A TRANSATLANTIC AGENDA

EU/US Co-operation for Preventing Computer Related Crime

TRANSATLANTIC AGENDA

With financial support from the TRANSATLANTIC AGENDA Programme

European Commission

Edited by
Ernesto U. Savona
Shawna Gibson
Daria Angelini

TRANSCRIME

IN COOPERATION WITH:
ERASMUS UNIVERSITY OF ROTTERDAM SCHOOL OF LAW (ROTTERDAM, NETHERLANDS)

UNISYS BELGIUM SA (BRUSSELS, BELGIUM)

UNIVERSITY OF PITTSBURGH'S EUROPEAN UNION CENTER (EUC) (PITTSBURGH, USA)

THE MATHEW B. RIDGEWAY CENTER FOR INTERNATIONAL SECURITY STUDIES, UNIVERSITY OF PITTSBURGH (PITTSBURGH, USA)

CERT®/CC AT CARNEGIE MELLON UNIVERSITY (PITTSBURGH, USA)

UNIVERSITÀ DEGLI STUDI DI TRENTO

UNIVERSITÀ CATTOLICA DEL SACRO CUORE

A TRANSATLANTIC AGENDA

EU/US Co-operation for Preventing Computer Related Crime

FINAL REPORT

EXECUTED BY

TRANSCRIME

IN COOPERATION WITH

ERASMUS UNIVERSITY OF ROTTERDAM SCHOOL OF LAW (ROTTERDAM, NETHERLANDS)

AND

UNISYS BELGIUM SA (BRUSSELS, BELGIUM)

AND

UNIVERSITY OF PITTSBURGH'S EUROPEAN UNION CENTER (EUC) (PITTSBURGH, USA)

AND

THE MATHEW B. RIDGEWAY CENTER FOR INTERNATIONAL SECURITY STUDIES, UNIVERSITY OF PITTSBURGH (PITTSBURGH, USA)

AND

CERT®/CC AT CARNEGIE MELLON UNIVERSITY (PITTSBURGH, USA)

FOR THE

EUROPEAN COMMISSION

WITH FINANCIAL SUPPORT FROM THE TRANSATLANTIC AGENDA PROGRAMME
EUROPEAN COMMISSION

Università degli Studi di Trento

October 2002

Transcrime Reports n.5

TABLE OF CONTENTS

References and Resources

ACKNOWLEDGEMENTS

This study has been directed by Ernesto U. Savona, Professor and Director of Transcrime – University of Trento. It has been managed by Shawna Gibson with the help of Daria Angelini and the other Transcrime staff.

Many people have made this project possible. The top of list would clearly be those who work for the European Commission who we gratefully acknowledge for their patience and understanding with this difficult project: Eric Hayes, Chris Kendall, and Arja Kilpelainen. We would also like to thank Luigi Soreca of the European Commission for helping formulate the project as well providing critical feedback during the conference in Pittsburgh.

We are indebted to Alberta Sbragia, Lauren Skrabala, Margaret Butler, Stephen Salas, and Gemma Marolda from the European Union Center for their attention to detail and making the conference a success. We would like to express our special thanks to Alberta Sbragia for having the ability to know what we wanted even if it was not always said in so many words.

Our sincerest gratitude goes to all of the people who participated and presented at our conference in Pittsburgh:

- Fred Cohen – *Research Professor at University of New Haven President – Fred Cohen & Associates*
- Nicola Dileone – *Europol*
- Casey Dunlevy – *CERT®/CC*
- Albrecht Funk – *Research Associate, European Union Center*
- Kimberly Kiefer – *U.S. Department of Justice*
- Dan Larkin – *Federal Bureau of Investigation*
- Howard Lipson – *CERT®/CC*
- Dinos Stasinopoulos – *European Union Fellow, European Union Center*
- James Breckenridge – *Mercyhurst College*

We would like to express our deepest gratitude to Kyo Oliver – *U.S. Secret Service* for providing a list of people who would be willing to fill out our questionnaire and provide useful feedback.

- Donald Rebovich – *Utica College*
- George E. Curtis – *Utica College*
- Gary Gordon – *Economic Crime Investigation Institute*
- Dan Ryan – *Attorney at Law*

Very special thanks go to Rosilyne Borland for editing various parts of the report and providing critical feedback to make the final product better.

We are particularly grateful to all the partners and who have worked so hard on this project. A special thank you goes to Ann Mennens and the people at Unisys for all their hard work and patience.

Phil Williams would like to express his appreciation to Tom Longstaff and Timothy Shimeall for many of the ideas and arguments contained in his section – computer as target – particularly in relation to the flow of activities in criminal acts targeting computers. Tim also read the paper and offered some critical and helpful insights. In addition, he would like to thank Casey Dunlevy, who helps to provide a stimulating and congenial environment in which to work.

EXECUTIVE SUMMARY

This report represents the completion of all the outlined tasks for the project entitled EU/US Co-operation for Preventing Computer Related Crime (project number c262/05 4). The European Commission awarded this project in March of 2001 to Transcrime-University of Trento in partnership with Erasmus University of Rotterdam Faculty of Law (Rotterdam, Netherlands), Unisys (Brussels, Belgium), University of Pittsburgh's European Union Center (Pittsburgh, USA), The Mathew B. Ridgeway Center for International Security Studies, University of Pittsburgh (Pittsburgh, USA) and CERT®/CC at Carnegie Mellon University (Pittsburgh, USA). Panelists and participants of the conference, held October 4 and 5 in Pittsburgh PA, USA, reviewed and commented on the report. These have been included in the body of the report where appropriate.

The issue of computer related crime (CRC) and in particular, the need for further co-operation in the field has been identified as a priority in the new transatlantic agenda. The project proposal properly recognized that many international institutions have already developed various initiatives regarding international co-operation against cyber-crime.

There are many milestones in this field, the first of them being the Council of Europe Convention on computer related crime (2001), which focuses on international co-operation and provides important guidelines in the fields of investigation, prosecution, and extradition for international computer related crimes. Second, in 1997, the UN released a Manual on Cyber-crime that urged nations to harmonize laws and cooperate in combating this illegal activity. During the UN Congress in Vienna on the Prevention of Crime and Treatment of Offenders (2000)[1], computer related crime prevention was discussed in a number of separate panels. One of the more important requests from this congress was the opening of international channels of communication and co-operation in order to effectively investigate and combat computer related crime.

Other important initiatives in this field must be noted, such as the Organization for Economic Co-operation and Development (OECD) guidelines in the field of protection of privacy and personal data and security of information systems (1980). The most recent OECD security guidelines put forth several suggestions in the hopes that security will continue to receive increased attention (2001). In particular, they note the importance of networks and network security and identify primary principles including awareness, responsibility, and response, all of which coincide with the findings of this report.

Many of the above-mentioned initiatives were first outlined in the project proposal. However, the events of September 11, 2001 left many with the distinct knowledge that we are more vulnerable than first imagined. Those events have led to a flurry of legislation and papers produced in both the European Union (EU) and the United States (US). Many of these initiatives are discussed throughout this paper in an

[1]For additional information on this conference see: http://www.uncjin.org/Documents/documents.html#Congress

attempt to analyze their ramifications and to offer the best ways in which they can be effectively implemented.

Regardless of the number of laws passed, international initiatives proposed, and summits held in an attempt to resolve this problem, it is strikingly clear that until there is broad international co-operation and communication none of the work completed can be effective in the fight against computer crime. Given this, the aim of this report is to first analyze the illegal use of new technologies by organized crime and the modus operandi of criminals committing computer related crimes. Second, the project offers an analytical examination of the preventive measures, at both national and international levels, specifically as they relate to issues of privacy and e-commerce. Finally, it seeks to define minimum criteria for future CRC prevention programs in order to provide a general framework of co-operation among the different institutions involved in this field.

Part I of this report, submitted to the European Commission on April 30, 2002, attempts to provide a more comprehensive understanding of computer crimes and suggests two frameworks that may ease communication difficulties and aid analysis. The introduction was added utilizing comments from the panel discussion in Pittsburgh and was written, in part, by Unisys.

One of the original goals of the project was to create taxonomies for the different types of computer crime. These taxonomies were to be divided between computer as target and computer-facilitated crimes. It became clear, however, that a taxonomy, in the truest sense of the word, is exceedingly difficult to create for a variety of reasons. Primarily, a taxonomy must be widely accepted and used by the professional community. Considering we are in the initial stages of identification and agreement of what constitutes a computer crime, it was agreed that frameworks for analysis would be created. These frameworks seek to provide legislators, researchers and other interested parties a way in which to categorize and discuss computer crime cases.

Two frameworks are presented. The first, created for computer-facilitated crimes, developed by Shawna Gibson and Daria Angelini at Transcrime -University of Trento, takes a legal approach to the analysis and attempts to categorize crimes in a way that reduces legislative difficulties. This approach was adopted as it is clear that one of the major obstacles in the battle against computer related crimes is their multi-jurisdictional nature. The second framework, created for computer as target crimes, was developed by Phil Williams at CERT®/CC with the questions of who, what, why, how, when, and where, and is outlined and explained from that standpoint.

It is imperative that one conduct a thorough risk assessment in attempt to protect one's assets. It is clear from the findings of this report, however, that a general scale of risks for either computer as target or computer-facilitated crime contributes little value to the overall understanding of this phenomenon; each crime must be looked at individually and must be assessed from the perspective of the perpetrator, victim, and location. Chapter 3, of this report, concludes that that each individual, business and nation must have its own risk assessment completed by a professional who is familiar with risk assessment and risk management.

Part II of this report outlines EU/US prevention strategies and how they specifically relate to the issues of privacy and e-commerce, it was submitted, in part, to the European Commission on June 30, 2002. Shawna Gibson and Daria Angelini from

Transcrime –University of Trento and Paul Verloop from Erasmus University of Rotterdam Faculty of Law, completed this chapter. Prevention strategies were first divided into several categories: legislation, self-regulation and compliance, informative and instructive measures, technological and finally those which do not fit into the previously mentioned categories. One of the more paradoxical findings of this part of the report was the fact that the majority of prevention information is found online. This is not that surprising however, it does not bode well for prevention in general as it appears one of the more effective ways to prevent computer crime is through educating people of the risks and how to protect themselves *before* they engage in online activity. Many books have been written about prevention. They are however, aimed primarily at parents or children, which present its own set of problems and issues.

The Internet has become a breeding ground for criminal and commercial activity. Clearly, the former activities must be prevented and the latter must be protected. Yet, in reality, cyberspace primarily consists of individuals who possess rights and freedoms that should not be infringed upon. The discussion regarding privacy encompasses such issues as government controlled encryption keys, data retention as well as information gathering and warehousing by businesses. This report, written by Unisys, highlights the needs of the individual and the protection of society and concludes that one must always be weighed against the other if there is to be effective policy.

The emerging marketplace is yet another issue that was taken into consideration by Unisys. As with each of the previous sections, the issues at stake are defined and explored. This section suggests that one of the best ways to create a secure commercial environment is through the purchase of e-insurance. This keeps the idea of security at the forefront and ensures that businesses take the necessary precautions to protect their client's information.

Utilizing all of the information gathered several tables were created by Shawna Gibson at Transcrime-University of Trento highlighting the prevention strategies already in place in both the EU and the US. A set of descriptive variables for prevention practices was created early on in the research process and it became abundantly clear that unless one is working with an informed and interested population, no prevention strategy would be effective. In co-operation with one another we must continue to search for discrepancies and loopholes in our legislation and prevention measures, yet in hindsight, the overlap among the strategies may serve to create a multilayered safety net and should, therefore, be maintained. As a broad generalization, Europeans and Americans are different in the way they think and the way they approach problems. We are plagued with the same issues but we approach them from entirely different sets of values and cultural experiences. This is clear within the borders of the EU and it is strikingly clear when we cross the Atlantic. Where we overlap is where we can find our solution as that is our common ground. However, we all need to continue to create strategies that are specific to the people in our own country, particularly when it comes to educational strategies, as what works in one country may not be as effective in another. Ultimately, computer crime boils down to one person and one machine and from that humble starting point – we may find a possible solution.

RESEARCH DESIGN AND METHODOLOGY

This report has been developed according to four primary goals. Each goal has several tasks, which include instructions for their completion. These were first outlined and submitted in the research proposal for the European Commission.

The goals of the research are as follows:

Goal 1 – To analyze the illegal use of new technologies by organized crime and the *modus operandi* of criminals committing computer related crimes.

Goal 2 – To describe analytically the preventive measures, at both the national and international level, which have previously been adopted by institutions in the EU or the US against computer related crime.

Goal 3 – To define the minimum criteria for future CRC prevention programs in order to provide a general framework of co-operation and to avoid further overlapping or discrepancy between prevention projects in this field.

Goal 4 – To develop an online database of existing CRC preventive programs globally, in order to provide an effective dissemination of results. Results of the study will also be disseminated at a conclusive panel aimed at spreading the model and creating the opportunity for further communication and collaboration between different law enforcement agencies.

Goal 1 was developed for the Intermediate Report and included the following tasks, which were completed by CERT®/CC and Transcrime.

Task 1 was to characterize and classify computer related crimes into closed categories, thus creating a standard definition of different computer related crimes.

Task 2 was to describe the typical *modus operandi* of criminals involved in different typologies of computer related crimes by reporting real or simulated cases for each category.

Task 3 was to create a scale of risks for each computer related crime category.

Tasks 1 and 3 were complete by reviewing and analyzing relevant literature. Task 2 was complete by using the crime script methodology (Cornish, 1993), which required the researcher to break down each crime into its component parts in order to more fully understand the crime and make prevention suggestions.

Goals 2 and 3 were accomplished through the completion of the following tasks. Several partners including Unisys, Erasmus University, and Transcrime worked together on these goals. Much of this work was submitted to the European Commission for the second intermediate report.

Task 4 required in-depth research and analysis of national and international initiatives against computer related crime.

Task 5 was to develop a set of descriptive variables in order to create a comprehensive comparison table, which identifies common characteristics or major discrepancies between preventive strategies.

Task 6 required the analysis of privacy concerns versus computer related crime prevention strategies.

Task 7 concerned itself with the issue of the development of the e-economy versus computer related crime prevention strategies.

These tasks were completed by reviewing relevant literature including online articles, textbooks, and legal materials. Expert interviews were conducted and a questionnaire was created and disseminated to several key people. Unfortunately, the questionnaire did not receive the number of responses expected and was therefore of limited use in most cases.

Goal 4 of this research project is the creation of an online database and the dissemination of the results. The tasks for the completion of this particular goal have been refined and the website is currently under construction. In accordance with the timeline, an initial website, which can be updated will be available for the end of October. The panel was organized by the European Union Center and took place October 4 and 5, 2002 in Pittsburgh, PA, USA.

INTRODUCTION

Computer related crime has had a variety of meanings, and can be defined differently depending on context. While researchers have been careful to define their terms no final consensus or definition has been reached. A review of the most recent literature available on computer crime finds that researchers and legislators are providing three definitions of how a perpetrator can utilize the computer in the commission of a crime. The first two are *computer as evidence* and *computer as target*. Computer as evidence should not create significant difficulties for law enforcement or in the prevention of computer crimes as the computer in this case is not central to the commission of the crime but rather only contains evidence that would be useful for the prosecution of a crime (e.g. a spreadsheet that has information about money laundering activities). Computer as target and computer-facilitated crime are discussed at length in the following pages.

Crimes that are perpetrated via the computer, regardless of their target, are receiving increased scrutiny from a variety of parties, namely legislators, academics, professionals as well as every day users of computers. Before the numerous issues related to computer crime are presented, it is first important to have a basic understanding of the technical issues related to the Internet as well as an understanding of the terminology that is used. This introduction provides a brief overview and lays the groundwork for the rest of the report.

The Internet and various technologies that we use today provide us with capabilities far beyond our imagination of just a few decades ago. The first thoughts of what we now call the Internet came about in the late 1950's. The main purpose was to create a secure place where people could communicate as well as send and receive information. Large mainframe computers, owned by government institutions, large corporations, and universities, housed this first "Internet." The users were, largely, known and trusted. The original ideals of the Internet, widespread communication and exchange of information, have remained the same, but the users have not. The creators of the Internet, in all likelihood, had no way of knowing that computers would become a household item and that the Internet would be potentially accessible to every person on a global scale. Given these changes, we are now faced with both old and new forms of crime occurring in a place without borders and for which no contingency plan had been created.

Several key issues exist and must be addressed eventually. This report attempts to highlight some of these concerns and offer solutions when feasible. Some of the important issues that can be identified, as it relates to computer crime, are those problems associated with definition and language as well as concerns regarding privacy and e-commerce. It is clear that many of the problems currently being addressed revolve around the issue of an individual's privacy and their ability to protect their personal space. Our private space now reaches far beyond what was previously agreed upon. In theory, our personal space is now accessible to a global population, which causes further problems of jurisdiction when that space is violated. Considering we are now dealing with an "unbounded threat in a bounded society" we must find other options to help reduce the present danger, this reduction is hoping to be found in co-operation and trust across the Atlantic.

TECHNICAL DESCRIPTION OF INTERNET USAGE

Before describing the multitude of problems that are present when using the Internet, it is useful to review briefly its technical basis. In short, the Internet is a network that interconnects millions of computers worldwide. It allows computers to communicate with each other, based, in part, on the Transfer Control Protocol/Internet Protocol (TCP/IP). In this way, people all over the world can interact with each other and access all types of information.

Physically, the Internet consists of clients and servers with network hardware connecting them. Servers are computers providing services such as e-mail or file-storage for groups of clients. The hardware consists of wires, switches, routers, modems as well as transoceanic cables and satellites.

Several actors are involved in the Internet:

- **The User or Client** uses personal computers to connect to the Internet. This can be an individual or an organization.
- **The Telecommunications Operator** processes traffic information.
- **The Internet Service Provider** (ISP) provides access and services to individuals and companies on the Web. An ISP connects clients and servers to the Internet using telephone lines or other telecommunication channels. ISPs generally also provide their customers with other services such as e-mail accounts, Web space to publish their own websites, etc. Generally, the term ISP also includes IAPs or Internet Access Providers. The term IAP is used when it is clear that the provider only provides Internet access.

The Internet is based on many different **protocols** for the exchange of information between the different computers. These technical standards allow computers worldwide to "translate" the digitized information that is located on another computer. The main protocol for data transmission online is the TCP/IP. Other protocols are designed to offer services that are more sophisticated to users; for example, Hyper Text Transport Protocol (HTTP) for surfing, File Transfer Protocol (FTP) to transfer files, Simple Mail Transport Protocol (SMTP) and POP3 to send and receive e-mails.

On the Internet, computers communicate with each other using an addressing system. Each computer connected to the Internet has a unique address called an Internet Protocol or more commonly **IP address**. This IP address is composed of a string of numbers between 0 and 255, which are separated by dots and is provided to a computer by an Internet Access Provider. An example of an IP address is 209.125.170.30. Communication between computers happens through the appointment of the concerning IP addresses.

Depending on the relationship with the provider, a user can receive a static or a dynamic IP address. A *static* IP address means that the user receives the same permanent IP address, each time he connects to the Internet. A *dynamic* IP address on the contrary, changes each time the user connects to the Internet. The provider assigns an available address to the user when he dials into the provider to connect to the Internet. The user retains that IP address for the duration of the session. Once the session is closed, the IP address is assigned to another user.

Because IP addresses are difficult to remember, the **Domain Name System** (DNS) was created. This mechanism assigns names to computers identified by an IP

address. Domain Name System is a global network of servers that translates host names like www.unisys.com into numerical IP addresses, like 209.125.170.30. One specific domain name always refers to one particular IP address.

The transmission of information on the Internet occurs through small packets of information, which are smaller parts of the actual data. Each packet includes the IP address of the sender and of the recipient, and is transported separately to the indicated destination. An additional layer (the most commonly used is the Transmission Control Protocol or TCP) ensures that the packages will be correctly recombined by the recipient in order to form the original message.

When a user asks for information from another machine, this request goes first to the user's Internet Service Provider. The ISP then sends the request to the machine containing the information wanted. On its way to the destination machine, the request passes through different **routers**. A router connects two or more IP networks and passes packets of information from one area of the network to another choosing the best possible way. This route is not necessarily the shortest way, but the fastest one, taking into consideration the amount of traffic. For example, the fastest way to travel from Brussels to Paris might be through New York. After the intended machine has intercepted the request, the information is sent to the requestors' machine. The message is again broken up into several packages and passes through several routers.

SERVICES AVAILABLE ON THE INTERNET

The Internet offers several services to its users. Most important are the World Wide Web, e-Mail, newsgroups, as well as forums and chat rooms.

World Wide Web: The most common way of communicating over the Internet is through the World Wide Web. This allows users to search and retrieve information that is stored on remote computers by connecting to the Web. The information available on the Web is published on web servers. A server, also called the host, is a piece of software that enables a computer and its files to be accessible from the Internet. Often the computer itself, which is also connected to the Internet, is referred to as the server. Clients can view the information stored on web servers by using a piece of software called a web browser. The browser interprets the hypertext language in order to display the concerned documents. Examples of browsers are Netscape Navigator and Microsoft Internet Explorer. Documents available on the World Wide Web all have a unique web address, called a Uniform Resource Locator (URL), which consists of a protocol name to retrieve the document, a domain name (name of the web server on which the document is located), its path to locate the document and its file name. An example of an URL is "http://www.unisys.com/srvcs/networks/default-06.asp."

E-mail: Electronic mail or e-mail is a service that allows individuals to send an electronic message to another point of destination. E-mail uses the Internet network to transport the mail and various types of attachments between a sender and an addressee. An e-mail address consists of two parts: the "username" or the name of the sender, and the "hostname," which refers to the mail-server on which a user's mailbox is located. This service is offered by e-mail service providers, who host mail servers. The sole responsibility of mail servers is to store and forward

users' mail messages to the destination mail servers. To be able to send and receive e-mails, the user needs an e-mail client software package.

Newsgroups: A newsgroup is a virtual forum that allows users all over the world to share information or to discuss a particular topic online. Newsgroups also provide the possibility to read what others have posted without responding to it. Today thousands of newsgroups are available on the Internet, covering all types of subjects. Newsgroups are located on special news servers.

Forums: A forum or discussion board is similar to a newsgroup, except that it exists on a single server, which is maintained by the owner of the forum. Today, many websites have their own forum.

Chat Rooms: The chat service offers users a way to communicate directly across the Internet and to engage in real-time dialogue with various people worldwide. The most common versions of chat are Internet Relay Chat (IRC) and Web-based chats. An IRC consists of multiple servers connected to each other, while web-based chats run either on dedicated websites or on individual homepages running a chat facility. Internet Relay Chat is not under the control of any organization and uses open standard software, enabling anyone with sufficient knowledge to write and operate an IRC program.

RISKS DURING INTERNET USAGE

Because of the technological mechanisms that support the Internet and its open character, several risks exist when using the Internet. According to a study conducted by the European Commission Article 29 – Data Protection Working Party (November, 2000), there are three major privacy risks, in particular, inherent in the use of the TCP/IP protocol or some other type of permanent Internet connections via cable or dedicated server line (DSL):

- The route followed by TCP/IP packets is dynamic and follows the logic of performance. This route may for example pass through a country that has less adequate data protection.
- The DNS server translates the domain name into a numerical IP addresses. Consequently, the DNS server receives and keeps track of all the names of the Internet servers the user has tried to contact. These kind of servers are, in practice, mainly maintained by Internet Access Providers, who can register the information captured by DNS servers and much more.
- The ping command, which involves typing the letters PING followed by the IP address (or the corresponding name) of a selected computer, is available on all operating systems and allows anyone on the Internet to know if a particular computer is turned on and connected to the Internet. Usually the user of the targeted computer will be unaware of both the “pinging” as well as the motives for which the person is trying to find out if he or she is connected or not.

High-level protocols also present privacy risks. For example, when a user inputs an URL to access a certain website by using the HTTP protocol, different forms of data are systematically transmitted in the HTTP header and thus available to the server.[2]

The use of cookies can also have serious consequences to a person's privacy. Cookies are small pieces of information that a server sends to a client. When a user visits a Website with cookie capabilities, its server sends certain information about the user to the concerned browser, after which the information is stored on the user's hard drive as a text file. This information can be retrieved by the server, at a later time, or can be read by anyone who has an understanding of this data. This enables the companies who own the servers and on which all of this raw data is available, to have significant amounts of information about their individual users. By combining the raw data together with other data already available on the users, companies could have the capability to create an invisible profile of every individual Internet user. In this context, cookies are often used to track surfing habits across the website, or to store the items a person has ordered in a Web supermarket.

PERSONAL DATA ON THE INTERNET

As described, users can leave behind a trail of information or 'electronic fingerprint' when connecting to the Internet, often without knowing it. During the Internet session, substantial amounts of data is systematically "logged" in a file by the Internet Service Providers or telecommunications operator, such as the date, time, duration of the session, and IP address attributed to the Internet user. The user's IP address can be linked to other personal data that eventually identifies the user. It is obviously easier to identify Internet users who make use of static IP addresses, than linking dynamic IP addresses to other personal data (European Commission, November 2000).

