subject to an exclusive right while a thing or property is subject an exclusive right but computer data can’t be protected by the right from disturbance and computer data can move by nature. Therefore, computer data is not a thing and can’t be stolen from a possession so we can’t bring the criminal code (Offences of theft) to apply with computer data.

Now, the new technologies are rapidly developed so the law should also cover the computer offences. Although, at present Thailand has draft of computer

crime but this draft is only the first series of the country computer related laws and to enforce them effectively there need more laws to be enacted and amended. However, there are many problems that could arise when it comes into enforcement either from the law itself or from other relevant laws.

Nevertheless, even the best and strict laws cannot solve all the cyber-crime problems. Both the government and private sectors have to be ready for the new laws and regulations. The co-operation between the public and private sectors is needed to enable the effective solution.

After analysis, it is found that the criminal law of Thailand is not sufficient to protect and resolve the problems of computer crime so the researcher would like to suggest some solutions for this problem.

Thailand government should set up a preventive measure, in each organization there should be a security system of the computer system. There are many measures to prevent the crime as the following;

It is needed to set up the measure of policy and administration for limiting power or responsibility. There should be power balance of figure or important work and control by the management team, especially, to set up a penalty to enforce with the people who break the rule. Especially, the government should legislate a special law and should be flexible because the offence of this crime involves with technology and the improvement of technology is very fast so if special law is inflexible to enforce, it cannot follow with this offence.

Currently, Thailand has a draft of computer crime by the National Electronics and Computer Technology Center (NECTEC) and now it is under the supervision of the Ministry of Information and Communication Technology (ICT). The office of the secretary of the national information technology committee is now responsible for the draft. The draft is now under the consideration of the office of the Judicial Council and in the process of

selecting the committee. There are some amendments to the first draft; the bill now has 17 sections instead of 13 and the definitions part is not yet finalized. In this draft, it is providing against the offences as follows;

- (1) Unauthorized Access to information system
- (2) Computer interception
- (3) Computer espionage
- (4) Computer sabotage
- (5) Computer forgery
- (6) Computer fraud
- (7) Propagate the obscene picture

However, in some parts of the draft it does not cover the offence of Gambling and Cyber Stalking. So, it ought to revise and add up this offence to this draft.

It is recommended to set up a measure of technical such as the physical protection for storing and keeping data of computer to prevent them from the people who come in by unauthorized access and to set up a measure of Access, for example, identifying users with passwords or control by biological feature such as check of finger print, sound or retinas of the users, but these methods do not protect all of the offences because they are only simple methods of protection.

Bibliographies

Books

- Janine Hiller, S., and Ronnie Cohen. Internet Law & policy .New Jersey: Pearson Education, 2002.
- Kiatkajorn Watchanasawat. The Explanation of Criminal Law.Bangkok :Thamasart University Press, 1997.
- Maritn Wasik. Crime and the Computer .Oxford: Clarendon Press,1991.
- Chavarit Artasart. Cyber Law.Bangkok: Provision, 2455.
- Bryan A. Garner, Black's law dictionary. St.Paul, Minn.,2001.
- Ulrich Sieber. Legal Aspect of Computer –Related Crime in the information Society. vol. 1, 1998.
- Carl Benson.Computer Crime .Bloomington,Indiana University, 1997.
- OECD. Computer-related Crime : Analysis of Legal Plolicy.OECD: Paris,1986.
- John T.Soma.Computer Technology and Law.USA:Colorado,1993.
- Chitti Thingsapat. Explanation of Criminal Law section 2 and 3.Bangkok:Thai Bar Association,2532.

Thesis

- Pornchai Reawpatanapong. Virus Computer. Master's Thesis, Graduate School, Chulalongkorn University,2004
- Phanu Rungseesahus. The Commit an offence: Related Computer Crime, Master's Thesis, Graduate School, Chulalongkorn University,2533
- Rertlug Parnlerd. Computer Crime, Master's Thesis, Graduate School, Chulalongkorn University,2531
- Buncha Lertbunnapong. Thailand Computer Crime Bill. Master's Thesis, Graduate School,Chulalongkorn University, 2004.
- Gristsana Changgom. Computer Crime in European Union .Research, European University, 1999.
- Mana Savangjit and others.Computer Crime .Master's Thesis, Graduate School ,Assumption University, 2003.