This logged data can be used for different purposes. Internet Service Provider's for example, collect personal or communication data for business use, such as customer profiling or billing reasons, for prevention of abuse or sometimes even to share this personal information with third parties (LINX, 2001). Normally these actions can only be taken if they are clearly described in the ISP's privacy policy and only after the individual user has given his or her approval.

In addition to the commercial uses of data, Internet enterprises are often approached by law enforcement agencies seeking access to personal data to investigate a crime and to gather evidence. In this case, a statutory authority is mandatory. The logging of data is a common strategy in tracing criminals who have committed a computer related crime. Considering the importance of this particular action there is a whole section dedicated to this topic.

Other logs on the Internet regarding activity can be the following (LINX, 2001):

[2] More information, plus a demonstration of this, can be found on the website of CNIL http://www.cnil.fr/uk/index.htm.

- Logging of mail servers, which records the source and destination of mail for diagnostic purposes or for tracking down spam mail
- Logging of news servers, which mainly contains summary information
- Logging of web servers, to collect information about which pages were accessed and other useful information like the referral page to website
- Special case logging, for unusual events such as errors or failures, to fix the system
- Processing server activity logs.

Although justified under specific conditions, the collection of personal data can have serious consequences for an individual's right to privacy. This is especially true if the activity is occurring without their consent or when the information is abused, manipulated, or distributed to unreliable third parties.

INTERNET SERVICES

When using the various Internet services, several opportunities exist for privacy invasion and thus further exploitation (European Commission, November 21 2000).

- **E-mail**: When sending an e-mail to someone else, invisible processing can be performed by "mail clients" and SMTP relays. Traffic data can be stored by mail service providers, the e-mail content can be intercepted, or the person's address can be stored in e-mail directories. Another invasion into privacy is the so-called 'Spam' or the sending of unsolicited mails.
- **Surfing and Searching on the Internet:** The increasing use of monitoring software can also have serious consequences for the privacy of Internet users.
- **Newsgroups and Forums:** The main privacy risk in public discussion forums results from the accessibility of personal data disclosed by the Internet user. This data can be used for purposes that were not the original intention of the user. For example, the information could be combined with other available data collected through a registration form or from chat rooms. Software programs like Data-Warehousing or Data-Mining can collect large amounts of personal information from public registers or other publicly available sources such as directories by automatically searching the Web. However, this type of activity should normally be protected by legislation or other technological means.

Economic transactions on the Internet: Many risks can also come about from the secondary use of personal data without the user's consent (e.g. advertising) or the interception of data during transfer (breach of confidentiality).

It is clear that the Internet is a complex set of functions that provides the individuals users with a number of services. Unfortunately, those services do not come without some level of risk. It is important to place the remainder of the report within the context of privacy and jurisdiction as these two issues will be visited repeatedly as places of contention and possible intervention. The issue of privacy and ones ability to protect their personal data is crucial to prevention of the crimes discussed. This further demonstrates that we live in a world where information is king and the ability to protect it dominates.

PART I

DEFINITIONS AND FRAMEWORKS FOR ANALYSIS

CHAPTER 1

COMPUTER-FACILITATED CRIMES

1.

COMPUTER-FACILITATED CRIME: A DEFINITION AND FRAMEWORK

1.1 THE DEFINITION

– Time has been transformed, and we have changed; it has advanced and set us in motion; it has unveiled its face, inspiring us with bewilderment and exhilaration. – Kahlil Gibran

The information age, with all of its grandeur, has presented us with new problems wrapped in familiar clothing. It is similar enough to our old ways to enable us to reflect upon the problems, however, it is dissimilar enough to force us to create new solutions and ways of thinking about our future. The category of computer-facilitated crime epitomizes this dilemma. Computer as target crimes are sufficiently unique that we are able to approach them as we have approached other changes in technology with legislation and understanding. Computer-facilitated crime, however, forces us to look beyond what is simply new and identify what has changed.

Computer-facilitated crime, is the largest category of criminal activity within this realm and fraught with the most difficulties. It has often been referred to by several names, such as "computer related crime," "high-tech crime," and "cyber-crime," which has only added to the confusion. Given the unique nature of computer-facilitated crime – it can be perpetrated quickly and simultaneously in several jurisdictions and is generally anonymous – if we are to be successful in combating computer crime, it is crucial to create a common language through which the various parties are able to communicate. The term "computer related crime" has been used in reference to multiple categories; thus, we suggest the term *computer-facilitated crime* to refer to this category of criminal activity. The use of this term provides the first step towards a common language and allows one to separate (as much as possible) the different types of crimes.

The primary sources utilized to create this definition are those that have been created by the governmental bodies that are interested in the Transatlantic Agenda, primarily the European Union and the United States. In a paper created from a US Presidents working group entitled *The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet* (2000), a framework was provided to evaluate this type of activity. What they initially deemed as useful was the online-offline consistency. "If an activity is prohibited in the physical world but not on the Internet then the Internet becomes a safe haven for that unlawful activity" (2000, p.12). Laws should be applied equally to crimes that are committed in the physical world as well as to those activities that are perpetrated over the Internet.

The Council of Europe's Convention on Cyber-crime (2001) did not provide an all-inclusive definition of computer-facilitated crime. Instead, it described the types of offences that would be found, such as computer related, content related and copyright violations. This is also true for the paper created by the Council of Europe for the European Parliament entitled *Creating a Safer Information Society by Improving the Security of Information Infrastructure and Combating Computer*

related Crime (2000). In this communication, it is clear the European Parliament wants a commonly acceptable definition of computer related offences. This particular statement utilized "computer specific" and "computer related" crimes as opposed to computer as a target. These groups do not facilitate communication in general terms. In an effort to provide a commonly acceptable definition and ease communication difficulties, the following definition is proposed:

Computer-facilitated crime **– traditional crimes that can be or have been committed utilizing other means of perpetration which are now being or are capable of being executed via the Internet, computer related venue (i.e. email, newsgroups, internal networks) or other technological computing advancement.**

1.2 A BRIEF HISTORY

As stated earlier, this particular category is fraught with many difficulties for investigators and legislators alike. Considering computer-facilitated crimes are often multi-jurisdictional, anonymous and are rapidly completed, the ability to fight such activity largely depends on the ability to communicate and work together quickly and efficiently on an international level. One of the first problems encountered is the fact that what is a crime in one country may be completely legal in another. Many of these crimes are typically considered "victim-less" and change from one state to the next such as gambling, prostitution, possession of firearms, soft drugs and so on. The question quickly becomes one of regulation and enforcement. Who is responsible for regulating the Internet when it comes to some of the questionable activities that are based in jurisdictions where it is legal? How does the country where the given activity is *illegal* monitor and regulate what is broadcast into their country via the Internet and how do they prosecute those people who engage in, what they deem to be, illegal behavior?

The purpose of creating a framework for computer-facilitated crimes is to ultimately prevent or combat this activity. The main challenges are the variety and multi-jurisdictional nature of computer-facilitated crimes. One way to understand these activities is through the legal system. To begin, it is crucial to highlight that computer-facilitated crime is not strictly connected to the area of criminal law, but is also related to civil and administrative law. Thus, the problem of computer crime cannot be solely addressed by legal means and must include non-legal measures such as private security (U.N. Manual, 1999). Any solution that is presented must therefore have the co-operation of all parties involved.

Currently, the focus of this type of security is primarily on computer crime in the strictest sense of the term – *computer as target*. This is evidenced by the continued growth of computer security companies as well as then recent US legislation entitled the "Provide Appropriate Tools Required to Intercept and Obstruct Terrorism Act," which is now referred to as the PATRIOT Act. This act was passed shortly after the September 11 attack on the World Trade Center and provides stiffer penalties for hacking activities. Today, discussions in IT circles revolve around issues of encryption and network security. *InformationWeek* interviewed 300 business-technology executives in December 2001. Over half stated their companies would increase their security budget in 2002. According to this same

survey, the majority of the money will be spent on "fortifying networks." In addition, international governments, also reflect this particular focus through the passage of acts and conventions that have been primarily concerned with *computer as target* crime with only a passing reference to computer-facilitated crimes.

This focus is further demonstrated by the European Commission's most recent proposal for a *Council Framework Decision on Attacks against Information Systems* (2002). This proposal seeks to protect the various information systems on which businesses and individuals have become increasingly dependant. The proposal identifies four primary threats, hacking, disruption of information systems, execution of malicious software, and interception of communication, all of which can be considered computer as target type crimes. The fifth identified threat was that of malicious misrepresentation such as fraud or identity theft. The primary concern of this proposal is, rightly, the protection of various critical infrastructures and this is particularly crucial in light of current events. In addition, the Commission demonstrates an ability to identify other threats, particularly to the individual, which is one of the first documents to scratch the surface of this complex phenomenon and asks for concrete results in this arena of computer-facilitated crime.

Traditional crimes committed via the Internet are receiving increased attention. Private and public sectors, on an international basis, are beginning to cooperate in an effort to address this growing problem more effectively. Computer-facilitated crimes are largely prosecuted under existing laws pertaining to each specific crime. For example, in the US most Internet fraud offences have been prosecuted under the Interstate Transportation of Stolen Property (ITSP) statute, which encompasses many types of activities and has allowed for the prosecution of these types of offences. Unfortunately, use of this statute alone proved to be insufficient and several changes have been made in an effort to create more effective criminal statutes (for a more complete legislative history see Rasch, 1996).

The European Commission introduced the *e*-Europe initiative in December 1999 to ensure that Europe can effectively handle all aspects of digital technologies, from the economic to the social and legal implications. This project has led to the recent publication of many important documents in terms of preventing criminal activity on the Internet, such as the Communication from the European Commission entitled *Network and Information Security: Proposal for a European Policy Approach* (2001). The *e*-Europe project also plays a key role in the future of the European law enforcement fight against cyber-crime by creating legislation meant to make the Internet a safer place for e-commerce and individuals to conduct business. Efforts to address the issues of computer related crime more effectively, in general terms, have led to some legislative initiatives in both the EU and the US, yet they remain largely insufficient.

Criminal provisions adopted by each state provide the framework through which computer-facilitated crimes must be addressed. This problem is not limited to Europe but also exists within the US as no two American states have identical criminal statutes. The ever-increasing interconnectedness of our global society magnifies this challenge. Perhaps one of most important legal work in this field is the Council of Europe's Convention on Cyber-crime (2001). This was the first meeting of its kind and called for the harmonization of international laws to combat computer crime more effectively. Although this convention is unique and considers a variety of criminal activity it fails to adequately address the issues presented with

computer-facilitated crime. In fact, the only crimes that are sufficiently discussed, because there is international agreement, are child-pornography and intellectual property violations. This highlights the fact that little has been done to address the issues within the computer-facilitated crime category on an international basis and there is minimal agreement regarding their definitions or how to combat them.

Regardless of its drawbacks, the Council of Europe's Convention is widely supported by other international players, in particular the United States, Canada, and Japan. It provides a starting point from which the international community can begin a discourse and start to enact the necessary legislation to address the transnational nature of computer crimes, the necessity of which is becoming increasingly evident. This particular convention has also received substantial criticism from privacy advocates and others in the field reminding all those concerned that this is a starting point, in need of continued revision as the field grows, and changes.

When developing a comparative analysis for the variety of illegal behaviors related to the use of computer, the main problem derives from the different criminal provisions utilized in each country. Some states (both EU/US) have no particular interest in criminalizing certain behaviors, or they defend certain interests by creating civil or administrative law provisions. For example, what is considered a hate crime in one European state could be seen as a freedom of speech issue in the United States. The recent court case between a student group and *Yahoo! Inc* and *Yahoo! France* (2000), wherein student requested that the French Court find *Yahoo!* in violation of French penal code regarding the propagation of anti-Semitism, exemplifies this point. Ultimately, *Yahoo!* lost the court battle after several appeals and *Yahoo!* France was forced to post warnings informing people to terminate their connections if they were in violation of French law. *Yahoo!*, an American based company, had no such regulations, thus they were not in violation of any crime in their "home" country.

In an effort to remedy the multi-jurisdictional problem, *The Legal Aspect of Computer Related Crime in the Information Society -COMCRIME Study* (1998), prepared for the European Commission by Ulrich Sieber, divides behavior into four categories based on the protection of the following needs: protection of privacy, protection against economic offences, protection of intellectual property and protection against illegal and harmful contents. These categories originate from the primary areas in which EU lawmakers established new regulations for preventing computer crimes.[3]

It is becoming increasingly clear that the Internet, computers, and the variety of technologies upon which the developed world is progressively more dependent has provided a virtual breeding ground for criminal behavior. An emerging problem in recent years, in need of intense scrutiny, is the evolution in the technology era of those behaviors that are considered traditionally illegal. It is important to examine how criminals have benefited from the computer, which in turn should allow us to take a more in-depth look at potential prevention strategies. Additionally, these

[3] For more information on EU computer crime legislation, see Communication on Illegal and Harmful Content on the Internet (1996). As it relates to each Member State, see Interim Report on Initiatives in EU Member States with Respect to Combating Illegal and Harmful Content on the Internet, Version 7 (1997).

methods must take into account the importance of the continued growth of the Internet and information technology as a means of commerce and communications.

A prime example of passing legislation before there is a thorough understanding of the crime is the US Digital Millennium Copyright Act. This act has caused significant problems for researchers and has been accused of stifling innovation on many fronts. This act was in, all likelihood, well intentioned and meant to protect the information upon which most of our life's work is now based. Unfortunately, it has inhibited the sharing of ideas across borders and has put a large amount of control regarding Internet content in the hands of a few people or corporations with enough money to fight long, drawn-out court battles.

Considering the multi-jurisdictional nature of computer-facilitated crimes, as well as the variety of behaviors that can be deemed part of this category, the framework must be created from a legal standpoint. This is the first attempt to provide such an international legal framework. This framework differs from those provided and discussed in the section on *computer as target* for several reasons. First, the perpetrator can be nearly anyone, including someone who has minimal computer skill. This framework can be used in addition to others provided or as a stand-alone concept depending on the needs of the user.

Frameworks are designed to ease communication and provide basic categories through which advanced work can be accomplished. Computer-facilitated crime is an enormous category of activity that affects people on a global basis; the perpetrators can be anyone, anywhere with various levels of computer skill. The common concept from which this framework operates is the activity and its criminality. The researchers hope that it will facilitate communication on a Transatlantic or even global scale.

1.3 The Framework

The inherent need for a starting place requires that one identify a foundation from which to build. The foundation for computer-facilitated crime is rooted in the physical world, thus one can return to that place and identify first what is a crime or wrongdoing. This appears to be one of very few starting places, as no legal definitions for computer-facilitated crime currently exists. Given this, the questions become what is a crime and why do we deem it as such? Several sources were utilized to create a working definition of crime, for the purposes of this framework. The first definition of crime – "the intentional commission of an act, usually deemed socially harmful or dangerous, and specifically defined, prohibited and punishable under the criminal law" – came from Encyclopedia Britannica (2002). The second definition was provided by Black's Law Dictionary (1979), which is "an act committed or omitted in violation of a law forbidding or commanding it and to which is annexed a punishment." Thus, the working definition became *all acts or omissions deemed by the law to be a public wrong before the information technology era, which are therefore punishable in criminal proceedings.*

To define a set of workable traditional crimes for the different legal systems it is important to emphasize some peculiarities of each state's criminal provisions. For

example, each country gives a specific definition of what they consider a crime. Law provisions generally describe crimes in terms of the action or omission, the target, and the type of damage required for the prosecution. Some crimes are prosecuted in a similar manner in both the United States and the European Union. However, there are significant differences in the underlying theories that affect the development of future law provisions, which create problems for legislators. For example, larceny statutes protect property rights but the actual concept of property has developed differently according to civil or common law. The common law system divides property between real property and personal property, which is more inclusive, while civil law systems consider different categories such as tangible and intangible assets (e.g. copyrights and patents).

Some actions are considered a crime only if they are perpetrated in a particular manner. For example, some states in the European community prosecute prostitution *ex se*, while other states consider it a crime only if one person has succeeded in inducing another person to become a prostitute. This is also true for parts of the US. Prostitution is legal in Nevada, while in other states it is illegal for both parties (the prostitute and the client). Even if there are law provisions common to all states for a determined behavior, sometimes there are significant differences in the punishment or sanctions.

In spite of these differences, a common theme of protected legal interest emerges, which helps to create the final criminal statute. Utilizing the similarity highlighted, one is able to outline three main categories that contain a variety of behaviors usually prosecuted under criminal law in both the EU and the US:

- **Crimes against person:** Offences against the physical or psychological well-being of a person; this category also includes those behaviors found to be morally offensive.
- **Crimes against property:** Offences against private or public property which is defined as "anything of value including real estate, tangible and intangible personal property, contract rights, choices in action and other interest in or in claim to wealth, admission or transportation tickets, captured or domestic animals, food and drink, electric or other power" (*Black's Law Dictionary*, 1979).
- **Crimes against public order and public interest:** Behaviors that can offend state interests or interfere with public order.

The illegal behaviors contained in these categories include a variety of crimes with an array of severity from minor to more serious violations depending on the crime as well as the particular state (EU/US) being addressed. Some crimes that have been placed in one category could also be considered under a different heading depending on the particular criminal law statute. The identified behaviors represent more than a list of *traditional crimes*; they are instead likened to a catalogue of "traditional criminal phenomena." The following are drawn from a review of the legal literature; however, they have been elaborated upon in an effort to make them more applicable to the different legal systems and do not necessarily reflect strict legal definitions. For example, the larger category of identity theft includes the specific crimes of personate (stealing and utilizing personal data for gain) and impersonation (presenting oneself as a licensed professional).

The researchers are fully aware that the full extent of traditional crimes is not covered in this list. However, for practical purposes we have limited our research to the most common crimes that have been or are facilitated by the use of computers.

This was determined through a review of the literature, governmental texts, and industry information that is available via the Internet as well as listservs. We encourage other researchers to be aware of other possibilities in this field and to know that this inventory is not all encompassing. Crimes that are perpetrated in a unique manner in relation to computers, such as trespassing will not be considered as each state was forced to create specific law provision solely for those crimes. Other crimes such as theft and espionage, which span both *computer as target* and *computer-facilitated* categories, are included in the framework but are not covered in this section as they are more appropriately analyzed within the section on computer as target.

The working definitions for each criminal phenomenon were created from United Nations (UN) conventions or papers when possible. Crimes outlined under the category "crimes against public interest and public order" were drawn primarily from those sources. *Black's Law Dictionary* was utilized for the remaining behaviors as it provides a more cohesive definition of criminal phenomenon and no such dictionary or reference material exists within the European Union.

The following table provides a general overview of the various crimes considered within each category. The crimes within the table are organized according to similarity of perpetration and not severity of punishment or level of victimization. The modus operandi is provided for each crime or combined where possible. In some instances, the combined crimes come from different categories as it became clear that they take advantage of the same technological characteristics.

The following sections are organized in a similar manner as the initial table for ease of referencing. The subsequent tables have been built according to the crime script methodology (Cornish, 1993) which separates the criminal behavior into its component parts and highlights possible points of intervention to control or prevent illicit conduct. Several case studies were analyzed for each crime (where possible) and all of them can be found in Annex I. Each crime is defined, analyzed, and broken down into sections based on their physical world perpetration with its corresponding technological facilitation. The table includes a conclusion section, which is meant as a summary of that particular criminal phenomenon.

Figure 1: Computer-facilitated Crimes

Against persons	Against property	Against public order & public interest
Violation of privacy	Violation of intellectual property	Trafficking:
		Drugs
Identity theft (personal data)	Violation of industrial property	Firearms
		Organs
Hate Crimes	Fraud:	Human
	Business fraud (trading, banking, credit cards, stocks manipulation)	
Defamation		Gambling
	Investment fraud	
Blackmail	Customers (sale online, false advertisements, confidence trick)	Money laundering
Cyber-stalking	Economic espionage	Government Espionage
Prostitution	Theft[4] & embezzlement	Corruption
Child exploitation		Terrorism
Child luring		
Child pornography		

Before beginning the analysis, it is important to keep in mind that this demonstrates an attempt at creating a common language for computer-facilitated crime. As stated above, the main obstacle to comparing the criminal provisions in different states is the differences that exist between each country's laws. The three categories outlined should help to avoid this obstacle in that they describe a common starting point for the law-making process and define the elementary principles that guide legislators. Moreover, they identify the goods and values protected by the creation of various laws. Those core groups of interests provide an understanding of how different criminal law provisions function and also suggest how a territorially based law, such as criminal law, could operate in cyberspace.

[4] In reference to computer-facilitated crime, theft often occurs with the appropriation of property (e.g. copying a file). Those crimes are referred to as theft although they do not fit perfectly within the traditional definition.

Dealing with crime is not only related to the definition but also to the practical application of the law. Difficulties in analyzing the issue, because of the existence of different jurisdictions, have already arisen. The borderless character of the Internet makes it very difficult to apply locally implemented laws to online activities. As long as time and space depend on the perspective of the user, they may switch from an environment where their actions are illegal to another one where they are not, by simply changing the web site visited. Thus, a well-designed criminal provision could be completely ineffective due to jurisdictional problems.

Although one could say that the Internet is a place filled with anarchy and no jurisdictions exist in cyberspace, the Internet is theoretically more regulated than the physical world (Wall, 2000). Mechanisms exist whereby individual sovereign states can impose their rules on those not physically present within the jurisdiction, such as the ubiquity rule, international arrest warrant, and extradition. Thus, each state, which claims to be offended by a criminal action committed on the Internet, may start its own procedure against the perpetrators. However, these mechanisms entail additional law enforcement costs and they may not operate under all circumstances.

The solution usually involves coordinating and harmonizing the legal regimes of competing sovereignties. This may be considered the best way to tackle computer crimes but a realistic approach should be maintained. It is far more difficult to define a strategy, which assumes a unified global approach to legislation capable of responding to the dynamic relationship within cyberspace. Furthermore, creating conventions or multilateral treaties requires time, but the countermeasures that need to be implemented must occur more rapidly. The loopholes between countries can be closed through co-operation and by defining crimes only where a general consensus already exists. When a behavior is widely considered as a wrongdoing, new common provisions are implemented relatively easily and judicial co-operation works faster. Crimes against persons and crimes against property provide two such examples.

When one looks at specific behaviors, several traditional crimes are labeled in different ways in various states. Therefore, criminal law cannot be used as the main solution. This can be better understood by using one of the crimes from the category *crime against public interest and public order* as an example. Legal scholars consider gambling as a "crime without victims." Gambling, however, in economic terms refers to a person who invests money in a business where the results can only be partially predicted. Therefore, investing money on the stock market could be considered gambling as some level. Thus, the reasons behind the choice to criminalize gambling could be related to criminal policies. It is a fact that casinos are often exploited by organized crime for money laundering activities. Other reasons to allow this activity could be related to the economic benefits governments receive from gambling.

Cyberspace radically undermines the relationship between protected interests and its criminal provision. The Internet requires one to reflect upon policies and legislation enforced to protect the local interest of a higher authority. Criminal law ground rules are still valid but the structure of criminal sanctions do not always adapt well to the features and players within cyberspace. It is possible to change and develop existing provisions, but there is also a need to look at the current policing model and open it to a new approach focused primarily on prevention.

The routine activity approach theory in criminology suggests that a crime will occur when "a motivated offender and suitable victim coincide in the absence of capable guardian" (Felson, 2001). On the Internet, there is a mass presence of both motivated offenders and suitable targets, but there is still a lack of capable guardians. However, it does not mean that policing the Internet is the only solution. Measures to tackle computer crimes should also include the development of capable guardians. The education of consumers, entrepreneurs, and public administration on the harmful effects of computer-facilitated crimes, the widespread application of technical security measures and the creation of systems of self-regulation and compliance are the three elements that may ensure the respect of different legal regimes that share the same space. Thus, the political thinking on the regulation of cyberspace should be modified from a top down approach to a multilevel one, the pillars of which should be co-operation and prevention.

2.

THE ANALYSIS

2.1 CRIME AGAINST PERSONS

VIOLATION OF PRIVACY:

The right to privacy is a generic term encompassing various rights recognized as an inherent concept related to the personal intimate sphere. The law generally attempts to prevent violations of privacy by punishing the infringements made with the motives of curiosity, gain, and/or malice.

Identity Theft:

The act of assuming the identity/person of another without their consent or knowledge and using their personal data for gain or other type of advantage. The victim of this type of illegal behavior could be anyone from a public officer to a licensed professional as well as the average citizen

ANALYSIS

Privacy is one of the biggest issues related to the use of high technology. Considering this, there is an entire section devoted to this topic alone. As previously stated violations of one's privacy forms the basis of nearly every computer crime at one level or another. This topic encompasses many different areas such as the selling of personal data, electronic surveillance and spamming. Each topic is important individually and deserving of extensive research and commentary. Spamming, the most common form of violation of privacy, has many issues connected to it and is the online version of junk mail. It is typically related to civil law regulations, does not usually garner stiff penalties, and is rarely prosecuted.

One's privacy can be violated in a variety of ways by a number of different sources. This is covered at length in the privacy section of this report. Suffice it to say, an Internet user often leaves a trail of information for anyone, including companies, retailers and individuals to find or purchase and then exploit. What information is not gathered through technical means can be collected by using social engineering techniques and asking the person directly about useful information the individual may not think twice about providing.

The amount of data available is astounding and can include birth dates, addresses, as well as shopping preferences. Several websites will sell their databases without the consent of the legal owner, while others offer a search service to gather specific information. As shown in the *docusearch.com* case, this can have serious ramifications and lead to more severe crimes such as stalking, continued harassment, or even murder. Violation of one's privacy has moral, social, and legal implications; however, the amount of available data does not appear to be

lessening. Online merchants and service providers continue to ask for the data and consumers continue to provide it. Some consumers may not be aware of what is collected about their web surfing practices or believe their information is anonymous (Green, Norm, Borrus, & Yang, 2000).

One crime that invariably begins with violation of one's privacy is identity theft. The Internet allows a person to create an entirely new identity or steal someone else's. If someone has easy access to personal data such as bank account numbers, identification cards, and other similar information in the real world then the use of technology is usually limited to the creation of fake documents. However, the Internet is changing this type of criminal behavior and now provides the largest potential opportunity to create, market, and sell high quality false identification (Hoar, 2001). Several websites manufacture almost any type of false identification and documents, including driver's licenses, birth certificates, military cards, press passes, college diplomas, or university degrees. If one would like to create their own documents one can easily find, steal, or purchase another person's data via the Internet or other network connections. Personal information is readily available on websites and in chat rooms for anyone who desires to find it.

Intercepting commercial or personal communication or cracking into a database is one of the fastest ways to collect personal data. A common way to steal information is the *link capture* technique. The criminal creates a link to a site outside of the chat room or to a commercial website the potential victim is visiting. The link opens a web page where the victim is asked to enter personal information. The look of this new page is usually similar to the original chat room or commercial website. A variant of this scheme is *site cloning,* in which case an entire website is cloned from a real one in order to maintain the trust of the customer and steal their data (see the PairGain case in the *Fraud* section*).*

The theft of data and the creation of a false identity is usually only a part of a larger criminal scheme (Arnold, 2000). For example, an identity theft could be the crime necessary for blackmailing or for committing some kind of bank or commercial fraud. The stolen data is often used to create a new bank account, to obtain loans or make large purchases. Historically, few people had access to any particular person's information, which made finding the perpetrator relatively easy. In cases where someone's information was stolen from a trashcan or similar method by an unknown person (i.e. dumpster diving), locating the perpetrator behind the identity theft was much more difficult for investigators. With the advent of technology, the person responsible for the theft could be virtually anyone, which amplifies law enforcement problems.

	Traditional Aspects	Technological Facilitation	Consequence
Violation of privacy and Identity theft	Obtain personal information	Purchase information from a search created on personal data	The Internet has allowed large amounts of personal data to be accessible to countless people with relative ease. This can lead to the perpetration of additional crimes, sometimes with severe ramifications. Identity thefts have increased with the introduction of the Internet. The creation of a false identity is often connected to the perpetration of other crimes, making it more difficult to discover the subsequent crimes.
		Use cookies and/or similar software to create customer profiles	
		Steal personal information available online via chat rooms, published websites or through hacking into websites and databases	
	Use personal information for illicit purposes	Sell/purchase illegal personal data/documents over the internet	
		Use computer hardware (printers and scanner) to create false documents	
		Obtain bank loans or credit cards using fake documents and/or stolen data through online banks	
		Make online or other types of purchases	

HATE CRIMES:

All forms of expression that incite to racial hatred, xenophobia, anti-Semitism, and all forms of intolerance (Council of Europe, 1997).

DEFAMATION:

The act of subjecting a person to ridicule, scorn, or contempt in a considerable part of the community. This category also includes both libel and slander.

ANALYSIS

Defamation and hate speech both utilize the ability communicate with large groups of people for their successful perpetration. Websites, e-mail as well as public or private Usenet facilities and virtual boards are common as they are typically reserved for certain users. Defamation generally has one intended victim whereas hate speech encompasses whole groups of people. The perpetrator generally chooses the venue with the most significant impact, depending on the targeted victim(s). Because the discovery and removal of some statements does not occur immediately the comments may cause problems long after the original publication. The true scope of a slanderous remark made in cyberspace, through any method, is impossible to quantify. The Internet allows one to communicate with a virtually endless number of people in a variety of formats. Thus, the ramifications of defamation and hate speech could be felt globally (Judah, 1997).

Hate crime is a key area where international regulation exists and yet there continues to be significant problems within the realm of the Internet. The Nazi memorabilia case provides an example of an international problem in which racist propaganda, in any form, can cause considerable legislative difficulties. The major problem with regulating the Internet in regards to hate speech is the First Amendment to the US Constitution in addition to the legislation of other countries, namely Canada. The US has been consistent with reference to this Amendment and was given special consideration in the UN International Convention on the Elimination of all Forms of Racial Discrimination. Thus, people who wish to propagate hatred in any of its forms, be it against race, religion, or sexual orientation, can do so by selecting an Internet Service Provider (ISP) based in a country that allows this type of material. Hypothetically speaking, if there was agreement on free speech issues on an international level and no website was allowed to broadcast hate speech, one would still have to contend with email and the multitude of other forums that people subscribe to via their computer.

One of the main difficulties is the level of severity of the crime required before there is legal action. For example, in the US, hate speech is only prosecuted if there is a real and legitimate threat. Given this standard, one is forced to question the veracity of the information published on the World Wide Web or distributed in other electronic forms. Depending on one's perspective, either this is a standard that stimulates critical thinking about Internet publications or one that promotes hate speech and does not provide proper protection.

Hate speech and defamation are the best examples of the purpose and the problem of the Internet. These activities were once accomplished by flyers, telephone calls,

public beatings, cross burnings and symbolic violence. Attempting to identify the various parts of this activity appears to be a futile effort as one only needs to purchase a domain name, get an email account or join a newsgroup and the world of speech and exchange of ideas has begun be it for positive or negative aims.

<table>
<tr><th></th><th>Traditional Aspects</th><th>Technological Facilitation</th><th>Consequence</th></tr>
<tr><td rowspan="4">Defamation and Hate Speech</td><td rowspan="4">Say or publish something slanderous or libelous about another person or something that is derogatory or incites violence towards a particular group</td><td>Utilize Usenet facilities, virtual message boards or websites</td><td rowspan="4">The use of the Internet makes it more difficult to identify the person who commits the libelous, slanderous, or hateful act. Damage to the victims' reputation may be more severe considering the potentially vast audience for the message. Citizens have greater access to their countries' censored items. Further violence may be perpetrated against certain groups based on the published message.</td></tr>
<tr><td>Send email</td></tr>
<tr><td>Chat rooms</td></tr>
<tr><td>Sell or distribute defamatory or hateful material (e.g. books, videos, or newsletters etc…)</td></tr>
</table>

BLACKMAIL:

Unlawful demand of money or property under threat to do bodily harm, to destroy property, to accuse of a crime or to expose discreditable defects of character or actions.

FRAUD:

An intentional perversion of truth to induce another to part with some valuable possession or to surrender a legal right by relying on false statements. In order to refine this extensive category the analysts at the Internet Fraud Complaint Center (2001) developed different definitions of fraud according to specific behaviors. Some of the more common categories that will be addressed are (1) Business or Financial Institution fraud (the most common forms perpetrated via the Internet are credit card fraud and e-payment systems fraud); (2) Investment fraud; (3) Customer fraud – (contained within this category is auction fraud).

ANALYSIS

Fraud and blackmail have several things in common in both the physical and virtual realms. Within the physical, it is clear that someone is attempting to get something from another without being entitled to it. Remaining anonymous is an essential key to extortion or blackmail as well as fraud. One only wants to provide enough information to get the money or desired goods from the victim. Given that it is relatively easy to remain anonymous on the Internet by using re-mailers and Web-based email services (for example), the technological capabilities of the criminal

appear to be fundamental issues for the success of these particular crimes. The ability to make information or photos available to millions of people in a short period is an additional tool for the blackmailer as it could also be a powerful way to extort money on a global basis. The anonymity, growing e-commerce, and ease of communication, makes it likely that the Internet will increase the number of blackmail attempts and frauds or make the perpetration more creative. Neither crime has to be complicated to be successful, have not changed significantly from the physical to the virtual world, and do not need new legislation in order to be appropriately prosecuted.

Blackmail perpetrated via the Internet typically involves extortion based on information about a website or software security issue. In some cases, the information is the result of previous crimes such as the theft of data from a database or the interception of credit card numbers from a commercial website. These crimes are often found in fraud schemes as well. Blackmail, in particular, can be analyzed using both frameworks *computer as target* and *computer-facilitated crimes.* How these crime will ultimately be perpetrated depends on the motivation of the perpetrator and the information he or she is able to gather about the victim.

Because of the significant number of frauds perpetrated via the Internet, a larger amount of research exists. The way in which contact is made with the victim varies, however, according to the Internet Fraud Complaint Center's (IFCC) annual report (2001), the most common method is through an email or a website. Some of the cases demonstrate however, that combinations of technology and traditional contacts (i.e. physical letter) have also been used to convince the victim the scheme was legitimate. Other ways of making contact have included a combination of chat room dialogue coupled with a false website. Fraudsters also utilize legal websites or well-known trademarks to mislead their victims. Aside from stock manipulation, other areas that are growing attractions for fraudsters are Internet auction sites. These allow one to sell things that do not exist or to present fake items as genuine. Other ways fraudsters take advantage of online auction houses is through shill bidding wherein they place false bids to inflate the final price.

Perpetrators and their victims can be either businesses or individuals. Large amounts of money are lost yearly by businesses that unwittingly accept stolen credit cards or have sent the goods and had the payment stopped by the customer. The types and ways in which to perpetrate fraud are virtually endless. Because of this fact, the profile of who is likely to commit fraud is not extremely useful. Although a large percentage of fraud occurs in one country, the crime is still plagued by the "border-less ness" of the Internet when it comes to investigations.

Other types of activities that can be categorized as a type of fraud are forgery and counterfeiting. The case entitled "other frauds" is a good example of document forgery. Forgery logically fits into this category in that one is trying to get something for nothing; selling forged art pieces or forging desirable documents can be one of the key elements to a successful fraud. Counterfeiting on the other hand is slightly different in that one is creating money to use on the legitimate market. Historically, counterfeiting has been left to the criminals with artistic talent who can copy something to the smallest detail. This however is no longer the case. Technology allows anyone to be a counterfeiter; all one needs is the desire and the right software and printing apparatus.

	Traditional Aspect	Technological facilitation	Consequences
Blackmail and Fraud	Gather information about victim	Break into a website and/or database; use the security issue as potential blackmail material. Steal information and/or intercept communication. Utilize information known through a job position or research purpose	The use of the Internet for blackmail and for fraud makes them more difficult to track due (in part) to the anonymity and the use of re-mailer techniques. Disclosures of the secrets or stolen information may cause more severe damages to the victim(s) due to the potentially large audience of the Internet. Fraudsters have a larger audience from which to choose their victim and the ability to give an air of legitimacy to their schemes.
	Original contact with victim	Use of email, websites, message boards, chat rooms to make contact with potential victim(s)	
	Communicate with potential victim	Send email to victim outlining desired actions and/or money as in the case of blackmail or to further gain the trust of the victim in a fraud scheme	
		Use the Internet as a threat in the communication	
	Receipt of goods or services from the victim	Wire or bank account transfers	
		Use credit cards that were obtained fraudulently to purchase goods online	

CYBER-STALKING:

A person's course of conduct that places another person in fear for their safety. The actions that are prosecuted under the different stalking statutes vary from state to state. In general, virtually any unwanted contact between a stalker and their victim, which directly or indirectly places the victim in fear, can be referred to as stalking.

ANALYSIS

Stalking is one of the more difficult crimes to prosecute simply because harassment, in any form, is complicated to prove. The use of technology, however, makes it even more problematic. Stalkers obviously utilize the ability to remain anonymous to law enforcement, while allowing victims to know they are being traced, to their advantage. The Internet clearly provides the possibility to locate all the necessary information to make cyber-stalking a reality (see the cases under violation of privacy). Often times, however, the data used is already in the hands of the stalkers, as they know their victims quite well. Many different groupings of behaviors characterize stalking. However, a large degree of variance exists between individual cases. Stalking is not usually a violent crime; nonetheless, it has the

potential to escalate to assault, rape, or other types of criminal behavior (Emma, 2000). Given the global nature of the Internet, however, cyber-stalking is not likely to manifest itself in the physical sense. What is important to note is the presence of the threat and the psychological effects of this type of harassment are comparable to that committed in real life (Tracey & Mattinson, 2000).

<table>
<tr><td rowspan="5">Cyber-Stalking</td><td>Traditional Aspects</td><td>Technological Facilitation</td><td>Consequence</td></tr>
<tr><td>Find victim(s)</td><td>Meet victim in a chat room, find a personal web page or other information about that person</td><td rowspan="4">Use of special software, an anonymizer, or a re-mailer makes it difficult to track stalkers. The harassment may not reach legal standards thus the legal system can often be powerless. The damages suffered by victims depend on the intensity of the harassment and can be quite severe.</td></tr>
<tr><td rowspan="2">Make repeated unwanted contact with victim</td><td>Send obscene or threatening emails, spam, or send viruses or worms. Deface their personal web page</td></tr>
<tr><td>Harassment via chat rooms- direct threats or flooding the victim's channel to prevent conversation with other people</td></tr>
<tr><td>Violation of victims privacy</td><td>Gain access to victims personal accounts, information or web pages</td></tr>
<tr><td>Use victim's identity</td><td>Use of his/her account, nickname, or email address to talk with other people, shop online etc. Harassment with unsolicited mail or contacts from other people</td></tr>
</table>

PROSTITUTION:

Performing an act of sexual intercourse for money or goods. Offering or agreeing to perform unlawful sexual act for hire. Unlawful sexual acts are considered all those actions prohibited by the law, which vary by state and country.

ANALYSIS

Some prostitution websites depict the photos from their catalogue and use the Web for advertising purposes, as this is not a crime a several countries. Sites that are more sophisticated offer customers appointment scheduling or online payment services. Other websites include a disclaimer informing customers the services offered are only for the escort's time as a companion. Bequai (2001) suggests that people who operate online brothels are likely to be either male or female prostitutes who have moved their business from the street to the Internet and/or people working for organized crime groups; defined here as two or more people working together to commit an illegal act. The anonymity provided by the Internet

could act as a catalyst for people trying to earn money in the sex industry. Further, arranging meetings via the Internet could be considered more socially acceptable than offering themselves on the street.

The relationship between the Internet and prostitution is not limited to supply and demand but also effects the recruitment of new prostitutes. The Internet allows criminals to lure women and children into prostitution (see Brazilian email case in *Trafficking of Humans* section). For example, chatting via the Internet allows one to gain another persons trust, which in turn makes it easier to try to convince them to become prostitutes.

	Traditional Aspects	Technological Facilitation	Consequence
Prostitution	Recruitment	Contact potential and actual prostitutes through Internet technologies (email, chat rooms, Usenet groups)	The Internet allows one to bypass local regulations regarding prostitution. The supply and the demand may increase because it is easier and safer (for all parties) to arrange meetings and pay for services. The Internet provides global access to both men and women for recruitment purposes.
	Supply	Advertisement of prostitution through websites, emails, and message boards	
	Demand	Access to more pornography on the WWW increases the demand as it makes it easier to find anonymously and provides access to people who may not otherwise seek it out	
	Delivery	Use email to make arrangements/requests Utilize web cams to provide requested acts	
	Payment	Utilize online payment methods by credit/debit or other mode of payment	

CHILD EXPLOITATION:

1. **Luring of children**: Presenting oneself in such a way as to entice a child victim to meet in person for the purpose of exploitation.

2. **Child Pornography**: Possessing, creating or distributing materials (audio or visual) which depict the sexual conduct of minor children, or that which appears to be a depiction of a minor children, engaging in sexual conduct.

ANALYSIS

Increased public discussion has brought greater awareness to the fact that some children are abused via Internet. The Internet in particular has assisted these specific crimes, as it creates anonymous and relatively quick access to a repository of child pornography, all of which can be accessed from the privacy of one's home. Thus, the risk for apprehension could be relatively low.

The Internet provides several places wherein the exploiter (e.g. a pedophile or someone who creates or sells pornography or otherwise takes advantage of children in some way) can have access to real children as well as child pornography (Arnaldo, 2000). First, some websites sell or offer free photos and/or videos depicting children in sexually explicit poses or engaged in sexual acts with adults or other children. Some of these photos may be genuine while others may be digital depictions or altered photos. It is important to note that not everyone who accesses this type of material is a pedophile, which is a common misconception. Some people view child pornography because they are curious, which is not in and of itself a crime whereas possessing, creating, and/or distributing this material are criminal acts.

The most frightening aspect of the Internet is that the newsgroups and virtual boards allow people in this area to network and exchange pornographic material or information about the ways to lure children in order to have actual relations with them or for some type of exploitation. For pedophiles in particular, this network also allows them to provide psychological support to one another regarding their activities reducing their cognitive dissonance (believing in one thing and acting in a manner contrary to those beliefs, this feeling is generally lessened with the use of justifications and excuses). This informal support network also provides information about possible police investigations making it more difficult to apprehend the offenders.

The Internet provides access to children via chat rooms and through websites that arrange travel to a country, such as Southeast Asia, where underage prostitution is practiced (Opperman, 1999). Exploiters typically enter teen chat rooms by concealing their identity and then attempt to gain and maintain the child's trust. Once that trust has been achieved, they attempt to arrange a real life meeting with the potential victim. Often child exploiters have access to the child's personal data – as in the violation of privacy cases – and can contact the child directly, bypassing the need for the chat room.

The pornographic websites that offer free photos as well as the virtual community where the exploiters meet one another are generally run by a small group of individuals (usually pedophiles) who find that building a network allows them to access a larger catalogue of materials for their own purposes. In general, websites that sell materials or offer child prostitutes have been connected with organized crime. The number of people connected to child pornography rings could involve hundreds of suspects from all over the globe as demonstrated in the Barcelona pornography ring case.

Usually only selected persons know the URL of the website dedicated to the illegal activity, which changes frequently. These measures facilitate anonymity and make it more difficult for law enforcement to find the users and for Internet Service Providers to remove the sites from the servers. If the sites are removed, another is created and the whole process starts again (Fournier de Saint Maur, 1999).

	Traditional Aspects	Technological Facilitation	Consequences
Child Luring	Find the child (or their information)	Create a false identity and enter a teen chat room to meet potential victims	The Internet provides a place in which an exploiter can masquerade as someone younger or a trustworthy adult. They are able to gain the confidence of the child often without the knowledge of the parents. Exploiters are also able to add to their repertoire of skills by collaborating with others and creating a support network that normalizes and supports their activities.
		Locate a website that organizes tours to countries where child prostitution is legal	
	Gain the trust of the child (not required)	False identity and no face to face contact helps to gain trust	
	Convince the child to meet	Largely dependant on the skills of exploiter. No technological facilitation per se	

	Traditional Aspects[5]	Technological Facilitation	Consequence
Child Pornography	Connect to a child pornography network.	Locate a pornography website, chat room or newsgroup to get information about participating in a network	Use of software to hide the IP address or an anonymous re-mailer makes it difficult to track the perpetrators; the Internet provides a safe place to meet other exploiters and arrange illegal plans to gain access to and exploit children; the range of possible victims is likely to be larger than in the physical world.
	Create child pornography (can be connected to luring)	Digitally enhance pictures with the faces and bodies of children from other sources	
		Use web cams and/or digital cameras to photograph or record real images of children being sexually abused	
	Obtain child pornography	Purchase or download images from websites, Usenet groups, email, and chat rooms	
	Sell/distribute child pornography	Usenet facilities, chat rooms, email to share pornographic material and information	

2.2 Crimes Against Property:

Violation of Intellectual Property:

Intellectual property, defined as the right that entitles an author and his assigns to the use and profit of his work (book, video). Piracy is the most common violation of intellectual property, which is the copying and use of property without paying for or giving proper credit to the original author.

Violation of Patent and Trademark:

All behaviors that violate the laws referring to patents for inventions, inventors' certificates, utility certificates, utility models, patents or certificates of addition, inventors' certificates of addition, and utility certificates of addition (For more information see Agreement on Trade-Related Aspects of Intellectual Property Rights, 1994).

Analysis

The rights related to intellectual property laws as well as patents and trademarks are defined in order to protect several types of original products by ensuring that other people do not copy or adapt the material without the consent of the creator. The generally protected works considered intellectual property are literary works,

[5] The same individual does not necessarily participate in all of the traditional aspects.

artistic works, sound recordings, and films. Literary works encompass any original written work including computer programs (e.g. novels, poetry, letters, Web pages, email messages, and news bulletins). Artistic works include photographs, sculptures, maps, and plans. Also protected are all pictures, images, logos, and other graphics found on the Web. Sound recordings include music and lyrics, and films are any moving images or video clips. Thus, each of the protected works has components in both the physical and virtual world (McDonald, 1998).

Two different modus operandi are utilized in conjunction with the Internet in order to bypass intellectual property law. The first way is demonstrated by the known case of Napster and the presented case of Morpheus wherein there is a virtual community sharing files. The original work was created for distribution in the physical world but later becomes a digitally pirated product. The sharing of files between Internet users is the most alarming violation of intellectual property due to the large number of virtual communities that exist on the Internet who generate vast catalogues that are updated daily (Cooper & Harrison, 2001).

One problem that is created by intellectual property law as it relates to the Internet is that websites, in and of themselves, are protected as intellectual property. In some cases, however, protected websites make literary or artistic work available (e.g. a scanned book or another website) without the consent of the author. As shown in the "deep-linking" case, the Internet itself actually provides a set of technological tools that could bypass the law protection. The ability to "deep-link" to another site does not always allow the surfer to see the original author of the web page (Ciminiello, 2000). There is, however, legitimate debate regarding the utility and potential violations regarding "deep-linking." The World Wide Web has extensive amounts of information and "deep-linking" actually allows one to connect directly to a part of the site where the information the reader is searching for is located. This problem can be easily solved if website creators utilize their own logos on all connecting pages and the person who has created the deep-link explains where that particular link will take the reader. In addition, there are ways in which one can build a website that prohibits "deep-linking" to certain areas.

A more intrusive variant of "deep-linking" is the practice of "framing" in which the author of the website uses portions of other web pages as if they were his own (Smith-Kubiszyn, 2000). Finally, there is the illegal use of meta-tags as in the *Playboy case* wherein copyrighted names or works may be out of context with the page. Not only is this a violation of intellectual property law but it is also often a violation of trademark law.

The Internet provides a new distribution channel for pirated materials such as software, videos, and music. Internet auction sites in particular provide an electronic market where the sale of pirated works is quite common. The widespread diffusion of reproduction technology has led to an increase in the number of people who produce and sell pirated materials without the use of a professional studio or equipment. An extensive black market for pirated material exists and typically utilizes the Internet to sell a small portion of the total production, which is generally supported by organized crime groups who operate on either an international or a national level (Malagò & Mignone, 2001). This is logical considering only those criminals associated with piracy rings are able to develop a sufficiently large and structured system of distribution to provide several thousands of low price copies (US Dept. of Justice, 2000).

Many of the same issues highlighted for violation of intellectual property can be applied to violations of trademark and patent law, which includes two basic violations: infringements and dilution. Infringement of trademark is the most obvious and occurs when a third party uses a trademark in such a way that it causes confusion as to the source or sponsorship of the goods or services involved. Dilution is different in that a third party changes the look of a trademark but maintains the "distinctive quality" which causes the "likelihood" of confusion.

The growth of the Internet has increased the number of potential violations due to the invention of domain names (Locke, 2000). "Cyber-squatting" is the term used to refer to those cases of deliberate and bad faith registration, as well as the use of domain names in violation of trademarks. In a case of cyber-squatting, there is a conflict between two entities in order to define which corporate or physical person has the right and legitimate interest to register a particular domain name (Ott, 2000).

There are three basic types of domain name violators. Squatters or Cyber-squatters register a known trademark as their domain name intending to sell it back to the legitimate owner. Parasites register a recognizable trademark or something similar in order to advertise their business exploiting the competitors' reputation. Finally, there are the Twins or poachers who, as the owners of the domain name, have a legitimate interest to register that name because they have a company with the same or similar name. Further violations of trademark could be committed using banner advertisements. For example, a recognizable trademark appears, but when the advertisement is followed the user is connected to a website selling similar products from a completely different company. In sum, the modus operandi of the perpetrators of patent violations is the same in both the physical and virtual world. Considering this a version of commercial fraud, as the use of the Internet continues to increase so too does the risk for consumer fraud.