Magazines and Journals

- Jittapatt Kruawann.Lersan Tanasukarn and Sudham Unaidham. Law Relating to Internet Service in Thailand. Nectec Journal (July 1998):pp.42-47.
- Chaiyuth Limlawan. Attack and Protection of Hacker.Nectec Journal (July2002):pp. 6-13.

Internet

- National ICT Security and Emergency Response Centre. Is cyber crime reigning on a no man's land. In http://www.niser.org.my/resources/no_man_land.pdf.
- Surin A.J. To catch a cyber criminal, 2003.In <http://www.crime-research.org/articles/cybercriminal>.
- Computer crime research center.Latest Cyber stalking Statistics Released. In <http://www.crime-research.org/news/2003/04/Mess2301.html>.
- Dave Pettinari. Cyber stalking investigation and prevention . In <http://www.crime-research.org/library/Cyberstalking.html>.
- International review of criminal policy. In <http://www.uncjin.org/Documents/EighthCongress.html>.
- Computer crime. The Draft Of Computer Crime. In <http://www.ictlaw.thaigov.net/>.
- Rachael Kenders. Computer Crime-Laws, Regulations, & Today's Issues,2002. In <http://www.personal.psu.edu/users/a/a/aaw136/ist432/>.
- Karen Eder. Defining Computer Crime and Technology Misuse. In <http://lrs.ed.uiuc.edu/wp/crime/definition.htm>.
- Delving Into Computer Crime . In <http://www.wowessays.com/dbase/ab2/nyr90.shtml>
- Ronald B. Standler.Computer Crime ,2002. In <http://www.rbs2.com/ccrime.htm>.
- Stein Schjolberg. Unauthorized Access To Computer Systems, 2003. In <http://www.mosstingrett.no/info/legal.html>.

- HyperText Transfer Protocol. Wikipedia, the free encyclopedia, 2005. In <http://en.wikipedia.org/wiki/> .
- Broadly.Computer Crime-Laws, Regulations, & Today's Issues,2002.In <http://www.personal.psu.edu/users/a/a/aaw136/ist432/> .
- Bowen Mace, Compute Crime.In <http://www.wowessays.com> .
- U.S. Department of Justice.Chardon.Ohio Woman Sentenced for Computer Fraud via Unauthorized Access of Employer's Computer System, December 14, 2001. In <http://www.cybercrime.gov/brownSent.htm>.
- U.S. Department of Justice, Chardon.Woman Charged for Unlawful Access to Computer Server, July 6 , 2001. In <http://www.cybercrime.gov/BrownIndict.htm>.
- U.S. Department of Justice.Three Men Indicted for Hacking into Lowe's Companies' Computers with Intent to Steal Credit Card Information, November 20, 2003. In <http://www.cybercrime.gov/salcedoIndict.htm>.
- Patrick Meikle, Ex-student charged with Net fraud, September 3,1997. In <http://www.monitor.ca/monitor/issues/vol5iss1/netbytes.htm!>.
- U.S. Department of Justice. San Jose Man Indicted for Theft of Trade Secrets and Computer Fraud, April 2, 2003. In <http://www.cybercrime.gov/murphyIndict.htm> .
- U.S. Department of Justice.Former Employee of Viewsonic Sentenced to One Year for Hacking into Company's Computer, Destroying Data, February 23, 2004. In <http://www.cybercrime.gov/garciaSent.htm>.
- U.S. Department of Justice. Former Employee of American Eagle Outfitters Indicted on Charges of Password Trafficking and Computer Damage, February 26, 2003. In <http://www.cybercrime.gov/pattersonIndict.htm>.