	Traditional Aspects	Technological Facilitation	Consequences
Violation of intellectual property and patent and trademark	Create a copy of the original work, trademark or patented technology	Utilize available computer software and hardware	The use of the Internet amplifies the consequences of a single violation due to the sharing of files between users; the lack of uniform laws on the protection of intellectual property. In addition, the vast number of websites makes prosecution and monitoring of violations more difficult and places Internet users at a higher risk for being victims of commercial fraud due to the use of comparable domain names or websites with the same appearance.
		Use recognizable trademarks on personal websites to gain a larger customer base or to sell back the trademark to the legitimate owner	
	Use copy distinctive trademark or technological characteristics to perpetrate further crimes (fraud).	Publish/quote/show a website or other protected work without the permission of the author	
		Use technological devices to bypass intellectual property protection (deep linking, framing)	
		Use meta-tags to bypass patent or trademark laws	
		Slightly alter names or graphics on websites, banners, or domain names to mislead the consumer	
	Distribute or sell unauthorized copies (Intellectual Property)	Distribute/sell pirated material via Internet auction sites or other medium that connect buyers and sellers (chat rooms, newsgroups)	
		Utilize programs designed specifically for Internet distribution (e.g. Napster)	

2.3 Crime Against Public Interest or Public Order

Trafficking of Drugs:

The physical transfer of drugs from one state to another state, or from one territory to another territory of the same state (Convention Against Illicit Traffic in Narcotic Drugs, 1988).

TRAFFICKING OF FIREARMS:

The import, export, acquisition, sale, delivery, movement or transfer of firearms, ammunition and other related materials from, or across the territory of, one state to that of another state if any one of the states concerned does not authorize it (United Nations, 2001).

TRAFFICKING OF ORGANS:

The dealing in or sale of human body parts for financial gain. The World Medical Association during its general assembly stated, "payment for organs and tissues for donation and transplant should be prohibited. A financial incentive compromises the "voluntariness" of the choice and the altruistic basis for organ tissue and donations" (World Medical Association, 2000).

ANALYSIS

The trafficking of the variety of illicit goods is virtually the same, regardless of the commodity in question. The Internet reflects the global community that we live in and the issues that plague us in the physical world are magnified in the virtual one. Many conventions exist in an attempt to curb or stop the trafficking of illicit goods on a global scale (for a review see Dyer & O'Callaghan, 1998). The success of which could be questioned as trafficking continues, apparently unabated.

Trafficking of drugs can take on two appearances; one being the illegal selling of prescription drugs without the necessary prescriptions or the arrangement for and sale of illicit substances such as cocaine, heroin and so on. The Internet can offer valuable services for those people who are homebound and would like to have their legitimate prescriptions filled and delivered to their house. This aspect of the Internet should be encouraged to grow as it increases competition between pharmacies. Further, it allows people to purchase medicine at reasonable prices. Unfortunately, some people utilize the Internet to purchase prescription drugs illegally as they may too embarrassed to ask for it from their doctors (i.e. Viagra, hair loss prescriptions) or may not need the desired the medication. The ramifications of this could be quite severe as there is no control over the quality or quantity of the illegal prescription drugs available online.

A recent report released in February 2002 by the UN International Narcotics Control Board (INCB) took an in-depth look at drugs online and found that the Internet as well as other technologies are being used more frequently by drug traffickers. The report confirms over a thousand websites worldwide offer to sell illegal drugs. The most common drug is marijuana; however, ecstasy (methylenedioxymeth-amphetamine, MDMA), cocaine, and heroin can also be purchased online. In addition to the websites, people are arranging for drug sales online (chat rooms, Internet cafes) and with cellular telephones at rates faster than what law enforcement can intercept. The exchange of money for drugs no longer needs to occur in person, as some dealers are willing to mail the drugs to a person's house. These deliveries can then be monitored using the traditional tracking systems that many courier services offer to alert the dealers of potential law enforcement interception. For example, if the delivery has been delayed the possibility for law enforcement interception is higher.

The INCB report discusses a case in which there were "31 traffickers who kept in touch with each other by using Internet chat rooms protected by firewalls…" This method was used in conjunction with encryption and "cloned" cell phones allowing them to "move hundreds of tons of cocaine . . . before being detected." They backed up the day's activity onto a computer located on a ship so if one of the computers were compromised the rest of the network would remain intact. Not only does today's technology assist in hiding the illegal activity, it also aids the traffickers to monitor law enforcement. This highlights the variety of ways in which contemporary technology can be used in support of organized crime. The sophisticated use of technology outlined here can easily be applied to organized crime activity that operates on a network basis and requires the shipment of goods.

The International Narcotics Control Board (2002) states that the ability to make illicit substances has also been enhanced by the Internet. Thus, the Internet not only facilitates the traffickers, sellers, and buyers but it also assists those who wish to make the drugs. Recipes that were once secret and could only be made by educated chemists are readily available to the public. In addition to the recipes, there are instructions on where to locate some "hard to find" substances for the process.

The former president Clinton gave an address aimed at curbing the sale of guns online, in which he cited a case of two underage boys from New Jersey who succeeded in purchasing weapons online ("Clinton announces," 2000). What is most troubling about this case is that the Internet is now providing a way to bypass the laws and regulations that have been implemented to monitor the sale of weapons. Thus, a legitimate item sold on the real market is then re-sold to someone who should not have access to guns, creating a way to supply the already substantial black market.

The trafficking of weapons has two key issues that are similar to other identified cases. One is the US Constitution and the Bill of Rights, particularly the 2nd Amendment. This amendment likely lessened the effectiveness of the United Nations 2001 conference on the illicit trade in small arms and light weapons. This creates global problems, as the US is believed to be one of the largest suppliers of weapons. This is similar to the problem created by the first amendment regarding hate speech. However, the large pro-gun lobbies that exist amplify this problem. The Internet creates another problem through the tools it offers to individual sellers and buyers as well to those who specialize in the smuggling of weapons.

Trafficking of organs has many of the same issues as those of drugs and guns. It is, however, more similar to the trafficking of narcotics as the sale of human organs is illegal in every country except for Iran. Nations, medical associations, and religions largely condemn the practice. However, as it has been demonstrated various times, where there is a demand someone will be willing to supply what is being requested. A kidney is the only organ that can be harvested in its entirety from a living person with minimal risk to the donor. With the advent of immunosuppressant drugs, the transplanting of kidneys has become a very successful operation. Thus, a market emerged and people became willing to sell their kidney to people wanting to purchase them. It appears that organized crime groups saw the opportunity to connect the buyers and the sellers, so they stepped in to take a small percentage of the asking price. Considering this is a complex operation it would likely not exist without organized criminal groups.

	Traditional Aspects	Technological Facilitation	Consequence
Trafficking of Illicit goods	Creation of Network	Use computer based communication – email, chat rooms, newsgroups, web pages, including auction sites (advertisement) – to solidify network, locate seller and advertise to potential buyers	Anonymity and ease of communication between various criminal organizations has brought about a phenomenon of co-operation. The Internet and the other modes of communication associated with it allow for relatively easy and quick transactions that are extremely difficult to trace.
	Supply		
	Advertise		
	Initial contact and negotiations and ongoing communication	Utilize Internet, email or other modes of encrypted communication to "broker the delivery and sale" of the illicit good	
	Payment	Wire transfer completed online	
	Delivery of illicit product or services	Technology only facilitates the communication during this part of process. Except in the case of drugs wherein web based couriers could be used to monitor the shipment	

TRAFFICKING OF HUMANS:

The recruitment, transportation, transfer, harboring or receipt of persons, by the use of threats, force, coercion, abduction, fraud, deception, abuse of power or a position of vulnerability, the giving or receiving of payments or benefits to achieve the consent of a person having control over another person, for the purpose of exploitation. Exploitation shall include, at a minimum, the exploitation of the prostitution of others or other forms of sexual exploitation, forced labor or services, slavery or practices similar to slavery, servitude, or the removal of organs (United Nations, 2000).

ANALYSIS

There are numerous documented cases of women and children being trafficked from one country to the next. Often the method of recruitment, especially in rural areas, is through word-of-mouth or responding to newspaper advertisements that promise legitimate jobs in another country. However, that is often not what happens. Generally, the victims end up in foreign countries without documents, forced to pay back large sums of money to the trafficker by working in the sex industry or in sweatshops. They are often threatened, coerced, and beaten if they attempt to leave or disobey their traffickers.

It is unclear at this point what role the Internet is playing in this specific crime. It is believed by many, however, that it is in fact playing a role (Hall, 2001; Vartti, 2002; Richard, 1999). The sex trade is the largest industry on the Internet and presents a variety of facades. Everything that is available in the offline world is available online. The Internet has facilitated the growth of every sexual fantasy imaginable and has offered them for sale. The advent of the digital camera has allowed creative criminals to force women into global prostitution. A woman may find herself captive and forced to do any number of sexual acts for a digital camera, which is broadcast globally as the act occurs. In the past, this occurred with black market pornography, which had a relatively small clientele in comparison.

Although there are no documented cases against mail-order bride companies for trafficking of women, it appears this may be a potential cover for trafficking operations. In general, mail order bride companies market women from economically disadvantaged countries to men from wealthier, usually western, countries. Phil Williams (1999) points out that many of the source countries for traffickers are the same as those for mail-order bride companies. There have been very few studies on the connection between mail-order bride companies and organized crime. Mail-order brides and arranged marriages are not illegal; however, trafficking women and making a profit from the sale of another human is. More attention needs to be paid to this particular area, as traffickers are likely to be attracted to the high profit margin and anonymity the Internet offers for all parties involved.

<table>
<tr><td rowspan="7">Trafficking Humans</td><td>Traditional Aspects</td><td>Technological Facilitation</td><td>Consequence</td></tr>
<tr><td rowspan="2">Recruitment</td><td>Create and distribute mass emails to potential victims</td><td rowspan="6">The internet offers virtually unlimited and anonymous access to the sex industry. The increased access to the online sex industry may have created a larger demand off-line. Organized criminals seem to be filling this demand by trafficking humans. The internet is likely to further facilitate this crime, though precisely in what manner has not yet been determined.</td></tr>
<tr><td>Create a website designed to attract potential victims and provide the information, in much the same way as newspapers are used</td></tr>
<tr><td>Demand</td><td>The increasing amount of sexual material online as well the availability of sex tours increases the demand for prostitution</td></tr>
<tr><td rowspan="2">Supply and Delivery</td><td>Utilize the internet and encrypted emails to make contact and facilitate the trafficking operation</td></tr>
<tr><td>Utilize Internet based mail-order bride companies as a cover operation for trafficking</td></tr>
<tr><td>Payment</td><td>Online wire transfers</td></tr>
</table>

GAMBLING:

The act of dealing, operating, carrying on, conducting, maintaining, or exposing any game for pay or remuneration of some kind.

ANALYSIS

In some states, gambling is legal provided certain regulatory bodies exist. The criminality of online gaming continues to be hotly debated in many countries and individual states. Given this fact, it is likely that Internet gambling will continue to be a heavily regulated and monitored activity but outright prohibition is not likely to occur. However, in a recent case, the Greek government outlawed every type of computer game including Game-boys and those found on cell phones. In addition to native citizens, many tourists face heavy fines or even imprisonment for violating this law. The first case under this new law will be tried soon and significant protest is expected (Goodwins and Loney, 2002).

Gambling is mentioned as a precursor to more serious crimes such as money laundering. Online casinos typically operate offshore and are often exploited by organized crime groups to facilitate money laundering. The credit card case demonstrates other issues that have been encountered by this industry and for the most part, are being addressed by the individual casino or credit card operator.

There are basic concerns some governments have mentioned in regards to Internet gambling. First is the issue of economics, which is especially important to those states whose main industry is gaming. If virtual casinos begin to compete with physical casinos, it could cause serious financial problems for those areas. Many states have therefore outlawed online gaming. Another concern is for the citizens who the state believes need some level of protection from this industry and its addictive side. In line with this last point is the inability to regulate underage gambling in those states that have age limitations. These are valid points and worth considering. However, more importantly is the existence of unregulated offshore environments. It is unrealistic to think gambling will be banned and thus it appears the only option is to regulate the industry and lobby for transparency in an attempt to prevent other crimes such as money laundering.

MONEY LAUNDERING:

Any act or attempted act to conceal or disguise the identity of illegally obtained proceeds so that they appear to have originated from legitimate sources (Interpol, 1995).

ANALYSIS

There are three basic steps to money laundering: placement, layering, and integration. Placement is the first introduction of the illicit proceeds into the legitimate financial system. This is often accomplished by exchanging small bills, usually used to pay for the illicit goods (drugs) and services (casinos), for larger bills, bank checks or cash equivalents. Once the tainted funds have been introduced into the financial system they are moved through a series of apparently legitimate

transactions. This creates distance between the money and their illicit source, erasing the "paper trail" and making it more difficult for law enforcement to track the money during investigations and to prove that the money comes from illegal activity. This is commonly referred to as the layering phase. The final step is integration, which includes utilizing the laundered money within the legitimate market.

The steps to successfully launder money remain the same in both the physical world and the virtual world. The Internet can facilitate each step of the money laundering process; however, it is probably more useful for layering and integration than it is for placement. Nevertheless, this is not to say that placement is excluded from the Internet; it is simply not the primary focus. In other instances placement is avoided entirely. The "Maize.Ltd" case highlights how if all the illegal proceeds are directly deposited into an account there is no longer a need for the placement stage.

As demonstrated in the "game.com" case the layering process is greatly enhanced by the Internet as it becomes increasingly difficult to follow the money trail through several jurisdictions, companies, and people. An in-depth study of money laundering and the Internet is beyond the scope of this project. The literature on this phenomenon is increasing and provides a more detailed look at this particular crime and how it relates to the Internet (see Cabot & Kelly, 1998; Haines & Johnstone, 1999; Savona, 2000).

The Internet is a haven for money launderers in that it is often fast, anonymous and one's activity can be erased with a single keystroke. Money launderers survive on anonymity and the Internet provides a number of ways, from encryption to false passports, in which one can remain unknown or change one's identity all together. It appears a large portion of money laundering activity has emerged with the introduction of online casinos and banking. These two activities have only recently gained significant popularity with the public; it is likely that as their presence on the Web increases so too will their exploitation.

This exploitation is especially pronounced when looking at the offshore community, which provides high levels of secrecy to their clients. A person can incorporate an offshore company, whose business is virtually unknown, and then create a bank account with the company name and the person who is behind that business is in effect anonymous. The Internet allows someone to do this without ever leaving his or her home. This makes it nearly impossible to trace funds and it creates immense jurisdictional problems for investigators of laundering activity.

Money laundering is closely connected to other crimes and questionable industries on the Internet primarily the online gaming industry and the various types of fraud that are perpetrated. This is not necessarily surprising; money launderers have historically utilized casinos and unsuspecting people to transfer large amounts of money through legitimate sources. The offshore community of banking, companies and casinos found on the Internet offer immediacy, security, cost efficiency and anonymity, which can be exploited by launderers, which in turn represent substantial obstacles for investigators. Lessons from the physical world however may apply in that the solution is likely to be found in the transparency of the online financial services, as is being currently attempted by several jurisdictions. Considering money laundering is how criminals stay in business it is imperative that the EU and the US find a way to cooperate to stifle its growth online.

	Traditional Aspects	Technological Facilitation	Consequence
Money Laundering	Create false documents	Utilize the various services available on the internet to manufacture or find other identities	As online banking, companies, and casinos increase so will their exploitation. Illicit money must ultimately go through a bank in order to be laundered; the issue is whether that bank is online or not, offshore or not. The worst combination for law enforcement is the online/offshore banks as it is virtually impossible to trace the illegal funds as the transfers occurs too quickly, the offshore banks are highly secretive and the identity of the account holder may not be known. All of this is magnified and facilitated through the use of the Internet
	Placement	Open accounts (banks, casinos etc.) using only a photocopy of fake documents	
	Layering	Withdraw or transfer the money to another account through the casino	
		Utilize multiple online bank accounts for several transfers	
		Exploit the multi-jurisdictional nature of the Internet, utilize or create businesses in one (generally offshore) country, transfer funds to a different country and still reside in yet another	
	Integration	Make purchases online or use online casinos to give illicit money the appearance of legitimate winnings	

GOVERNMENT ESPIONAGE:

Gathering, transmitting, or losing information with respect to the national defense with intent or reason to believe that the information will cause injury to the state deprived of the information or the advantage to any foreign nation (Blacks Law Dictionary, 1979). This crime in particular does not have a United Nations definition as it is regulated by the individual states (see previous section on theft and business espionage).

TERRORISM:

Who is considered a terrorist often depends on who is providing the definition. According to the Federal Bureau of Investigation, terrorism is defined as the "unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives" (Terrorism Research Center, 2000). In general terms, terrorism includes the use or threat of force to get another person (or group of people) to do as one wishes politically or socially. The most recent example of traditional terrorism is the September 11 attack on the World Trade Center and Pentagon in the United States. This attack has had a profound global

effect and has provided the basis for increased research in all areas related to terrorism and national security.

One area receiving increased scrutiny is how information technology could or is facilitating terrorist activities. Cyberterrorism is the word that encompasses this thought and refers to the integration of cyberspace (and all it has to offer) and terrorism. When one tries to understand what cyberterrorism is one inevitably receives a mini lesson in the art of war and its relationship to cyberterrorism and "Infowar." The book *Networks and Netwars: The Future of Terror, Crime and Militancy* (2001) edited by John Arquilla and David Ronfeldt is an excellent collection of literature on this topic. "Infowar" is something deserving attention as our dependence on technology increases and ones ability for intelligence collection becomes the deciding factor in a war. In fact, some states in the US have ordered the removal of some types of information from public libraries and websites. This was done in the hopes of lessening the abilities of terrorist groups to gather critical knowledge about various places such as nuclear power plants and federal buildings (McKinnley, 2002).

For the purposes of the current framework, terrorism easily fits into both the category of *computer as target* as well as *computer-facilitated*. The most common case studies are those that contain stories about viruses and other computer as target based crimes. However, the attack is not the only part of the terrorist operations and to think that information technology is not used by terrorist organization is to make a very grave mistake. Technology is not center stage in terrorist activities, and that is precisely point, it is "enabling different forms of . . . command, control and communication (C3)" (Zanini & Edwards, 2001, p30). The same authors highlight the fact that new technologies have reduced the transmission time and cost of communication all the while increasing the complexity of the information that is being dispersed.

It appears the best example of the use of technology can be found within bin Laden's al-Qaeda terrorist network. Zanini and Edwards (2001) discuss the information that has been gathered by reporters who visited bin Laden's compound before September 11. From those reports, it appears that this network uses very modern computer and communication equipment. According to several sources used by Zanini and Edwards, technology used by this group include satellite phone terminals thought to be rarely used by bin Laden himself. Typically, these phones travel separately from him and are used by assistants who have received messages from him and relay them in different locations. Also used within the network are CD-ROM disks that provide instruction on potential terrorist activity (bomb making, heavy weaponry, recruiting and terrorist operations).

It appears that al-Qaeda also utilizes the Web for communication. From a 1995 FBIS report that was used by Zanini (2001), it was clear that a communication network was in place that used email and bulletin boards to exchange information. This has been recently confirmed by an al-Qaeda email that was intercepted by US government officials (Risen & Johnston, 2002). This article highlights two crucial points about the technological facilitation of this particular terrorist group. One, they are using it to regroup after the war in Afghanistan which may mean that the traditional warfare that has been recently used has been largely ineffective. Second, their ability to remain anonymous is facilitated by their use of Internet cafés or other public places making it much more difficult to know their location and activities. Other technologies that are used by terrorist groups as well as organized

crime groups are cryptography and encryption. These provide a higher level of anonymity and the ability to send messages that if intercepted cannot be easily understood.

One issue that must be discussed is the terrorists ability to attack a nations critical infrastructure using a computer and causing serious damage and/or loss of life. Denning (1999) points out that as of now there has not been a substantial threat against these services; however, this will not always be true.

Information regarding terrorist activities as they exist today makes it impossible to have a specific case studies of who uses technology to carry out what activity in particular. However, the information that has been summarized in this section allows one to see how information technology can and is being used by these groups. One lesson learned is that criminals and terrorists are one step ahead of law enforcement; they are utilizing the idea of a network to survive and thrive in this increasingly global environment. If a hierarchical structure exists, it is limited and the destruction of the perceived leader does not necessarily mean the destruction of the group. Terrorism is based on a cohesive ideology that is strengthened by group membership. Technology facilitates this group membership through increased communication between members. Technology also provides the ability to recruit new members using websites, email, and chat rooms. Furthermore, it gives the group complete control over a media source. They are able to tell "their" story through various mediums to further advocate for their cause.

	Traditional Aspects	Technological Facilitation	Consequence
Terrorism	Recruitment	Provide propaganda by creating websites, email, chat rooms	Technology has enabled terrorist groups to become more strategic in their planning and provided the ability to function as a network that could continue to function if an apparent leader is killed. Increased communications lower costs and raised levels of planning and recruitment provides the possibility of launching an attack from another country with potentially devastating results.
	Command, control and communication	Use of encryption technology, email, chat rooms, bulletin boards, satellite connections, and mobile data storage devices to prepare for terrorist operations and communicate between cells	
	Direct Attack	Use of hacking strategies including viruses, logic bombs, or other malicious computer program to attack a critical infrastructure or cause a computer malfunction that would cause loss of life	

3.
CONCLUSIONS

Many researchers have produced small papers on the topic of computer-facilitated crime. They have briefly compared the similarities and differences of those crimes perpetrated on the Internet to those carried out in the physical world. This analysis however, attempts to incorporate several perspectives. This is unique in the field, in that the crimes have been assessed from legal, technological, and physical world standpoints. This has been done in the hopes that some level of insight in regards to prevention and/or risk assessment can be provided. From the prevention perspective, this provides a multi-dimensional approach to this complex problem. The other unique aspect is that it is one of the first attempts at creating a legal framework through which to analyze these crimes. It endeavors to find a common ground between the EU and the US then it takes the analysis to the individual level, highlighting the need to understand the perpetrator. If we are to be successful in our co-operation in combating computer-facilitated crime, we must first understand the motives of the offender regardless of his of her citizenship.

Organized criminals have, in all likelihood, now added technology to their repertoire of tools to perpetrate various crimes successfully. There are aspects of today's technology that all of the analyzed crimes have exploited in some way, which we will term "Internet resources," such as anonymity, the ability to affect or contact a global population, speed and widespread information exchange. These assets can be added to the already existing resources of organized criminal groups, which include violence (or threats of violence), money, and social capital (personal relationships). Each crime uses the various resources in a unique manner. For some crimes, anonymity is the most important quality whereas for others it takes a secondary role as in a classic stalking crime. Other crimes may be completed in the virtual world and are only enhanced by the Internet or technology (i.e. trafficking of drugs, arms, and humans). Finally, the perpetration of each crime improves in a unique way from the utilization of the Internet. Some of the improvements can be found in the lower likelihood of being apprehended and/or prosecuted, increased damage, higher profits, and/or lower costs. Technology can augment nearly every aspect of the criminal scheme from the damages to avoidance of apprehension. Because of this particular risk, it is crucial that the lines of communication between the EU and US remain open and the desire to cooperate stays in the foreground.

It is imperative that researchers remain aware of the risks associated with technology and its continued advancement. As technology changes so too will the risks and their subsequent exploitation. We must continue to be aware of network security and remain cognizant of computer as target crimes but we must not forget the vast number of computer-facilitated crimes as those can often be carried out by people with little computer experience and can have serious ramifications for the victims. If we are to be successful in our fight against computer related crime, we must be flexible enough to continually reevaluate the crimes that are committed and their modus operandi. Technology is an ever-changing entity; thus, we should expect those who exploit it to be dynamic in their application of it.

CHAPTER 2

COMPUTERS AS TARGETS

1.
INTRODUCTION

The famous philosopher of war Carl Von Clausewitz noted that in war, everything is very simple, but the simplest thing is also extremely difficult. Much the same could be said about efforts to categorize computer crimes and cyber-crimes – murky concepts referring to phenomena that are often elusive and difficult to define precisely. Cyber-crimes, computer crimes, and electronic crimes are often used as synonyms for one another. This is understandable as there is clearly overlap among them. Yet, they are not identical. At its broadest, for example, cyber-crime can include any criminal activity that takes place in cyber-space. This can extend from unauthorized entry into computer systems, sometimes accompanied by the theft of data (the virtual equivalent of burglaries or home invasions) or the modification or destruction of data (which can be a simple act of vandalism or part of a strategic warfare offensive, depending on the perpetrator and the motives) to cyber-dimensions of more traditional crimes such as stalking or child pornography. As for electronic crime, this encompasses a wider range of activities than computer crime, involving other electronic channels and devices such as telecommunications and cable services, which are distinct from computers. Computer crime appears a little more restrictive, but refers not only to computers as targets but also to activities in which computers are used as a medium to commit crimes. These activities can include unauthorized electronic relocation of money (bank robbery), the unauthorized acquisition of personal data (often a precursor to identity theft), false advertising efforts (fraud schemes), or the illegal copying of software.

Another complication is that even when computers are used as the medium or channel for committing a crime, the target is still usually another computer. Even the distinction between computers as targets and computers as medium, channel, or vehicle to commit crimes, therefore, is not nearly as clear and rigorous as it first appears. Moreover, computers can be targets not only for attacks and intrusions but also for theft – whether individual and opportunistic, such as the stealing of laptops from hotel rooms or airports, or planned and organized such as the hijacking of trucks loaded with computers and other electronic goods. Similarly, computer components can be targets for theft. During the 1990s theft of computer chips was a major problem in the United States and it was even suggested that kilo for kilo their street value was similar to heroin. Computer software is also a target both for theft and for counterfeiting.

At the same time, it is worth noting that items such as automated teller machines that do not take the form of traditional computers, but share many of the same attributes are subject to similar kinds of manipulation or attack. ATM crimes also illustrate the complexity of the issue of target versus channel. There are at least six ways in which ATMs can be involved in criminal activities. In the first place, they can be subject to physical theft – sometimes described as crash and grab raids. The perpetrators of such crimes range from petty criminals to organized crime groups such as the so-called YACS (Yugoslavs, Albanians, Croatians, and Serbs) who have been very active in ATM theft in the New York and New Jersey areas. Second, they can be tampered with in ways that temporarily capture customer cards. These are subsequently retrieved by the criminals (who have also found ways such as over the shoulder surfing or more sophisticated forms of surveillance to acquire information

about the Personal Identification Number (PIN) of the card-holder). Third, they can be used for fraud, with fraudulent check deposits followed by fraudulent cash withdrawals. Fourth, they can be tampered with – or false machines provided – to allow those responsible to gain access to card numbers and PINs. Skimming devices can be inserted that copy the magnetic stripe containing authentication and verification data. This can subsequently be cloned in fraudulent cards. ATMs can also be targeted more prosaically in a variant of the insider threats. There have been several cases in recent years, for example, where a firm or individual responsible for stocking ATMs with money has left suddenly with substantial sums of money – an ATM variant of the much discussed insider threat. Finally, it is possible to manipulate ATMs in ways that create transaction reversal or voiding, thereby facilitating removal of funds from an account without any record. In these circumstances, determining whether the computer is channel for committing the crime or the target of the crime is problematic to say the least.

The complications do not end there. It is not always clear what is cyber-crime, what is cyber-terrorism, or what is an act of cyber-warfare. An attack on computer systems could be any one of the three and still employ the same methodology and tools. There might be some differences in the scope of the attack, although even this is not always the case. In the final analysis, all that would distinguish one kind of attack from the other is not the attack itself so much as the objectives and the perpetrators.

The situation is further confused by the hyperbole and sensationalism that has all too often entered into many journalistic discussions of computer crimes on the one side and by the reluctance of many institutions to report intrusions on the other. Terms like cyber-terrorism, for example, are often used in ways that are both careless and inconsistent, while some hackers are given almost mythical powers. At the same time, somewhat paradoxically, computer crime is under-reported particularly by financial institutions and companies concerned about the impact on their reputation if security and confidentiality have been compromised. Thus, this area needs to be subjected to more systematic and rigorous research.

Against this background, this report is intended as a conceptual clarification of computer crimes in which computers are targets. In effect, this aims to provide a framework for analysis that will facilitate further research. The initial idea was that this would be an exercise in the creation of a taxonomy. Yet, even a taxonomy confined to computers as targets is problematic. There are several reasons for this, including the inherent difficulties of taxonomy creation. As several observers have noted, taxonomies generally have classification categories with several characteristics. First, the categories should be mutually exclusive and avoid overlap. They should also be exhaustive, in the sense that they cover all dimensions and possibilities; there should be clarity and precision about the terms that are included. The classification should be capable of replication by others and should be accepted as a helpful approach. Finally, it should be useful in that it enhances the understanding of the phenomenon under discussion (see p.2 Howard & Longstaff, 1998).

Recognizing that a formal taxonomy that exhibits all these characteristics is extremely difficult to create, the purpose of this analysis is rather more modest. It aims to provide a framework for analysis, in which empirical cases can be categorized and understood. Yet, two considerations must also be taken into account even with this more modest objective:

- It is essential both to reflect upon and to incorporate multiple perspectives. It is possible, for example, to examine computer crime from the perspective of the perpetrators or that of victims, to focus on the vulnerabilities in software, hardware, and network connections that can be exploited, or on the skills exhibited and the tools used by the perpetrators.
- It is necessary to go beyond simple laundry lists and provide a framework that both reflects the diversity of computer crime and allows different dimensions of computer crime to be related to one another.

Consequently, the creation of an analytical framework must start from a set of fundamental questions, that helps to focus empirical research but that also assists in framing the results of that research and their interpretation. In thinking about computer security, as in thinking about national security, there are certain crucial questions that inevitably arise. These are the questions that, to one degree or another, focus all research: the who, what, why, when, where and how questions. In this case, these can be elucidated as follows:

What? What precisely is being targeted? This question seems to have an obvious answer but, as suggested below, there are several different dimensions of computers and each of these is subject to different kinds of targeting. Other "what" questions exist. What is actually done by the intruders? Moreover, what are the consequences of the intrusion?

Who? Who are the perpetrators and who are the victims of crimes in which computers are the targets? Largely because of the anonymity of computer crime, as well as the capacity of the perpetrators to obfuscate both the crime and their role in it, conclusions about intruders are often inferred from incomplete evidence.

Why? Why questions generally focus on motivation issues: why are the perpetrators doing what they are doing? There are two broad approaches to answering this: one focuses on psychological motives and tries to identify the personal motivation for the behavior, the other focuses on what the perpetrator is seeking to achieve. It is the difference between "because of" and "in order to" motives. This distinction was made in a seminal study by Richard C. Snyder, H. W. Bruck and Burton Sapin, *Foreign Policy Decision-Making: An Approach to the Study of International Politics* (1962). Some studies of hackers have focused on the "because of" questions and started a process of building profiles emphasizing factors such as obsessive personalities, poor adjustment, loneliness and inadequate social skills (for a useful discussion see Taylor, 1999). The alternative approach is to focus on "in order to motives:" intruding into computers is treated as a "rational" action in the sense that those who do it want to achieve something, whether financial gain, revenge, or increased status among their peers. It is also possible to combine both approaches. This might be essential, for example, in cases where organized crime groups (composed of purposeful rational actors intent on monetary gain) recruit hackers who fit some of the psychological profiles suggested above.

How? One question at the center of many computer crimes is how are they carried out. Answering this requires obtaining some knowledge about the skills of the perpetrators and the kinds of tools they use to obtain unauthorized entry into, or otherwise attack, computers. Subsequently, how do they exploit unauthorized entry to achieve their objective? In focusing on this question, the analysis needs to reflect the dynamic nature of attack methods and the fact that they can shift very rapidly.

New tools are constantly being developed to exploit new vulnerabilities in both new software and new hardware.

When? Another set of questions is temporal. How frequent are intrusion efforts? Are they concentrated or diffuse? Do they cluster around holidays? Are they related to particular political events such as the World Economic Summits, or dyadic conflicts between states?

Where? This is an important question in relation to the location of victims, the location of perpetrators, as well as the path between the two sets of actors. Indeed, the where questions can be particularly important in determining the scope of the attack and the nature of the victims. Are the attacks directed at a particular firm, at particular kinds of companies or financial institutions, at government agencies, Internet service providers (ISPs) or particular individuals? How focused or widespread is an attack? In terms of computer crime the "where" dimension can be most usefully thought of as the scope of an attack.

This list of questions is obviously not exhaustive. Nevertheless, it provides the basis on which it is possible to develop a reasonably comprehensive framework for analyzing computer crime. Consequently, the next section elucidates the key dimensions of this framework.

2.
DIMENSIONS FOR ANALYSIS

2.1 THE COMPUTER AS TARGET

Focusing on computers as targets for crime appears to be an important but rather obvious starting point. Yet even this is not nearly as simple as it appears because of the various ways in which computers can be understood and conceptualized. Indeed, a computer can be seen in any of the following ways:

A computer as a set of functions

A computer is a functional object that carries out tasks for which it is programmed and facilitates many tasks for its users. These range from word processing and number crunching to Internet searching using smart agents, with a multitude of other functions in between.

A computer as a repository or depository of data

One of the most important attributes of the computer is its capacity to store large amounts of information in small amounts of space. Some of this data is proprietary software, some of it is specialized financial data; some of it is data belonging to people, plans and business strategies. Some of it is public but some of it is private and is restricted to those who have authorized access. The most obvious examples of this are government computers containing classified information, however many company computers have business data, which is also considered private. Other computers contain personal information such as medical history that is highly sensitive and subject to all sorts of privacy safeguards.

A computer as a system of commands

Many computers are used as control mechanisms in relation to broader processes. They automate a series of commands in ways that contribute significantly to certain kinds of processes whether industrial manufacturing, pharmaceutical production, the operation of traffic signals, and the like.

A computer as a financial depository and financial transmitter

One of the most significant developments of the last two decades has been the transformation in the nature of money. As Joel Kurtzman has argued, most money these days takes the form of megabyte money that is bits and bytes on computer screen. Other observers have talked about the development of virtual money. Although these concepts overlap with smart cards and electronic money, which is linked to e-commerce, they are essentially separate and distinct. For example, the vast majority of value transfers are in the form of electronic transactions done through systems such as FEDwire and CHIPs. Yet, as the ATM discussion above suggested, computers can also be a depository of physical money and are therefore subject to both physical and cyber-attacks to obtain unauthorized access to that money or to the data typically used to access it.

A computer as a network component

One of the most important facets of the revolution in information technology that has occurred during the last two decades has been the development of networks, consisting of nodes and connections. These include home networks where several computers are linked together, company intra-nets that facilitate internal communication and information sharing within a particular firm, and inter-firm or inter-agency networks that link together companies or agencies engaged in cooperative ventures. The most ubiquitous network of all, of course, is the Internet, a global network that transcends borders and encompasses virtually all countries from Albania to Zaire. In February 2002, it was estimated that there were 29,567,649 domain names of web sites in existence.[6] The number of Internet users was estimated at approximately 544 million, with the United States and Canada, Europe, and the Asia/Pacific region providing the vast bulk of them.[7] The following table highlights the breakdown of users.

Table 1: Estimated Number of Internet Users

World Total	544.2 million
Africa	4.15 million
Asia/Pacific	157.49 million
Europe	171.35 million
Middle East	4.65 million
Canada & USA	181.23 million
Latin America	25.33 million

The Internet is an environment or medium that promotes cheap and easy communication, facilitates commerce and business, and provides enormous opportunities for research and learning. This environment also has a dark side. The Internet can be exploited for many criminal purposes ranging from exchange of child pornography to cyber-stalking. Moreover, it provides a vast target set that ranges from individual home computers with particular kinds of information that might be useful to criminals, to repositories of personal data such as credit card information and passwords on business web sites. Internet service providers are also prominent in the target set, as are some major e-commerce sites.

A computer as part of national and global infrastructure

[6] http://www.netfactual.com/index.php?menu=25&reports=DOM

[7] http://www.nua.ie/surveys/how_many_online/

One critical aspect of the development and use of computers in the last decade has been the way in which they have come to underpin critical functions in the economic, political, and social life of postindustrial societies. In the United States, for example, several critical infrastructures exist – financial, energy, electrical power, telecommunications, transportation, and emergency management – that are fundamentally dependent on linked computer systems. Without the continued functioning of these infrastructures, much of the economy and society would be severely hampered. Indeed, so important are critical infrastructure that the United States, in February 1998, set up a National Infrastructure Protection Center under the auspices of the FBI. The Center is responsible for assessing threats, providing warnings and both investigating and responding to threats and attacks.[8]

2.2 The Objectives of Computer Crimes

As suggested above, the objectives of computer attacks can be understood either in terms of meeting psychological needs of the attacker or in terms of what the attacker is trying to achieve. From this point, it is possible to think about intrusions or attacks on a computer or a network in terms of two major purposes: malicious intent and exploitation for gain.

Malicious intent can stem from several psychological motives such as a desire for revenge or the desire to demonstrate or display skills and thereby achieve increased status with peers or within the broader hacking community. It can also include more instrumental objectives such as the desire to advance a political cause through actions that help publicize grievances or are designed to hurt those people and institutions the group is struggling against. Whatever the underlying motivation, however, the critical point about those who operate with malicious intent is that they seek one of what might be termed the "three Ds" – degradation, disruption, or destruction – as well as manipulation. From this perspective, the intent of an intrusion can be any of the following:

- To undermine, interrupt or disrupt functions or degrade them in such a way that they cause problems, difficulties, or harm, in the physical world
- To destroy data
- To degrade the functioning of the computer
- To deny access to the computer (denial of service attacks)
- To disrupt, degrade or destroy a network
- To deny access to a network
- To undermine provision of service
- To manipulate coding and alter commands and functions in ways which have harmful effects in the real world.

These objectives, of course, can be pursued by various kinds of intruders – ranging from the prankster to the terrorist, the social misfit teenager to the committed

[8] See http://www.nipc.gov/about/about.htm

political terrorist using virtual rather than physical weapons to create harmful consequences both in cyber-space and in physical space.

Exploitation in contrast, is usually about personal or group enrichment. It typically involves one or more of the following:

- Theft of money – virtual bank robbery
- Copying and subsequently unauthorized reproduction of data or software – intellectual property theft
- Acquisition of proprietary information which is later used by competitors – industrial espionage
- Acquisition of personal information that is subsequently used for fraudulent purposes. This has become a pervasive crime known as identity theft.
- Unauthorized acquisition of classified material – espionage
- Unauthorized manipulation of data to influence decision-making
- Demonstration of the capacity to exploit security vulnerabilities to destroy data or deny service and thereby provide a basis for extortion.

This last example, of course, reveals the permeability of these distinctions and is almost a combination of the two with an attack that displays malicious intent later used to provide a basis for extortion.

2.3 The Tools of Computer Crimes

In considering the tools of computer crimes there are two kinds: social and technical. The term social engineering is generally used to cover actions that manipulate people into supplying passwords and thereby facilitating unauthorized access to a computer or network.

Other social tools include spying on users as they type a password for system entry, unauthorized search for passwords that are written and stored in readily accessible places, dumpster diving for information that might provide details about access codes and so on. The social methods of obtaining access are the first two categories of attacking computers outlined by Cheswick and Bellovin (as cited in Howard & Longstaff, 1998, p.3-4) in their seven-fold classification. In their view attacks fall into one of seven categories: (1) stealing passwords; (2) social engineering; (3) bugs and backdoors – taking advantage of systems that do not meet their specifications, or replacing software with compromised versions; (4) defeating mechanisms used for authentication; (5) exploiting protocols that are improperly designed or implemented; (6) information leakage – using systems such as *finger* or the *DNS* to obtain information that is necessary to administrators and the proper operation of the network, but could also be used by attackers; (7) denial-of-service – efforts to prevent users from being able to use their systems.

Although this is a useful list, it is focused primarily on ways of obtaining unauthorized access. While these are important, the overall focus is somewhat narrow and leads to the question – after access what then? It is when an intruder has the knowledge to exploit access by manipulating, altering, or destroying the

system and its functions, or by acquiring, destroying or altering the data stored in the computer or on the network that real problems arise. For someone who is targeting the computer in order to steal a user's identify, for example, the real test is not getting in but obtaining information such as social security number, bank account details, credit card details and the like. The theft of credit card numbers is particularly useful when multiple card numbers are available. For this reason, more accomplished criminal hackers target certain types of businesses where they know the likelihood of such data being stored is high.

A more compelling categorization is that developed by John Howard and Tom Longstaff (1998) based on incidents reported to the Computer Emergency Response Team (CERT®) at Carnegie Mellon University in Pittsburgh. Howard and Longstaff identify six broad categories of tools, several of which contain some very important sub-categories.

User Commands: Traditionally, the most common means of attack was entering commands at the keyboard, opening a *telnet* session to a target computer and attempting to log in to a user or the super-user account, through password guessing or cracking, or the exploitation of a software bug.

Scripts or Programs: Attackers also make use of scripts or programs for the automation of commands. A script is a series of commands entered into a file that can be executed by a UNIX shell. Programs commonly used by system administrators to check for bad passwords, are also used by attackers to crack passwords on targeted hosts. Particularly important here are Trojan horse programs, which are programs an attacker may copy over another program on the target system. Deriving its name from the wooden horse at the battle of Troy, a Trojan horse has been defined as, "unauthorized code contained within a legitimate program [...] a legitimate program that has been altered by the placement of unauthorized code within it;" as well as, "any program that appears to perform a desirable and necessary function but that (because of unauthorized code within it) performs functions unknown to (and probably unwanted by) the user" (Anonymous, 1998, p. 236).

Autonomous Agents: Autonomous agents are "means of exploiting a vulnerability by using a program or programs, which operates independently from the user" (Howard & Longstaff, 1998, p.13). The most well known autonomous agent is the *computer virus.* This has been defined as "a program that attaches itself to other files on the target machine. During attachment, the virus' original code is appended to victim files. This procedure is called infection. When a file is infected, it is converted from an ordinary file to a carrier. From that point on the infected file can infect still other files. This process is called "replication" (Anonymous, 1998, p.159). The result can be to spread an infection through a hard drive or across a network. Although most viruses attach themselves to executable files, which infect other files upon execution, some viruses attach themselves to data files. The macro viruses in Microsoft Word are a good example and use the sharing of documents to spread or the virus, itself, causes the sharing of documents. Although viruses were initially a problem that was spread by disk sharing, as networks, email, and online information sharing have grown so have they become more ubiquitous – and more damaging in their impact. The "I Love You Virus" which began to hit computers in May 2000 was perhaps the most notable example of a computer virus. Subject to various mutations as hackers altered the original code; the virus was transmitted primarily through email messages and Internet Relay Chat.

Closely akin to a virus but an autonomous agent that that does not insert itself into other programs is called a worm. "Unlike viruses, worms are programs that can run independently and travel from machine to machine across network connections" (Howard, 1998). An early worm was the Morris Worm released by a student at Cornell University in 1988. This generated unprecedented concerns about network security. In recent years, there has been some overlap between worms and viruses.

Toolkits: Software packages commonly referred to as "toolkits" offer the capacity for what might be termed "hybrid attacks." As the name suggests they offer various tools including scripts, programs, and autonomous agents grouped together in a relatively easy to use kit. A widely used Internet toolkit is known, appropriately enough as, *toolkit*, and contains a sniffer and Trojan horse programs that can be used to hide activity and provide unauthorized backdoor entries into computers for later use.

Distributed Tool: A distributed tool is used to attack a victim simultaneously from multiple hosts. Initially attack tools are copied to surrogate sites distributed across the Internet. They are then synchronized to attack a single victim site at a pre-defined time. This has several advantages. The delay between the initial actions and the attack provide opportunities to ensure anonymity, while the coordinated attack of this kind overcomes many security precautions taken by the target site.

Data Taps or Screen Scrapers: Electromagnetic devices such as computers and network cables generate magnetic fields that can be exploited to reveal the information in the memory of the computer (particularly data displayed on the terminal), or to reveal data in transit. These can be read to provide access to the data.

2.4 The Scope of Computer Crime

One way of conceptualizing the "where?" question in relation to computer crime is to consider the scope of the target set and in particular whether any attack is random or focused. The target set can range from an individual computer to the Internet as a whole as in denial of service attacks wherein there are self-replicating tools that work their way through networked systems. Alternatively, an attack can be focused on certain targets. America Online, for example, has been a favorite mark for computer attacks designed to disrupt or deny service to its subscribers. The United States Department of Defense is another popular target with thousands of attempted intrusions each year. Targets can also be more carefully chosen. Since the late 1990s, periods of international tension between two countries have routinely included attacks on adversarial web sites. This has been a feature of the conflict between the Palestinians and the Israelis, an accompaniment to tensions between India and Pakistan. This has also been an element of the crisis between the United States and China over the downed US reconnaissance plane captured by the Chinese. There is also great concern in the United States about critical infrastructure attacks designed to undermine the operations of the financial, transportation, communication, power, and energy sectors. Other attacks are simply random attacks that work their way through the Internet disrupting access,

slowing down many services, and reduce the efficiency of businesses that increasingly use email for both internal and external communication. In some cases, these can have cascading effects on critical infrastructures.

In addition to assaults on the Internet or on critical infrastructures, there are also computer crimes that have more specific and focused targets such as banks and various businesses. In some cases, nuisance tools are even adapted for more overtly criminal activity. In August 2000, for example, a variant of the Love Bug was combined with a password acquisition program and was targeted against the United Bank of Switzerland and possibly some banks in the United States (Perera, 2000).

2.5 The Temporal Dimension of Computer Crime

As the weapons for computer intrusions have become more sophisticated, the options about how to use them have also become more varied. Some computer attacks and computer crimes can be almost instantaneous – rather like a bank robbery where the aim is to get in, get the money, get out, and get away. In other cases, however, an attack might be phased over time for maximum impact. With distributed denial of service attacks, there is what can be termed a delayed attack with an initial set up period in which a variety of host machines are, in effect, co-opted by the perpetrator or perpetrators. Some time later the actions that the hosts have been programmed to take are initiated – with devastating consequences for the targets. One important advantage of this approach is that it is difficult to trace back to the source and the perpetrators are able to maintain their anonymity relatively easily.

There are also certain kinds of computer attacks that, in effect, have a life cycle of their own. Worms and virus programs, for example, tend to cause considerable damage and disruption as they spread. Counter-measures are usually developed very quickly. Moreover, the kinds of alerts that are issued by a variety of bodies such as the FBI's National Infrastructure Protection Agency, Carnegie Mellon's CERT/CC as well as various private security companies and anti-virus software vendors, can be very important in limiting the extent of the disruption. Nevertheless, in some cases the initial virus is followed by a slight variant that can sometimes circumvent the protective measures that have been taken. In short, attacks can be instantaneous (especially when focused), delayed, phased, or simply allowed to take their course according to the life cycle of the virus.

2.6 The Perpetrators of Computer Crimes

Of all the dimensions of computer crime, the one that has been given most attention concerns the perpetrators. This is an area where several typologies and taxonomies have been created, often with some degree of overlap, using a variety of criteria. Donn Parker (1998), one of the most authoritative analysts of computer

crime, has emphasized the need to look at several different dimensions of the perpetrators, in particular their levels of skill, knowledge, resources, authority, and motives. The skill dimension focuses on social skills and covers the capacity of perpetrators to engage in the various forms of social engineering as previously discussed. In terms of knowledge, Parker (1998) suggests three levels: those who create the tools for crime, those who have the necessary knowledge and who plan and carry out crimes; and those who simply follow scripts to implement their crimes. In the hacking community, those who fall into this last group are generally referred to – in somewhat derogatory and dismissive terms – as script kiddies. They have no real skill and consequently have little status. Those who fall into the second group can include system administrators or network managers, as well as those involved in the creation of networks. Under certain circumstances, these people change roles from being upholders of network security become intruders. Those who fall into the third group are the super-hackers, those who have knowledge and skills to develop intrusion tools that exploit vulnerabilities in software and hardware. The third dimension covers resources. This, however, has become less relevant and important as access to computer technology has become more diffuse and readily available. A RAND Corporation study in the mid-1990s suggested that the entry costs for the capacity to conduct computer warfare were very low (Molander, Riddle & Wilson, 1996). The same could certainly be said for the entry costs to engage in computer crime. Even many developing countries for example, now have cyber-cafes that can be used to access the Internet and to engage in computer crimes. When discussing authority, Parker is referring to individuals who have authority over the operation of networks. As he notes, systems administrators or super-users are able to exploit their positions for criminal actions.

This leads very naturally to an important distinction that has increasingly come to the fore in computer security analysis in recent years – that between insiders and outsiders. The insider threat has come from a realization by many companies that much of the unauthorized action against their computer systems comes not from external hacking but from employees who for one reason or another are angry or resentful. Those who have responsibility at the network levels or particularly impressive skill sets are in the best position to exploit their access. More often than not, however, they have no desire to exploit their authority and access – at least under normal circumstances. When circumstances change, however, then the motivation can also change. In some cases of computer crime a systems administrator has lost responsibility and authority, or even his job – and seeks simply to strike back. In cases where the administrator is still at work, an intrusion can be designed so that the he can come to the rescue, thereby re-establishing his former status in the view of his follow employees. In other cases, those who set up networks created a back door allowing unauthorized entry to the network. Although often done as a convenience, this could also be done as insurance against being downgraded or fired. If the administrator is subsequently dismissed, the back door provides a wonderful opportunity for using access and knowledge to obtain revenge.

The final dimension of Parker's framework is motivation. He explores the complexity of motives for computer crime noting that they can include respect from fellow hackers, the desire to demonstrate knowledge of how a system works, the desire to take revenge, money, political causes, and the like. Having interviewed many hackers, he also notes many of them are poorly adjusted and engage in their criminal activities, in part, to solve personal problems. His resulting typology of perpetrators covers pranksters, hackers, malicious hackers, personal problem

solvers, career criminals, extreme advocates, and finally, malcontents, addicts, and irrational and incompetent people. He makes very clear, however, that particular criminals do not all easily fit into one category.

Two other approaches in categorizing perpetrators of computer crime are also worth discussing. The first is by Anderson (1994) and consists of individual intruders, organized groups, criminal, and espionage. The first category consists of individuals acting independently to gain unauthorized access to computers. The second category, organized groups, co-operation helps (1) to define common goals (strategy); (2) to select and research targets and develop intrusion methodologies (tactics); and (3) to use specialized skills to support the common goals (division of labor). This category is very broad with the degree of organization varying from loose affiliations with common interests to highly cohesive organizations with well-defined goals. Consequently, it covers groups such as the German Chaos Computer Club and other well-known hacking groups as well as those with political or environmental causes. Criminal groups, in contrast, are those who seek "access to a system for profit or unfair market share" (Anderson, 1994). The final category consists of those whose primary concern is to obtain access to systems or information for national, economic, or strategic objectives (Anderson, 1994). The difficulty with this is that it appears to switch the defining characteristics half way through. Initially the key distinction appears to be whether the perpetrator is an individual or a group then it moves to espionage versus crime. The difficulty is that individuals as well as groups can engage in crime and espionage.

Perhaps a more useful taxonomy is that by Marc Rogers (1999) who divides hackers into seven distinct (although not mutually exclusive) groups: tool kit/newbies (NT), cyber-punks (CP), internals (IT), coders (CD), old guard hackers (OG), professional criminals (PC), and cyber-terrorists (CT). These categories are seen as comprising a continuum from lowest technical ability (NT), to highest (OG-CT). The first category consists of the script kiddies mentioned above. "The CP category is compromised of persons who usually have better computer skills and some programming capabilities. They are capable of writing some of their own software albeit limited and have a better understanding of the systems they are attacking. They also intentionally engage in malicious acts, such as defacing web pages, and sending junk mail (known as spamming). Many are engaged in credit card number theft and telecommunications fraud" (Rogers, 1999). The internals are the disgruntled employees or ex-employees discussed above as insiders. The old guard group is at the top of the skill range but have no desire to commit crimes beyond demonstrating their capacity to hack into systems. The two most dangerous categories are the professional criminals who combine expertise with the desire for gain and cyber-terrorists who combine expertise with malicious intent (Rogers, 1999).

In attempting to draw on these categorizations to develop a framework, there are several observations worth making. First, motivation is considered not in terms of psychological factors, but rather in terms of objectives of the actions (i.e. what they were seeking to achieve). Second, it is important to recognize - and Parker (1998) makes this very clear under the heading of what he terms collusion - that those with real knowledge and expertise about computers and networks can be recruited by those who are criminals interested only in profit. This appears to be a particularly significant trend in Russia where traditional criminal organizations have recruited hackers (through coercion or bribery or a mix of the two) into carrying out

computer crimes on their behalf. With this in mind, the perpetrators can be considered as follows:

- *Script kiddies* are essentially mischievous and engage in what is little more than cyber-vandalism. Indeed, the analogy between vandalism and the kind of activities engaged in by many young would-be hackers is a compelling one, not least because in both cases, there is a tendency to graduate to more serious activities.
- *Serious hackers* with real knowledge and skills who have the capacity to inflict significant harm on individual computers or networks to which they gain unauthorized access. The creator of the "I Love You Virus" was a Filipino student concerned with demonstrating his skills and as a result unleashed a worm that cost businesses in the United States and elsewhere billions of dollars.
- *"Hacktivists"* who pursue political causes through political action and extend this into the cyber-world, using intrusions as a political statement and political weapon.
- *Amateur cyber-warriors* who engage in hacking and web site defacement in support of their government during periods of tension, crisis, or war. These can be individuals, small close-knit groups, or looser networks of affiliation.
- *Insiders* or former insiders who become disgruntled and have both the capacity and the motivation to inflict harm on their employer's computer network.
- *Criminal hackers* who decide to use their skills for criminal profits and engage in some kind of online theft, whether of money, identity, or intellectual property, or use their computer skills to highlight network vulnerabilities as a precursor to extortion. This does not include those who illegally download copyrighted music or videos for personal use. It does include those who organize intellectual property theft online as a means of making money.
- *Criminal organizations* that include either computer experts or that recruit such experts for various theft and fraud schemes and extortion.
- *Free-lance individuals* who engage in industrial espionage by obtaining unauthorized access to computer systems and networks of target companies.
- *Organized groups* that engage in industrial espionage by obtaining unauthorized access to computer systems and networks of target companies.
- *Cyber-spies* who seek to obtain unauthorized access to national security related computers and networks of target governments. These can be individuals or groups but are generally linked closely to intelligence services.
- *Cyber-terrorists* who exploit the Internet and attack computers to cause dislocation, damage, and destruction in the physical world. In effect, only the means of attack differ from those used by more traditional terrorists.
- *Cyber-warriors* or information warriors who attack computers and networks in rival countries as part of a geopolitical contest or hostilities and act on behalf of national governments. Although such activities are better categorized as acts of war than as criminal actions (even though computers are the targets) they are included here for completeness.

This list is based on variations in knowledge level, and differences in intent. It also seeks to make clear those instances in which the distinction between individual and group matters and those in which it does not.

3.

A FRAMEWORK FOR ANALYSIS

Having elucidated the various dimensions of computer crime, in which computers or networks are the targets, it is necessary to put these together in a comprehensive scheme that provides a set of categories within which individual incidents can be identified and understood. Figure 1 summarizes this scheme and brings together each of these dimensions and highlights the variety of potential paths that a particular crime or attack can take.

There are several observations worth making about this framework. First, it highlights the wide variety of plausible paths that can be followed to commit computer crimes in which computers are the target. Each layer or table contains a number of possibilities ranging from 12 (types perpetrators) to four kinds of phasing. Consequently, with seven different layers, the number of possible variations is enormous. Second and qualifying this first observation somewhat, there are certain logical links between these dimensions, so that not all possible paths are equally likely or plausible. Indeed, perhaps the major determinant is the objective that intruders seek to achieve. This will generally determine the target set and, in many cases, the tools that are used. Criminal organizations, for example, are more likely to target those computers that act as financial depositories or transmitters than they are infrastructure components. Similarly, for this purpose they will use tools that allow them unauthorized access and the capacity to manipulate rather than tools that disrupt, degrade or deny. Yet, they might also use denial or disruption tools when they want to highlight vulnerabilities as a basis for extortion. Conversely, distributed denial of service tools, for example, are particularly useful for disruption or vandalism but not necessarily for exploitation – apart from the extortion scenario. Similarly, certain objectives would only be pursued by certain kinds of group. This provides the basis for considering the modus operandi of computer criminals when computers or networks are the targets.

Figure 1

Perpetrators

Script Kiddies	Serious Hackers	Hacktivists	Amateur Cyber-warriors	Insiders or former insiders	Criminal hackers
Criminal organizations	Freelancers in Cyber- espionage	Groups - business Cyber- espionage	Cyber-spies (States as targets)	Cyber-terrorists	Cyber-warriors

Objectives - Exploitation

Theft of money	Intellectual property theft	Acquire proprietary information	Acquire personal information for fraud	Acquire classified material	Manipulate data for decision-making	Highlight vulnerabilities for extortion

Objectives - Malevolence

Disrupt	Degrade	Destroy	Deny	Interrupt	Manipulate

Tools

User commands	Scripts or Programs	Autonomous Agents	Toolkits	Distributed Tool	Data Taps

Scope of attack: Random or Focused

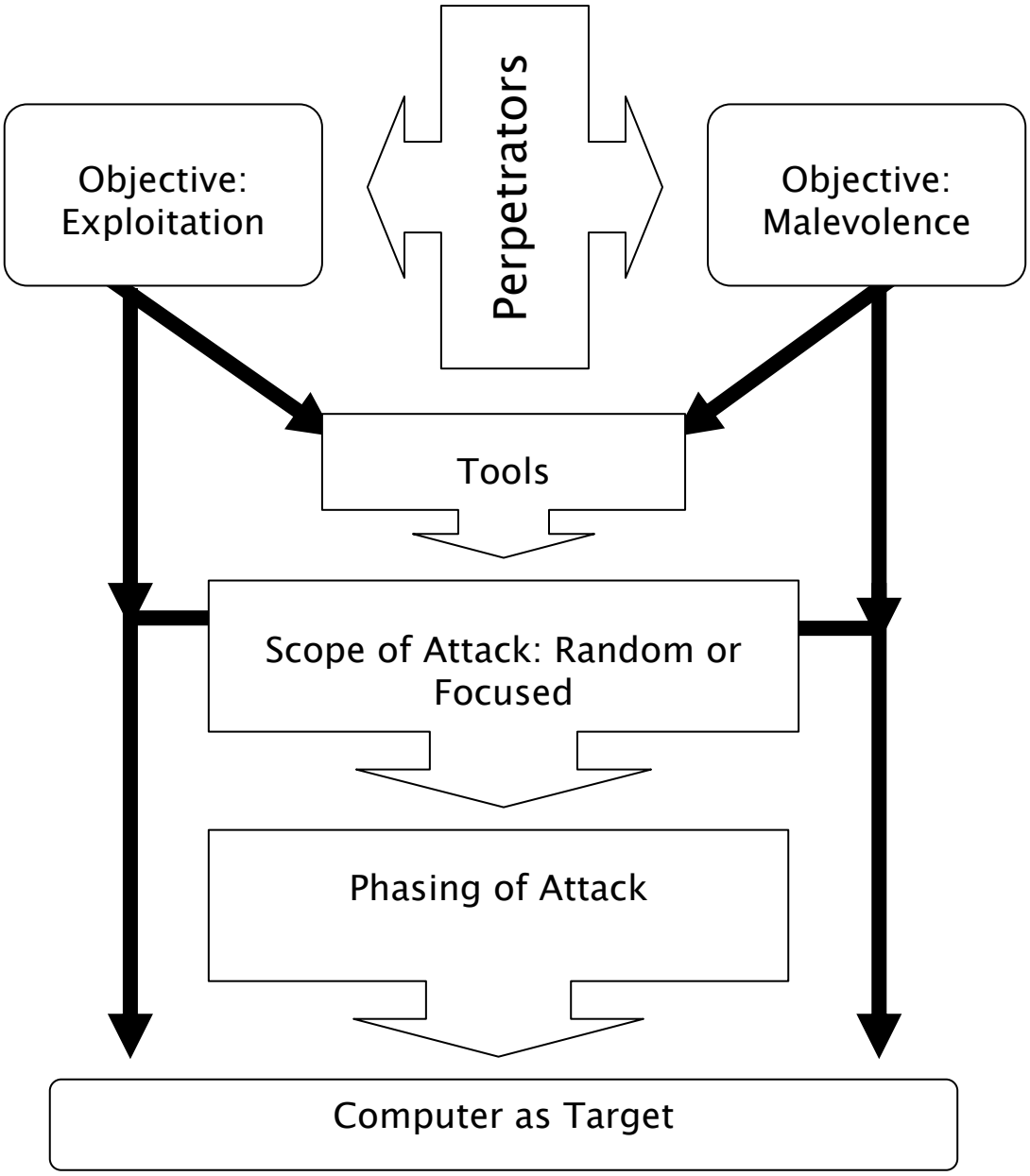
Single computer or website	Specific firm, institution or network	Service providers	Swarm attack on multiple targets	Internet wide attack	Critical infrastructure

Phasing of Attacks

Instantaneous	Delayed (e.g. DDOS)	Phased	Life Cycle

Computers as Targets

Functions	Data	Commands	Financial depository or transmitter	Network component	Infrastructure component


Perpetrators
Objective: Exploitation
Objective: Malevolence
Tools
Scope of Attack: Random or Focused
Phasing of Attack
Computer as Target

4.

THE MO OF CRIMINALS WHO TARGET COMPUTERS: A PROCESS ANALYSIS

In thinking about how to analyze the actions of criminals who target computers, there are several kinds of methodology that could be adopted. It might be possible, for example, to conduct a series of interviews with convicted criminals in order to identify the objectives they were seeking to achieve. An alternative approach is methodically identifying the stages of what are obviously relatively complex criminal actions. In criminology, such an approach has been used to explain the commission of some crimes – and has been elaborated as the crime scripts approach (Cornish, 1993). In essence, the development of crime scripts is simply a way of modeling complex crimes. It uses notions of sequential activities and can operate at several different levels of generality. Indeed, the script concept is sometimes elaborated in considerable detail with a range of additional concepts such as meta-script, proto-scripts, universal scripts, script tracks, and the like. Some observers have delineated various steps within scripts in terms of such categories as preparations, preconditions, instrumental preconditions, actualization, and post-condition prior to exit (see Cornish, 1993 for more detail).

In the final analysis, however, the crime script framework is no more than a process model. It simply disaggregates criminal activity into a series of steps that occur when a crime is committed. Nevertheless, it can be extremely useful both as a means of understanding specific crimes more fully and as a way of identifying possible reasons for failure. In addition, it can help to illuminate potential intervention points that might provide opportunities for introducing some kind of environmental or protective measures that might make the successful commission of the crime more difficult. Even so, the key is not the script framework so much as the process methodology that breaks crimes down into their constituent components, following a logical sequential flow but with illumination of the possible obstacles and the courses of action that might be necessary to circumvent these impediments. The following analysis uses a process model to decompose the stages and measures involved in several kinds of crime: a revenge attack, a crime for monetary gain, identity theft, a complex crime – compromising an e-business and manipulating stock, and an example of extortion using a swarm attack (for the concept of swarming see Arquilla & Ronfeldt, 2000).

4.1 THE REVENGE ATTACK

In the revenge scenario, it can be an insider or an outsider and the action that he takes is some kind of attack on the computer systems of an individual or company that he believed has wronged him. The aim is to inflict damage on the computer system or systems in order to inflict harm on the target person or company. There are multiple stages in this process.

1. The crystallization of the determination to get even in some way with a particular person or entity, which has done something that, has bred a serious

desire for revenge. The ultimate target for the revenge could have been someone who stole his ideas, a boss or company that fired him, a company that did not promote him fast enough or made him redundant. In a sense, the rationale for the revenge is simply the starting point for the commission of the crime in which a computer or computer network is the target. The process of getting revenge, however real or spurious the grievance might be is a rational one rather than automatic or not thought out. The individual concerned thinks carefully about what would hurt the victim in ways that would satisfy the desire for revenge. It might be the collapse of a business or simply the loss of a great deal of money. Whatever the level of hurt the perpetrator wants to inflict, he will settle on a set of actions that promises to damage the putative victim enough to satisfy this desire. It is possible, however, that as the action unfolds this will change, and the level of desired hurt will be increased.

2. The use of special knowledge on the part of the person seeking revenge. By special knowledge is meant something that is not generally known or something that is not a matter of public knowledge. If the person is an "insider," he might have particular knowledge of a company's computer network. If he is an outsider, he might have knowledge of a person's habits. The critical point however, is that this knowledge can be levered in ways that allows the perpetrator to identify and exploit a vulnerability. In effect, there is an internal search on the part of the would-be perpetrator, of how the special knowledge could be transformed into an asset. This paves the way for the planning stage.

3. At this stage, the perpetrator identifies what he needs to do to actually carry out the revenge attack. This involves the creation of hypotheses about vulnerabilities related to the kind of action he is considering. This is accompanied by an internal risk assessment: if this vulnerability is exploited, is he likely to be caught? If the risk attached to a particularly option is too high, then other vulnerabilities will be considered. Eventually a particular option is chosen.

4. The probing stage. The perpetrator probes for information on the vulnerability to assure himself that it is real and can be exploited. This might be done through social engineering or through acquiring particular tools to exploit the vulnerability. All the actions, however, are characterized by stealth.

5. The final preparation phases. At this point, the perpetrator takes the final steps ready for execution. This can involve electronic steps, physical steps, or combinations of both.

6. The execution of the plan. Once everything has been set up, the perpetrator decides to initiate the action. If he begins to execute and finds that something is amiss or not working he might abort and go back to the option set or, (less likely) decide to exit completely. If everything works as planned, however, the action that gives him the revenge he seeks will be carried out.

7. The assessment. The perpetrator wants to ensure that he is effective. Consequently, he needs to know that his actions actually hurt the target. This requires some type of evaluation. Again, this might involve social engineering or some kind of probing. If he is satisfied that the action had the desired impact and he has inflicted his revenge to his satisfaction and nothing can be traced back to him, the episode is over. If his attack worked, but he decides it

is still not enough and he is not at risk, the process will start again for an additional attack. If he finds something that has put him at risk, he may decide to flee.

4.2 Crime for Monetary Gain

The purpose in this case is not revenge but some kind of financial gain. The key difference from the previous case is that there is not, at the outset, a specific victim.

1. Deciding to carry out the crime. In this case, the special knowledge, expertise, or skill is the starting point and the determination to exploit this knowledge for illegal financial gain. It is only after this that a particular vulnerability is identified (the knowledge of the vulnerability was one of the starting points in the revenge attack) that can be exploited.

2. Target selection, planning and preparatory steps. An appropriate target is identified and preparatory steps are taken in a way that parallels the revenge attack. These steps include planning and probing to ensure acquisition of all the information and the tools necessary for the plan to be implemented. This covers stages 3, 4, and 5 in the revenge attack.

3. Execution of the plan. The implementation of the plan results in one of three outcomes: unexpected obstacles arise and it is aborted; unexpected obstacles arise and they are overcome; everything goes smoothly and the plan is executed. There are also three parts to the implementation: a cyber component, a communication component, and a physical component. The cyber component involves breaking into the system and changing or extracting data to force the impact of the crime. The communication can be done through the telephone or electronically and can be done by someone linked to the main perpetrator. It is done to clarify the nature of the transaction and to verify that the transaction is being completed. The third component is physical as on occasion it will be necessary to have a physical presence, including for the final extraction of the money.

4. The end-game. In this case, there is no need to evaluate the impact – the criterion is simply was the money received? If the money was obtained, the perpetrator can either flee or change his identity and enjoy his ill-gotten gains.

4.3 Identity Theft

There are some variations on the earlier themes and phases in this – partly because insider information and special knowledge or skills are less important and probing for information is more important. The targets in this case are computers as depositories of information. Much of this information is used for perfectly

legitimate purposes such as credit checks. What makes this different, however, is that there are multiple probes to obtain a holistic view of the person, and the use of this information by the perpetrator as if it is his own. The crucial decision point concerns the adequacy of the collected data. Is it enough information for the perpetrator to carry out transactions as the other person? When this decision is made, the perpetrator can then either make a one off transaction using the victim's identity or can use the person's identification for multiple transactions over a long period. The extent to which and the occasions on which the stolen identity is used will depend in large part on the criminal's risk assessments. There are likely to be variations in style here with some perpetrators exploiting the identity of a few victims to the maximum while other criminals exploit each victim less but have more victims.

4.4 A Complex Crime – Compromising an E-Business and Manipulating Stock

Although this crime involves computers as targets, with an intrusion into an e-business and compromise of the system, money is actually made through stock manipulation and involves public disclosure of the compromise. This crime involves selecting a target company, taking action that will lead to a sharp drop in the price of its stock, and making money by selling short.

The stages of the crime are as follows:

1. Selection of the target company. The target is likely to be a flourishing e-business that has maintained a good stock price by creating confidence in its product or service as well as in the security of its transactions and data. It is a company that has in its possession proprietary material on its customers and can be significantly hurt by unauthorized access or acquisition of this material.

2. Compromising security. This is done through the recruitment of individuals on the fringe of the hacker movement who want to gain status. It can be done anonymously. Once recruited, the hackers are equipped and motivated. There is preliminary surveillance and probing for vulnerabilities followed by the intrusion itself. Several hundreds of dollars might be paid to the group for proof that the target has been compromised.

3. Disclosure of the compromise to the local, national, and financial media. This can be done anonymously, perhaps with the provision of some evidence of the compromise.

4. Acquiring the proceeds from a precipitous decline in the price of the stock.

Throughout this process, there is a concern with risk management. The organizer of the crime maintains anonymity throughout in relation to the hackers. He uses public access emails rather than a dedicated personal account. Moreover, the short selling is done in a way that appears to be attuned very closely to public information rather than depending on any insider knowledge. Consequently, deniability is high and there is no more than circumstantial evidence linking him to the compromise or the public leak. Several problems could arise. Such as, the

hackers might not be skilled enough; the proof of compromise might not be convincing enough to create a stock depression, or the timing might be messed up so that the short sell does not occur or stands out like a sore thumb. So long as these are avoided, however, the crime could be very lucrative.

4.5 Swarming and Extortion

This is a crime involving large-scale extortion through denial of service attacks. It involves the following stages.

1. Choice of targets, timing, and demands. The first task is to identify the list of targets of sites and companies that could profitably be hit. These are likely to be profitable vibrant companies that depend critically on Internet access. The choice of timing is also important and could be a time close to the deadline for FCC filings. Alternatively, late November would be a good time to attack e-commerce sites so that they are in danger of not being ready for "Black Friday" (the day after Thanksgiving in the United States is the biggest shopping day of the year). This could induce panic. The third critical choice is how much to demand. Here there might be a significant tradeoff between the number of victims and the amount of money demanded from each. The key, however, is to keep the demand much lower than the costs that are otherwise incurred thus the victim has no hesitation about complying.

2. Choice of weapons. The method of attack is what can be termed an "uber virus," which strikes through a large number of vulnerabilities and is very fast moving (akin to a flash worm that might take as little as 15 minutes to cross the Internet). It is launched from 15 or more locations. These are chosen based on free hosting and low security so that they are easily compromised. The payload is three fold: (1) a distributed denial of service attack against 20 to 30 randomly selected sires on the list; (2) a local program to wipe the hard drive and crash the computer after a designated time: and (3) a key encoded stop command that is concealed. In effect, such an approach would cross hacker cultures and combine virus writers with DDOS people.

3. The Attack. The launch of the attack is likely to have an immediate impact. It is followed by demands to the targeted companies for a payment into an offshore bank account in return for a cessation of the attack. This might be accompanied by a temporary halt to the attack to demonstrate the capability to stop it.

4. The Payoff. The money is sent to a walking account (i.e. it is sent to an account in a bank in an offshore financial center in which the bankers have instructions to send it on to an account elsewhere). This might be done several times using a variety of jurisdictions that are widely separated geographically in order to complicate and confuse the money trail. If this is successful then the biggest problem subsequently will be to use the money and remain invisible.

All these scenarios depict crimes that are feasible, have a strong probability of being successful, and in some cases offer a prospect of high payoff either financially or in terms of personal satisfaction. They are also low risk for the criminals. Indeed, the next section considers the whole issue of risk management in relation to computer crime.

CHAPTER 3

RISK MANAGEMENT

1.
COMPUTER CRIME AND RISK MANAGEMENT

Risk – the likelihood of suffering some type of harm and invariably involves some level of uncertainty.

The initial task was to create a scale of risks, however, a scale implies something that has equal intervals and can be applied in a uniform manner. During the course of creating the various frameworks, it became clear that a scale of risks would not be very useful and would invariably change depending on the culture, the individual, and the available technology. Risk is something personal and must be determined on an individual basis, for the person, the business and for the singular country. More appropriately, the topics discussed are risk assessments and how they can be used to create a personal scale of risks. Researchers should continue, however, to strive for a concrete scale of risks or a type of dynamic instrument that could be used and applied in a particular context. We must continue to gather data in a systematic way and learn more about how the individual interfaces with technology in order to make this goal realistic and useful.

Several components of risk must be taken into consideration. First, there is a difference between actual and perceived risks. People generally behave according to perceived risk regardless of the validity. Renn (1998) outlines four biases that exist for individuals who complete their own internal risk assessment: availability, anchoring effect, representativeness, and avoidance of cognitive dissonance. If one is able to immediately recall something, or has experienced a particular event, that activity is considered more likely to happen than what the actual frequencies may be. If information is provided that contradicts what is already known, people tend to ignore the information or distance themselves from it in some way to reduce their level of cognitive dissonance. Cultural issues also influence the types of risks one perceives and is willing to take. This is particularly important and presents even further problems when one is trying to create a scale of risks that can span the Atlantic.

Most lay people are familiar with risk and how it relates to car insurance. Based on historical data the insurance company assumes a certain level of risk. For example in the US, insurance premiums for cars are typically higher for single people, under the age of 25, because historically they have had more accidents and are likely to engage in more "risky" behavior (driving fast, not wearing a seatbelt, loud music) then their counterparts who are older and married. This is a clear way to identify risk and its subsequent cost. Law enforcement gathers the information on accidents, it is analyzed, and certain patterns emerge. In this case the trend is that younger, single drivers are more likely to get into auto accidents. Insurance companies then use that data to set premiums and assess how much risk they are willing to take to insure this particular group of drivers. To define risk in the arena of computer-facilitated crime in this manner is difficult at best, because the historical data simply does not exist. For some crimes, particularly fraud, the data is beginning to be compiled in a more systematic fashion and generalized risk assessments will become increasingly useful and accurate. However, one must bear in mind that the fundamental basis of random probability for the occurrence of a particular event does not exist when assessing computer crime as it does in the car insurance arena. Furthermore, the public and the private sectors are still striving for

a common language. Until that is accomplished, a scale of risks is premature, as a common understanding of the crimes and the subsequent risks does not yet exist.

Risk assessment is an ongoing and dynamic process that requires continued attention from individuals concerned with security who have the appropriate level of knowledge (Broder, 2000). In the case of computer-facilitated crime, a dual assessment of risk must take place. The first assessment must take place at the user level - their use and knowledge of technology- followed by an evaluation of the actual amount of computer security used and what is available. In order to conduct a risk assessment Power (2001) identifies five areas that must be taken into consideration: assets, threats, vulnerabilities, impacts, and safeguards. These must be identified and evaluated on an individual basis and ultimately a unique conclusion can be designed for each situation.

In light of the five areas outlined, a scale of risk could be created for the particular situation that is important to the individual, business, or national interest. The following example is provided in order to understand the first steps in making a risk analysis. However, the following caveat must be provided; risk analysis must be done on a regular basis and should include all of the available information. This is particularly true for companies and nations who must contend with larger threats from a variety of places. The examples are provided for reference purposes only and are meant to initiate a more in-depth discussion on the complex issues of risk analyses as they relate to computer-facilitated crime.

A good example of what is meant by the need for a dual risk assessment can be found in the case of Elle McPherson within the *blackmail* section. Using the five areas outlined by Power, the following thought process is initiated. Her *assets* include her overall net worth, which also includes her reputation and status as someone who is famous. *Threats* can be from anyone who wants to exploit or tarnish her reputation, someone who wants to steal her assets, or someone with a more complex agenda such as a stalker. *Vulnerability* is the portion of the assessment that needs two sections, one as it specifically relates to the use of technology and the other as it is associated to the particular person or group. In this case, let us suppose she is aware of the threats and takes all the necessary precautions in the physical world to protect her assets but does not safeguard her computer. She uses simple passwords and leaves her computer connected to the Internet or vice versa (weak physical security and strong computer security). To make the example more complex, she may be well informed and uses the latest and most effective security for everything because she knows she is a likely target given her fame. Nevertheless, the perpetrators stole information in a traditional way and then used it in a non-traditional method, which was largely out of the control of the victim. What she, or even a qualified professional, may have assessed to be a vulnerable area may not have been considered in this case. This is particularly true in light of the current technology that could be used to alter photographs to appear authentic. This same crime could have easily been committed without the original traditional theft.

The *impact* in this case, as demonstrated in the case study, is clearly the loss of money and/or reputation, which includes future earnings. *Safeguards* for someone in this position are primarily things that can be done after the fact given the likelihood that she (being a person of means and knowledge of her risks) takes all the necessary preventive measures to protect herself. In this case, her safeguard is a good lawyer and bodyguards with very little that can be done on the technological

front. To complete the risk assessment the costs and benefits are weighed – is it worth it to implement the necessary safeguards given the threats? This is then integrated into the personal knowledge of the person or company and a final scale of risks is created.

The process of identifying the five areas does not change from person to business to nation state. However, what is placed in each of these categories does. In each area the amount is increased. Assets are higher, which is likely to increase the threat, followed by increased impact (monetary, reputation, security). This leads to the part of vulnerabilities and safeguards over which the individual, business, or nation state has more control. These in turn must be weighed against the first three areas.

A second example: A fledgling company determines they are at risk for fraud because those who want to commit fraud know the likelihood of prosecution is low. First, the company may not have the capital to press charges if the crime is discovered and second they will probably not disclose the fraud for fear of losing customers. How much then is the company willing and able to pay for technological and staff safeguards to protect what few assets they have? Would the implementation of safeguards at a level lower than advised, or not at all, be favorable in terms of a cost benefit analysis? This takes us full circle to the original dilemma; what is their relationship and view of risk from a psychological or cultural standpoint? For example, the company pays for a risk assessment, the professional provides a unique scale of risks for that company, and they decide to disregard the identified risks and use low-level security measures. If they are targeted, they have decided they will risk the crime and associated costs for their own reasons, be it personal or business. This obviously is influenced by the biases previously outlined.

The risks associated with computer-facilitated crime have been outlined (i.e. anonymous, fast, and multi-jurisdictional), however, this is not the only list, and for some crimes, one aspect should be given more weight than another. In our analysis, we have tried to highlight those aspects we consider the “riskiest” for each crime. As always, much is dependant on the victim, perpetrator, and the location of the crime. Today risk analysis is focused on firewalls, passwords, anti-virus software, encryption, and connection to the Internet – all of which can be appropriately analyzed and followed by concrete actions. The problems come about when the human factor is considered. At that point risk assessment and the subsequent creation of a unique scale of risks depends on the resources and the social and technological skill of the perpetrator (hacker or not) as well as the resources and knowledge of the victim.

The issue of risk in relation to computer crime can be further divided into two contrasting perspectives. The first is that of the criminal. One of the primary considerations that makes computer crime low risk for many perpetrators is what Jeremy Kinsell termed “jurisdictional voids” – there are many jurisdictions where there are, as yet, no legal or even regulatory framework making unauthorized intrusions into computers – for whatever purpose – a criminal act. This can provide protection for computer criminals in the event they are caught. “The Love Bug,” for example, was traced back, by the FBI, to a student in the Philippines. Yet, there was no law under which he could be prosecuted

Even when it is a prosecutable offence, it is not clear that the punishment is commensurate with the kind of harm that is inflicted. Some estimates, for example,

placed the global economic impact of "The Love Bug" at about 6 billion dollars. While there are problems with such estimates, the diffusion of the cost is such that much of the impact is lost. If the costs and risks were more centralized then there would be more effective and vigorous responses to computer crime.

There is an obvious lack of reporting. For banks, non-bank financial institutions and many businesses that depend on trust and consumer confidence there is a natural inclination not to report intrusions and other computer crimes, whether successful or not. The perception is that acknowledging one's system has been compromised is a route to a public relations disaster that can drive away customers and place the firm at a long-term competitive disadvantage. This very fact can be an important source of advantage for criminals as some of the examples of crimes demonstrated.

What makes all this more disturbing is that organized crime is increasingly becoming interested in computer crime. Indeed, this provides a new set of risks that will need to be taken into account. There are several reasons for the growing involvement of organized crime in computer crime. Significantly, the anonymity of the Internet makes it an ideal channel and instrument for many organized crime activities. The notion of a criminal underworld implies a murkiness or lack of transparency. Secrecy is usually a key part of organized crime strategy and the Internet offers excellent opportunities for its maintenance. Actions can be hidden behind a veil of anonymity that can range from the use of ubiquitous cyber-cafes to sophisticated efforts to cover Internet routing. Consequently, the synergy between organized crime and computer crime is not only very natural but also one that is likely to flourish and develop even further in the future. The Internet provides many lucrative targets for crime and enables them to be exploited for considerable gain with a very low level of risk. For organized crime, it is difficult to ask for more.

If organized crime is becoming more sophisticated and crossing into areas that traditionally have been categorized as white collar or economic or financial crime, its inherent and traditional willingness to use force and intimidation is well suited to the development of sophisticated cyber-extortion schemes that threaten to disrupt information and communication systems and destroy data. Extortion schemes are sometimes bungled, but they can be conducted anonymously and incur only modest risks, while still yielding high pay-offs. This might already be a form of crime that is significantly under-reported. Yet, it is also one that we can expect to see expand considerably as organized crime moves enthusiastically to exploit the new vulnerabilities that come with increased reliance on networked systems.

Against this background, it is not surprising that there are growing network connections between hackers or small-time criminals and organized crime. In September 1999, for example, two members of a US based group known as the "Phonemasters" were convicted and jailed for their penetration of the computer systems of the telecommunications companies MCI, Sprint, AT&T, and Equifax. One of those convicted, Calvin Cantrell, had downloaded thousands of Sprint calling card numbers. They were sold to a Canadian, passed back through the United States, resold to another individual in Switzerland, and finally the calling cards ended up in the hands of organized crime groups in Italy. The more relevant connection to the theme of computers as targets of crime is that organized crime will increasingly recruit skilled hackers to conduct intrusions for various kinds of theft as well as for purposes of extortion.

The other side of the risk equation, of course, concerns the targets of computer crime. In considering the responses of businesses, governments, or even individuals who are concerned that they might be targets of computer crime it is important to recognize that a comprehensive risk management approach is essential. This requires preventive and defensive strategies (such as the deployment of firewalls, constant applying security patches to both new and old software to eliminate both well-known and recently discovered hardware and software vulnerabilities) as well as plans to mitigate losses in the event that these other measures prove insufficient. Data backups and contingency plans are essential in a world where the risks of computer crime are not only inescapable but are increasing as companies become more dependent on them. It is one of the new realities of an era in which dependence and sophistication have become sources of vulnerability and in which, to paraphrase Clausewitz, computer crime has become the extension of computer use for malicious and illegal purposes.

In the end, however, the primary actor is an individual using a machine. Thus one must eventually return to the singular person and ask how many individuals know the dangers of leaving a computer connected to the Internet through a dedicated server line? As those computers provide the launch pad for denial of service attacks, for example. How many people know that computers come with security settings but are set by the manufacturer at the lowest setting or are disabled all together? How many use strong passwords and technology to protect their privacy? The answers to these questions are all directly related to risk for all persons and entities concerned. It is, again, the individuals' computer that is used in larger attacks on businesses and nation states. Thus, the problem comes to one of information and education for the individual consumer. It is not that a person must know everything about technology. It is that we need informed consumers who are aware of the dangers and can evaluate their needs and their risks. This leads directly to the question of what is being done to prevent both *computer-facilitated* and *computer as target* crimes on all levels, legislative, industrial self-regulation, and informative or instructive measures.

PART II

PREVENTION STRATEGIES, PRIVACY, AND E-COMMERCE

CHAPTER 4

COMPUTER RELATED CRIME PREVENTION STRATEGIES: UNITED STATES OF AMERICA AND THE EUROPEAN UNION

1.

PREVENTION STRATEGIES FOR COMPUTER RELATED CRIME

As demonstrated previously regarding the various terms for computer related crime, the language we choose to use is crucial to our co-operation as it either facilitates or hinders our progress. The two primary topics in the field of computer related crime are security and prevention. The *most important* prevention strategies, whether one is speaking of the European Union (EU) or the United States (US), cannot currently be identified as the topic is simply too new. Historically, computer crime legislation has been repressive in nature and has not addressed computer crime prevention per se. Today we are more concerned with prevention, as it is becoming increasingly clear that repressive laws are not effective methods to combat computer related crime.

The best way to understand the difference between security and prevention is in traditional criminological terms. Security consists of those measures people or businesses take in order to protect something, such as installing locks and car alarms. Prevention consists of those activities we engage in to stop an action before it begins. There are numerous prevention strategies in traditional criminology from which one can choose such as situational crime prevention, educational or awareness campaigns as well as legislation, which provides some sort of deterrent or prevention effect. The most effective strategies for crime prevention seem to have elements of both security and prevention. In his book, *Fighting Computer Crime* (1998), Donn Parker discusses security strategies at length; what is notable, however, is that within each strategy (whether for the individual or the multinational corporation) there is a strong element of prevention.

As stated previously the most important prevention strategies cannot yet be determined, as no basis exists within the field to which we can compare the various the actions. This is a new and growing area for all parties involved, including those charged with protecting the users and venue. However, a guide must be provided to discuss these issues. To create a comprehensive list of prevention efforts within the US or the EU would serve a limited function and is beyond the scope of this project. Therefore, this report will attempt to provide the most notable prevention strategies that have been implemented on both sides of the Atlantic and will be broken down into five sections: legislation, self-regulation, and informative measures, technological and other. In each category, several examples will be provided of those strategies which seem to be the most well known, or have otherwise gained some level of attention at the state, federal, national or international level.

Many of the examples for the US were originally found in a report entitled *Computer Crime: A Joint Report,* which was created by the State of New Jersey Commission of Investigation and the Attorney General of New Jersey (Celentano, Thompson, Edwards, Kernan, & Farmer, 2000). Locating and reading the appropriate organizations' websites provided additional information on the efforts suggested by the New Jersey report. The information for the EU was gathered utilizing the questionnaire and the help of a Europol representative as well as finding the appropriate EU websites. The following attempts to provide a brief overview of the information found on the websites, in the supporting texts and what was gathered from the questionnaire.

2.
LEGISLATION

2.1 LEGISLATION – UNITED STATES OF AMERICA

Legislation against criminal activity can serve many functions in a society. The main functions of this type of legislation are deterrence, payment to society or retribution and finally punishment. Ideally, this type of legislation would accomplish each of these aspects. In the field of computer related crime, viable legislation has been hard to create and has been even more difficult to maintain in the context of rapidly changing technology.

Every state in America has its own form of computer related crime laws under which a person can be prosecuted. In addition to their individual statutes, states must also comply with several federal laws such as the Computer Fraud and Abuse Act of 1986 and the Economic Espionage Act. Thus, a criminal act could be prosecuted through either the federal or the state statutes depending on the circumstances of the crime. According to Rasch (1996), the Computer Fraud and Abuse Act of 1986 is one of the most "comprehensive federal computer crime statutes." This particular law, including its amendments in 1994, 1996 and 2001, covers the following activities:

- Unauthorized access (which also includes exceeding the limits of one's authorization) of a computer to obtain information of national secrecy which could be used to injure the United States or for the advantage of a foreign nation;
- Unauthorized access of a computer to obtain protected financial or credit information as well as information from any department or agency in the US or information in a protected computer;
- Unauthorized access of any non-public computer used by the federal government;
- Unauthorized interstate or foreign access of a computer system with intent to defraud, unless the object of the fraud and the thing obtained consists only of the use of computer and the value is not more than $5000 in any 1-year period;
- Knowingly and without authorization causing the transmission of a program, information, code, or command to a protected computer, including reckless behavior that causes damage;
- Fraudulent trafficking in computer passwords affecting interstate commerce;
- Threatening to cause damage to a protected computer for the purposes of extortion;

This particular act makes every violation a felony except for those acts that are committed in a negligent manner. The significance of felony violations is that the punishments are much more severe and the perpetrator, among other things, is stripped of his or her right to vote. For the most part a large percentage of computer crimes are prosecuted under this statute as it can be applied to virtually any violation that takes place on a "protected computer," which is defined as any computer used by the federal government or used in interstate or foreign

commerce. Considering the nature of the Internet this can include nearly any computer connected to the World Wide Web.

The US Economic Espionage Act of 1996 defines a trade secret as all tangible or intangible forms of financial, business, scientific, technical, economic, or engineering information regardless of how it is stored. It is important to note, however, that the owner is required to take reasonable measures to keep it secret. Furthermore, the fact that this information is kept secret must have actual or potential independent economic value. When a person is prosecuted under this act, the penalties can include up to $500,000 and/or up to ten (10) or fifteen (15) years in prison, depending on whether or not a foreign interest is involved. Parker (1998), aptly points out, however, that a $500,000 penalty could be insignificant if, for example, the computer code that was stolen is worth billions of dollars. Therefore, the preventative or deterrent criteria for this particular law may not have been adequately met.

Child pornography has rightfully received substantial federal attention and many federal laws deal specifically with this issue and its relationship with the Internet. The legislative highlights would include the Child Protection act of 1984, which outlaws the use of computers to transmit, manufacture, or create child pornography. In addition, the Child Protection and Sexual Predator Punishment Act of 1998, which, among other things, requires Internet Service Providers (ISP's) to report incidents of suspected child pornography or be subject to possible fines of up to $10,000.

Several other laws in this area have also received attention, the first being the Child Pornography Protection Act of 1996, which was intended to fight the use of technology to create child pornography. Unfortunately, some states have declared it unconstitutionally vague (i.e. Maine) while others feel it is acceptable legislation (i.e. California). The other law worthy of mentioning because of the recent legal issues it has raised is the Child Online Privacy Protection Act (COPPA) of 1998. This particular law requires commercial websites to gather some type of information (credit card or access codes) to verify the age of the Internet consumer. This law has yet to be enacted because of various injunctions by the states and the American Civil Liberties Union (ACLU) who claim that this also inhibits adults from buying and seeing what they want on the Internet.

The Identity Theft and Assumption Deterrence Act of 1998 allows victims of identity theft to seek restitution for crimes that have been committed against them. Further, it required the Federal Trade Commission (FTC) to create the Identity Theft Complaint Center, which provides law enforcement referrals, general information, and advisories to credit agencies.

To outline each state law would serve no useful purpose other than to create a laundry list of the similarities and the differences between states. However, some states, namely California, have created what could be potentially useful legislation in an attempt to address the issue of jurisdiction posed by the Internet. California recently passed several laws that require "foreign" companies doing business in California to provide records regarding computing and electronic communication services. This applies even if the actual office and/or the information the officials want is out of state. The law states that the "foreign" corporation will produce the desired records within five days of the request and California businesses will treat "foreign" requests as if they originated in California (Cal Penal §1524.2(b) (c)).

In an effort to combat piracy and to continue to protect intellectual property rights, the United States enacted the Digital Millennium Copyright Act (DMCA) in 1998 (US Copyright Office, 1998). This act also reflects the implementation of two World Intellectual Property Organization (WIPO) treaties. This act, however, has been riddled with issues and criticism, particularly in the manner in which large corporations have used it to try to stop various activities. One of the crucial parts of this particular act is Section 1201, which states that it is illegal to make or sell a device designed to avoid technological measures meant to keep a person from illegally accessing or reproducing a copyrighted work.

"Fair use" procedures are those rights that institutions and groups of people have to legally purchased or accessed information. For example, if a person purchases an audiocassette, they have the right to make copies or resell it as they see they fit. The creators of DMCA contend that it is not intended to limit fair use, which has been a cornerstone for US copyright law, but rather to keep those who engage in piracy from creating "black boxes" which allows a person unlimited and free access to something that should be paid for, such as cable TV. Many exceptions were placed into this act in order to ensure that certain groups or activities would be able to continue to use copyright-protected material in the same fashion. These exceptions were, (i) nonprofit library, archive or educational institutions, (ii) reverse engineering purposes, (iii) encryption research, (iv) protection of minors, (v) personal privacy, and (vi) security testing.

Other problems with this act have included limiting free expression, scientific research as well as competition and innovation. Although these issues are beyond the scope of this particular report it highlights the important point that as more people use computers on a daily basis to access their information the same rights we have in the physical world should apply to the virtual world. The US constitution is based on the premise of free speech and those rights should exist on the Internet as well. For example, if someone creates and wants to publish something on how to avoid a specific copyright protection, the person should feel free to do so and not fear the legal ramifications. This stimulates innovations on behalf of all parties involved and supports free speech in a market economy. The Electronic Frontier Foundation has produced an excellent report on these various issues entitled *Unintended Consequences: Three Years Under DMCA* (2002), which provides further information and examples of these issues as they relate to this particular piece of legislation.

Other parts of DMCA are focused on bringing the existing copyright codes up to date with changes and additions primarily for ISP's. It attempts to limit the responsibility the ISP's have for copyright protected material in the performance of certain duties or engaging in certain actions. Liability limitations have been implemented for those who are qualified. For example, an ISP is not necessarily responsible if a user places material on a website in violation of copyright protection. However, ISP's are also responsible for carrying out certain actions (i.e. removing material if it is violating copyright laws) within a given time period.

2.2 LEGISLATION – EUROPEAN UNION

Preventing the exploitation of children on the Internet is one of the fields in which both the European Union and the Council of Europe have been active. The criminalization of this type of behavior relate to both human rights issues and the necessity to combat organized crime. Evidence from various investigations suggest that the "child pornography business" is often run by internationally organized criminals.

The European Commission adopted its first legislative measure against child pornography on the Internet in 1997. The *Communication on Illegal and Harmful Content on the Internet* stressed the need for a common definition of what should be considered harmful content. The obstacles to a common legal framework within the EU are related to each country's rules governing individual rights. Member States within the EU agree on the need for specific legislation on child pornography, but the approach to obscenity regulation, for example, varies according to different ethical standards. Therefore, the criminalization of child pornography differs between each country. Most EU Member States, except Greece and Portugal already have child pornography provisions. Only a few Member States have laws specifically directed at the use of computers and child pornography. Moreover, the possession of child pornography is forbidden in most EU countries, except in those already mentioned and Spain.

The main target of the European Union's plan is the creation of a common legal framework on issues related to the exploitation of children. The effort to create this common strategy for EU Member States is also mentioned in Council decision 2000/375/JHA to combat child pornography on the Internet. In article 1 the Council of the European Union obliges Member States to 'intensify measures to prevent and combat the production, processing, possession and distribution of child pornography material." The Council decision places fundamental importance on co-operation between the many law enforcement authorities, which is considered an effective way to investigate and prosecute child pornography rings. In addition, it promotes the development of channels for communication between each member's various law enforcement agencies.

The EU action plan against child pornography also takes into consideration that the spread of this type of material on the Internet could be reduced by the creation of a safe environment in cyberspace. Therefore, they promote filtering tools and rating systems as well as hot lines for reporting illegal content displayed on web sites. All these topics are reflected in the Decision 276/1999/ *Adopting a Community Action Plan To Promote Safer Use of the Internet by Combating Illegal and Harmful Content on Global Networks* as well as in the new *e*-Europe plan (COM 2002 -152).

The Council of Europe's Convention on Cyber-crime (2001) must also be considered when assessing European action against child exploitation. Article 9 of the Convention imposes a duty on Member States to criminalize, under their national law, all the conducts listed, which include: the production of child pornography for the purpose of distribution, offering or making available child pornography, distributing or transmitting, as well as procuring and possessing child pornography in a computer system or on a computer-data storage medium. The article also defines what is considered as child pornography and outlines that as being "all the material that visually depicts a minor engaged in sexually explicit

conduct or a person appearing to be a minor engaged in sexually explicit conduct or realistic images representing a minor engaged in sexually explicit conduct."

Although the Convention on Cyber-crime represents a milestone with regards to international legislative measures, the definitions adopted by article 9 could cause several problems in the prosecution of illegal behavior. There are two main points of controversy. The first is related to the criminalization of the simple possession of child pornography, while the second is related to the definition of child pornography as also being digital images. In the latter it is difficult to determine which is the law's protected interest as far as digital images are concerned because they are not related to any form of children exploitation per se.

It is important to note that the conventions created by the Council of Europe cannot be directly applied in the same way as a directive or a regulation, which is produced by the European Community. The Council of Europe is a much larger entity including, upwards, of 40 members as well some countries with special observer status. The European Union, on the other hand, consists of only the 15 Member States, and has the power to enforce sanctions upon Member States who do not comply with its regulations, directives and decisions. Thus, the state signing a convention produced by the Council of Europe has to ratify it and to provide the legislative measures to implement it but are not forced to do so by any supranational body.

Several Member States have been very active in the area of child pornography and already have specific law provisions. In order to understand what is being done at national level some member states are analyzed in more detail. Belgium, for example, has a specific provision which prohibits the making, publishing, distributing and disseminating of advertisements for sexual services in order to make a profit, particularly when these are provided by use of telecommunications including computers and the Internet (Article 380quinquies, § 2 Code Penal). Furthermore, Belgium has established a web site where complaints about child pornography can be reported. The site is entitled the *Belgian Citizen's Digital Reporting Site, which* is aimed at stopping the sexual exploitation of children through the Internet.

French legislation on child pornography, with respect to the use of telecommunication networks, resembles the previously mentioned Belgian regulation. In France, it is prohibited to facilitate or attempt to facilitate the abuse of a minor when . . . he or she has been put in contact with the perpetrator by using a telecommunication network or by the transmission of messages to the public. This could also include contact via the Internet. This legislation is particularly interesting as it highlights the perpetrator's ability to use chat rooms to lure victims and attempts to address the issue accordingly.

Italy also makes direct reference to the use of communication networks in the "Italian act on child pornography." Article 3 of that act clearly penalizes the dissemination, broadcasting or publishing of pornographic material and the dissemination and broadcasting of information aimed at the soliciting or sexual exploitation of minors.

The Irish "Child trafficking and pornography act 1998" specifically mentions the possibility of storing or producing child pornography via a computer disk. It also highlights the possibility of generating or modifying a figure resembling a person using computer graphics. The Irish act is, therefore, the only act of a European

Union member state, which clearly penalizes the use of computers in child pornography related crimes; this coincides with the legislation found within the United Kingdom (UK).

Similar to the Irish act on child pornography the "Protection of Children Act 1978" in the United Kingdom also refers to the possibility of the use of computers or the Internet in child pornography. It states that 'photograph' includes data stored on a computer disc or by other electronic means, which are capable of being conversed into a photograph. This act also refers to the concept of a "pseudo-photograph," which includes images made by computer graphics or otherwise appears to be a photograph.

As with child pornography, hate speech has also received attention from both the European Union and the Council of Europe. The legal problems regarding the creation of a common framework against racism and xenophobia on the Internet are related, once again, to single states agreeing on what constitutes freedom of expression. Therefore, EU action is restricted by its respect for each Member States' fundamental rights and the definition of the offences already established by their national criminal codes. The main EU legislative measures in this field are the 1997 *Communication on Illegal and Harmful Content on the Internet*, decision 276 *Adopting a Community Action Plan on Promoting Safer Use of the Internet* (1999) and the Communication COM(2000) 890 on *Combating Computer Related Crime.*

The Council of Europe is currently working on a draft of the first additional protocol for the Convention on cyber-crime regarding the criminalization of racist and xenophobic acts perpetrated on the Internet. These acts are defined as "any written material, any image or any other representation of ideas or theories, which advocates, promotes, or incites hatred, discrimination or violence, against any individual or group of individuals, based on race, color, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors." This definition derives primarily from the *Convention for the Protection of Human Rights and Fundamental Freedoms* as well as *Protocol No. 12* concerning the prohibition of discrimination. The illegal conducts described in the draft covers a large catalogue of behaviors such as the dissemination and distribution of illegal material as well as threatening and insulting behavior through a computer system.

While many countries have passed legislation on computer related crime over the years, attacks against computer systems are a more recent issue on the European Union's agenda. This appears to be a consequence of the Tampere Summit of the European Council in October 1999. The Council communication, (COM(2000) 890), *Combating Computer Related Crime*, outlines the aim of EU action as "the harmonization of substantial law provisions in order to ensure a minimum level of protection against computer crime and facilitate the prosecution of those crimes within the Member States."

In the Communication (COM (2000) 890), computer related crime is defined in the broadest sense as any crime that in some way or another involves the use of information technology. The EU action has been focused on content related offences (child pornography, racism and xenophobia), as well as economic crimes related to unauthorized access such as sabotage, intellectual property offences and privacy offences. In addition, the Communication states "the need to fight against computer related crime will be balanced with the individual right of privacy and anonymity on cyberspace." Therefore, the powers granted to law enforcement

agencies to trace and prosecute cyber-criminals should be restricted according to the policies established by the directives 95/46/EC and 97/66/EC and the recommendations of the Article 29 Data Protection Working Party.

Communication (COM/2001/0298) entitled *Network and Information Security: Proposal for a European Policy Approach* addresses the need to ensure computer system safety with criminal law provisions. In this communication, the commission proposed the analytic description of different threats against computer systems:

- Unauthorized access to information systems (hacking)
- Disruption of information systems (including denial of services attacks)
- Execution of malicious software that modifies or destroys data.
- Interception of communications.
- Malicious misrepresentation.

Under each category, the Communication analyses potential damages and solutions as well as mentions previously implemented legislation or defines a multilateral approach, which involves both legislative and non-legislative measures.

The latest action taken by the EU is represented by the proposal of the *Council Framework Decision on Attacks against Information Systems* (COM (2002) 173). The proposal highlights the need for harmonization between Member State criminal law provisions on computer crime, in order to safeguard national security interests and avoid criminal behaviors that may undermine the regularity of market exchanges. The proposal outlines a set of definitions that should help Member States to establish new criminal sanctions. The crimes are defined in a generic manner, which allows each Member State to follow EU guidelines according to its own legal system.

The Member States of the European Union also have a variety of provisions against computer related fraud. Some of the Member States have special provisions when fraud is committed using a computer or when alterations have been made to a computer or a file in order to create the possibility of committing fraudulent acts. Other Member States, however, have no specific provisions for the prevention of computer related fraud. Belgium, for example, does not have specific provisions and has had some difficulties prosecuting this type of crime. Prosecution for fraud or embezzlement under Belgian law, generally speaking, is much easier when documents are printed. Currently, there is an ongoing discussion in Belgium as to whether data should be considered as material property. These difficulties do not arise, to the same extent, in the other Member States that do not have specific provisions. Most courts have ruled that computer related fraud is the same as "normal" fraud. Denmark, for example, has had at least 102 convictions over the last 14 years for computer related offences. In France, court decisions tend to be more severe when fraud is committed via a computer. Therefore convicting and punishing offenders has not presented any substantial difficulties when there is a computer related fraud. Some of the above-mentioned problems are probably why many other European Union Member States have specific provisions for computer related crimes. For instance, Denmark and Finland have made computer related fraud a crime using a single article in their criminal code and the United Kingdom has the Computer Misuse Act.

Very few EU Member States have specific provisions regarding computer related forgery. In Italy and Luxembourg, laws specifically directed at computer related forgery exist, but most other countries punish this type of activity as part of their

general penalization of forgery. However, some countries have aggravated offences or special penalties for computer related forgery. These aggravated offences apply to the employees of a telecom-operator in Belgium, for example, or if technological equipment is used as in Finland.

Most European Union Member States also have special provisions for damaging computer data or computer programs. In some cases, however, a distinction is made between deliberately causing damage and causing damage without intent. This distinction is only expressed through the maximum penalty imposed. The Italian Penal Code, for example, is directed at the spreading of computer-viruses, trojans, or other malicious code. This definition of "a computer program that has the intention or effect of damaging a computer" is not found in most other European member states. Terms such as "fraudulent access resulting the deletion or alteration," as in Luxembourg, and "intentionally and unlawfully destroying, damaging or rendering unusable," found in The Netherlands, are more common, because they do not require a computer program to be used. In other Member States the damaging of computer data or computer programs is part of the legislation concerning the damaging of goods.

Unlike those provisions focused on the damaging of computer systems some countries also include those actions, which are carried out with the intent of keeping a computer system from functioning properly. This kind of criminal legislation mainly seeks to protect public installations like telecommunications networks. This can also be seen in the way in which the articles are written. Terms like "major disturbances," found in Denmark and "vital importance," as in Germany are used. This type of legislation does not seek to prevent hackers from breaking into and altering web sites, but to protrect public safety.

All Member States surveyed have legislation seeking to prevent unauthorized access into data systems, thereby making all acts of hacking punishable by law. It does not matter whether the hacking is perpetrated by taking another's identity or through bypassing security measures. The means used to gain unauthorized access to data can be a reason to impose a higher penalty.

At the larger European level, in the field of computer security attacks, the Council of Europe's Convention on Cyber-crime (2001) defines the following actions as criminal:

- **computer related fraud**: the input, alteration, erasure, or suppression of computer data or computer programs, or other interference with the course of data processing, that influences the result of data processing thereby causing economic or physical loss of property to another person with the intent of procuring an unlawful economic gain for himself or for another person
- **computer related forgery**: the input, alteration, erasure or suppression of computer data or computer programs, or other interference with the course of data processing, in a manner or under such conditions that would, according to national law, constitute an offence of forgery if it had been committed with respect to a traditional object of such an offence
- **damage to computer data or computer programs**: the erasure, damaging, deterioration, or suppression of computer data or computer programs without right

- **computer sabotage**: the input, alteration, erasure, or suppression of computer data or computer programs, or interference with computer systems, with the intent to hinder the functioning of a computer or a telecommunications system
- **unauthorized access**: the access, without right, to a computer system or network by infringing security measures

The approach chosen by the Council of Europe is a follow-up of its previous initiatives on computer crime Recommendations No R (89) 9 on computer-related crime and No R (95) 13 concerning problems of criminal procedural law connected with information technology. Therefore, the aim of the Convention is to increase the level of international co-operation as well as outline definitions of computer crime, which are detailed enough to distinguish between legal and illegal behavior. Furthermore, they must be general enough that they can be adapted into the different legal systems.

The Council of Ministers of the European Union has adopted several directives in the field of intellectual property rights. Directive 91/250 focuses on the legal protection of computer programs, directive 92/100 on rental and lending rights and certain rights relating to copyrights and directive 93/98 concerns itself with the protection of copyrights and certain other rights related to this field.

The latest initiative is directive 2001/29/EC, entitled the *Harmonization of Certain Aspects of Copyright and Related Rights in the Information Society.* This has been adopted in an effort to create a common legal framework for the intellectual property theme. Although the directive does not oblige Member States to create criminal provisions, article 8 asserts that [Each state] shall provide appropriate sanctions and remedies in respect of infringements of the rights and obligations set out in this Directive and shall take all the measures necessary to ensure that those sanctions and remedies are applied. The sanctions thus provided for shall be effective, proportionate, and dissuasive.

This final statement supports the structure of most criminal provisions. In general, this particular category of computer related crime is often not punishable using the penal code of the Member State, but instead must be enforced with special legislation such as copyright acts and intellectual property law.

3.

SELF-REGULATION AND COMPLIANCE

Self-regulation and compliance are a useful way to limit government monitoring and still provide industries a method to comply with laws as well as impose additional limitations if the institutions deem them necessary. This can be quite an extensive category. The focus of this section will be on those codes of conduct or other regulations that have been implemented within and/or for the industries or people who have a vested interest as opposed to specific codes of conduct that may not apply to a wider information technology audience.

Although the Individual Reference Service Group has been recently dissolved due to the implementation Gramm-Leach-Bliley Act, which now covers many of the privacy issues they originally raised, they provide a good example of a group of companies who created guidelines for themselves. The Individual Reference Service Group consisting of fourteen companies who have agreed (even now although they are no longer a formal organization) to comply with a set of self-regulatory industry guidelines, includes Acxiom corporations, CDB Infotek, Lexis Nexis, National Fraud Center, Experian and First Data Solutions. This set of guidelines goes beyond many of the implemented legal precautions. They agree to use only reputable sources, to take the necessary steps to insure the information they have is accurate, to distribute only that information which is publicly available, and to distribute non-public information only to other companies who comply with the principles they have outlined.

Those who receive information from this group must state an appropriate use of the information they receive, and they must limit their use and re-dissemination to such use. In addition, those who receive the information must be considered "qualified subscribers" before requesting the information, for which there are specified criteria that must be met. Non-public information, which the group will not disclose, includes such things as Social Security Numbers, one's mother's maiden name, unlisted telephone numbers or other non-published information. Further exclusions include credit and financial history as well as medical information. Additional regulations include responsibility for security, openness, and the ability to choose to disclose the information or not. Finally, they will not disclose any information about children less than 18 years of age. Several other regulations to which this group of companies adheres also exist.

The Better Business Bureau (BBB) online has developed a self-regulatory online privacy program. A BBB press release (2000, October 4), provides a general overview of their codes of conduct as well as what they attempt to provide to both businesses and consumers. If an online business meets certain basic requirements, they receive a BBB stamp of approval, which denotes that this particular company adheres to particular standards set by the BBB. *The BBB Online Code of Business Practices* outlines five basic principles designed to foster consumer trust in online businesses. Logically, if consumers do business on the Internet the same way they do business in the virtual world, their risk for fraud will be reduced (i.e. doing business with companies and people you know and trust). The *BBB Code of Online Business Practices* principles include truthful and accurate advertising, disclosure, information practices and security, customer satisfaction and child protection.

Truthful and accurate advertising refers to the idea that all information provided to the pubic should be correct. Disclosure refers to the actions taken by the company to inform current and future customers of what is available to purchase online and how that sale will be conducted. Information and security practices include a posted privacy policy that is respected as well as ways to protect the information collected from the customers. This category also includes the idea that companies should respect their customer's requests regarding unsolicited email. The principle of customer satisfaction is self-explanatory in that businesses should make sure their customer is happy. The protection of children principle requires the businesses to pay special attention to the developing cognitive abilities of children under the age of 13, particularly, if this population is targeted for advertising. They should adhere to the Children's Advertising Review Unit (CARU) guidelines (2001) for this type of activity.

Another organization that has a professional code of conduct related to computer crime is the Association for Computer Machinery (ACM). This organization has been in existence since 1947 and has at least 37 special interest groups who focus on specified topics with over 75,000 members, according to their website. Their code of ethics is divided into in five sections. The first section discusses basic ethical considerations such as avoid harm to others, be honest and trustworthy, do not discriminate, respect the intellectual property of others, and give proper credit to the authors of intellectual property. Further, it asks its members to respect the privacy and confidentiality of other people.

The second section offers specific additional professional imperatives for its members. Those who participate are asked to make their work the best they can by "striving for the highest quality, effectiveness, and dignity in both their process and products of work." In addition, they are to stay abreast of changes within the field and know and respect the existing law. They should also "provide evaluations of computer systems and their impacts, including analysis of possible risks." Two more demands are placed on the members, which relate more specifically to the prevention of computer crime. The first is to increase the publics' awareness of computing issues and the second is to only access another person's system after being asked. It is clear that one of the few ways to prevent computer crime is to educate the public about the risks that are posed online. This point is enshrined in their code of conduct reflecting a belief postulated by virtually everyone in the field. Furthermore, they are against hacking into systems to "highlight" security breaches unless expressly requested to do so.

The third section of the ACM code of conduct concerns itself with outlining the responsibilities of industry leaders who may be such by virtue of their position or education. This may also apply to various types of organizations as a whole (employers, volunteer organizations etc.) as well as individuals. The leader is charged with the responsibility to "articulate social responsibility . . . and encourage full acceptance of those responsibilities" (ACM, 1992). An organization should also acknowledge and support proper use of computing technology and create opportunities to learn about its benefits and limitations. This is not the complete list of ACM guidelines; however, this highlights those that could be particularly useful to computer crime prevention. As a sanction, if an ACM member does not comply with the stated code of conduct their membership can be revoked.

Nearly every professional organization that exists has some type of code or charter that outlines the behavior expected from its members. One area known for its self-

regulation is the banking industry. The best example of this is the "know your customer" policies wherein banks are required to know who their customers are and monitor their money flow. If they suspect suspicious activity, they report it to another body who then makes a decision regarding the information that has been provided. This has allowed the banks to cooperate with law enforcement and not be required to act as a police force with their customers.

The primary regulating body for American banks is the Federal Deposit Insurance Corporation (FDIC). This regulatory body produces a three volume series of the rules and regulations the banking industry is required to follow (Federal Deposit Insurance Corporation, 2002). Certain issues exist within the banking industry worthy of mentioning, particularly privacy issues and customer security. Both have been and will continue to be addressed as they relate to online banking and the other uses of technology within this industry. For example, banks use encryption technology to protect customer's information. In addition, they send information in pieces to make it more difficult for a criminal to put the information together about one particular customer (i.e. for an identity theft).

Within the fifteen Member States of the European Union there are also a number of self-regulatory initiatives, unfortunately few of them are obligatory. While many European countries have organized websites or opened telephone numbers where computer related crimes can be reported, there is no such thing as a European Code of Conduct or other regulation aimed at the parties that could be subject to computer related crimes. Interpol is currently working on cases concerning terrorism and child pornography. Other initiatives are taken at the Member State level. Although these differ slightly from state to state, and are created for the specific state situation, the differences are not that significant.

Most EU Member States have an Internet Service Providers Association (ISPA), which among other things formulates codes of conduct for the participating providers. However, participation in an ISPA is not obligatory. Therefore, codes of conduct drawn up by ISPA's can only be enforced with those participants who are willing to cooperate. Apart from the ISPA's in the EU Member States, there is also a pan-European association of the Internet Service Providers (EuroISPA). The nine members of this association are also EU Member States. At this moment, the ISPA's are focused primarily on privacy issues and not prevention of computer related crimes in general.

Many initiatives taken to prevent computer related crimes in the European Union consists of co-operation between governmental organizations and privately run organizations. One such organization is Eicar, which consists of experts in the field of computers. In this organization, legal and technological experts work together. Some work for public or governmental organizations, others work for Internet providers while others are lawyers or otherwise work in the private sector. The goal of Eicar is the prevention of computer related crimes in general. Many taskforces have also been created to reach this goal. One of the most important is the task force on 'European Cyber-crime Initiative – Misuse of Devices'. This taskforce was set up to handle the Convention on Cyber-crime, which was signed by the Member States of the Council of Europe and four other countries. This taskforce focuses on the issue of whether provisions of the Council of Europe Convention provide adequate and appropriate means for protection against computer viruses.

4.

INFORMATIVE AND INSTRUCTIVE MEASURES

Informative and instructive measures are likely to be the most important weapon in the battle against computer related crime. Educating the users of technology about its power as well as its dangers will more than likely create a safer computing environment for everyone. Education is an important aspect in a general crime prevention approach. Following this lead, a large number of educational strategies have been implemented in a variety of ways. The most important has yet to be determined, and such a determination would require extensive in-depth analyses on a wide range of issues, including a cost-benefit analysis for the various programs and/or an evaluation study on the efficacy for reducing specific types of computer crime. The current state of computer related crime does not lend itself to such critical analysis as the area is simply too new and sufficient concrete evidence has yet to be gathered.

4.1 US INFORMATIVE AND INSTRUCTIVE MEASURES

A non-profit program called *CyberSmart!* is currently being tested in the New Jersey area. This particular program instructs teachers on the how to give tips to their students in order to avoid online sexual predators. One person who is quite active in the field of informative and instructive measures is Parry Aftab, who currently serves as Chief Executive Officer of a non-profit called Cyberangels and is the author of the book *The Parents Guide to Protecting Your Children in Cyberspace* (2000). This organization, in conjunction with the Baltimore County School System, located in Maryland, has created the largest parent Internet education program.

A national education campaign started in 1999 called "kNOw Fraud™" was designed to inform the public about telemarketing fraud. This campaign provided 16,000 informational videos to public libraries. Over 120 million envelopes containing fraud prevention tips and numbers were sent to American households. Although this campaign was focused on telemarketing fraud, the information provided could also help with many of the risks for fraud found online.

One way to prevent identity theft is to make sure consumers are conscious of privacy issues when they utilize the Internet. The Electronic Privacy Information Center (EPIC) hopes to assist in combating this particular crime through a report they produced entitled *Surfer Beware III: Privacy Policies without Privacy Protection* (1999). This report assesses the privacy practices of the 100 most popular shopping sites. Unfortunately, their findings do not bode well for the person who is concerned with privacy:

Many of the companies profiling is more extensive and the marketing techniques are more intrusive. Anonymity, which remains crucial to privacy on the Internet, is being squeezed out by the rise of electronic commerce.

Further, the report contends that self-regulation has done very little; nothing short of legislation will make companies address the issue of "fair information practices."

Many books and guides to Internet and computer safety can be found online. In addition, various government agencies publish such manuals, particularly to help parents protect their children. The US Department of Education offers an online publication *Parents Guide to the Internet* (1997). This particular publication is aimed at helping parents find educational sites online and provides vital crime prevention activities as well. Several examples of this type of literature exist (US Department of Justice [US DOJ], n.d.) if a parent is using this type of book then the parent is likely to be taking an interest in what the child is reading while on the Internet. Parental interaction is a crucial component in protecting children and teaching them right from wrong. Thus, these types of books provide parents a way to educate themselves, their family and to take an active part in the online lives of their children.

The Internet Safety Watch Inc. provides Internet safety awareness and privacy protection information. This non-profit organization has noted several facts about Internet safety information, and is attempting to change them. Most importantly, they noted that the vast majority of online security information is found *online*. Unfortunately, people do not typically research security information unless they feel they are at risk by either being previously victimized or knowing someone who has. The people that should be educated are those who are just starting out. This type of campaign should make some type of impact on the computer crime rate as they point out that according to CERT® (Computer Emergency Response Team) "as many as 99% of all security breaches could have been avoided with proper updates, configuration, and security policies" (Internet Safety Watch Inc, 2001). If this holds true for security breaches it is likely to be true for other types of crimes as well.

The Internet Safety Watch is attempting to build an online educational database that informs the user about the various security issues and offers possible solutions. This, however, is only one of their platforms as they are also attempting to create programs for schools as well as collect and donate safety, security, and privacy tools to low income families. Their website is quite comprehensive and offers several possibilities for anyone concerned with online safety to become involved by donating their time as a mentor or in some other capacity.

The Simon Wiesenthal Center located in Southern California disseminates a CD-ROM entitled "Digital Hate 2000" which lists hundreds of extremist websites. This is a creative way to inform the public about websites that support hate speech, bigotry and other forms of discrimination based on the characteristics of a person or group.

Internet and computer awareness, however, is not limited to the traditional crimes currently perpetrated with the help of technology. There are also campaigns that seek to inform users about basic computer security issues. Much of this type of activity includes information about viruses, malicious codes, and security holes that need to be patched. Among the websites that offer this type of information are the Computer Incident Advisory Center (CIAC), National Infrastructure Protection Center (NIPC), Computer Emergency Response Center (CERT®), National Security Institute (NSI) and the SANS institute.

All of these organizations can be found on the Internet and offer vast amounts of information regarding computer security. In general, these sites are geared more

toward the person who already has a basic knowledge of the potential computing issues and is searching for more advanced information. In an effort to educate computer users in general, some of these sites also link to basic information and provide articles on issues like *How to Choose a Password* (n.d.) and *Almost Everything You Ever Wanted to Know about Computer Security* (1993).

4.2 EU Informative and Instructive Measures

The European Union has clearly understood that legislative measures are necessary but not, in and of themselves, sufficient to effectively combat computer related crime. Thus, the creation of a safe and productive environment in cyberspace, through user education, is seen as a priority. This has been accomplished by supporting several initiatives, addressed to both citizens as well as businesses.

Information on the various topics that relate to the Internet is provided by the Quicklinks website, which contains links to news items about legal and regulatory aspects of the Internet, particularly those relating to privacy, computer crime, and the technical and legal aspects of cyberspace. The website is frequently updated and contains an events page as well as news items, which are organized both chronologically and by category. The website also offers a free newsletter service that is distributed by electronic mail through an "announcement only" mailing list. Quicklinks is part of the Information Society website, which has been created to guide the users through different aspects of the Internet as well as the various related activities of the EU.

The Safer Internet Action Plan, which promotes safety on the Internet, is a European Union program designed to deal with the controversial issue of illegal, harmful, and racist content on the Internet. The actions are divided into three different categories: the creation of a net of European hot lines, the development of a responsible surfing culture and the promotion of the use of parental control mechanisms.

The Commission has financed the creation of several hot lines to raise the awareness of both Internet users as well as Internet service providers regarding child pornography. ChildFocus, Net Alert, Barnaheill – Save the Children, Iceland and InHope are only a few of the several hot lines run by non-profit organizations and Internet provider organizations that have been co-founded by the European Commission. The aim of these associations is to inform both citizens and legislators of the threat of child pornography, to exchange expertise as well as raise the awareness and educate people regarding the various aspects of child sexual exploitation and the possible consequences. This is achieved by the dissemination of reports on the cyberspace situation.

Awareness activities are another aspect of the EU action to build trust and confidence in parents and teachers about the safe use of the Internet by children. *Educanet* is one of the EU financed websites with the objective of providing an educational strategy that will help children to develop a responsible and autonomous attitude when they are using the Internet.

The problems related to intellectual property and liability in cyberspace are described on the Intellectual Property Rights (IPR) Helpdesk website. This particular resource is a project of the European Commission Directorate General (DG) Enterprise and is co-financed by the European Union. The site provides general information on intellectual property rights protection and exploitation through the release of documents and reports on the issue. In addition, a complete and detailed list of FAQs on intellectual property infringements (i.e. limits and contents of intellectual property rights, types of infringements) is provided. Further, the Helpdesk offers a number of self-paced tutorials on intellectual property and related subjects that can be downloaded directly from the website.

In the field of computer security and commercial fraud, the Joint Research Centre, a directorate general of the European Commission, should be mentioned. The main aim of this directorate is to ensure that all European Union institutes receive the logistical and technical support needed to carry out their missions. Currently there are seven JRCs. One in particular, the Institute for the Protection and the Security of the Citizen (IPSC), has been working on issues of anti-fraud, compliance monitoring, and cyber security.

The IPSC provides support for the conception and implementation of EU policy in the areas of cyber security and, at the same time, works on the concerns of citizens and consumers regarding cyberspace and related themes. The interests of the institute cover online privacy as well as identity protection of citizens, the prevention of computer crime and the improvement of consumer confidence in e-commerce. The technical area of the research focuses on creating preventative and security measures as well as analyzing information infrastructure vulnerabilities that could create risks for the general population. The results of IPSC research are available on the JRC website.

In the e-commerce sector, the “Dr. E-commerce” website has been created by the European Community to inform the citizens on the latest developments in electronic commerce regulation. Teams of experts in technology, legal, and economic issues are always available to answer citizens' questions. The service enables users to communicate, interactively, with the “Dr. E-commerce” staff. The website also provides a large catalogue of updated information about European and non-European initiatives concerning e-commerce.

5.

TECHNOLOGICAL

When one discusses technological measures that relate to computer crime, one is typically discussing security issues. Security obviously plays a preventative role in that it makes committing the crime difficult and may "prevent" the crime from being completed. This is not the primary focus of prevention strategies in the strictest sense of the word. However, considering the topic, no discussion of prevention would be complete without discussing at least the basic technological tools designed to protect ones privacy, information or to protect children from some of the content available via the Internet.

Nothing is foolproof when trying to prevent criminal activity, but certain measures can make it difficult for a crime to be initiated or completed. One of the most important things to remember about technological devices designed to protect a person from criminal activity is that prevention and computer security are part of a dynamic process and nothing is a "plug and forget it" tool. This holds true for everyday security as well. One does not buy a burglar alarm and then not activate it on a daily basis. More simply, you can have locks on your doors but they are ineffective if you are not cognizant of using them.

One type of technological device that is receiving increased attention is filtering or screening software designed to block certain content from the computer (i.e. child pornography and hate speech). There are several types of screening packages with different levels and types of blocking. The screening abilities can be accessed by subscribing to certain online providers who offer parental control features such as AOL. The parent configures settings for each user so it is easy to have unlimited access for the adults and different levels of filtered access for the children. They can also limit what chat rooms particular users are allowed to visit.

Filtering programs such as SurfWatch, CYBERsitter, Net Nanny, and/or Cyber Patrol are also available for personal installation. Either these types of programs block sites they deem as having inappropriate content or they filter sites based on words or phrases they found on the web page the user is attempting to view. A common problem with filtering software is words or phrases are taken out of context. If someone were trying to do a research paper on AIDS, many sites would be inaccessible because a common word that is filtered is "sex." Thus, the main purpose of the Internet – information – has been lost. These filtering programs can assist in keeping children from visiting websites the parents would rather not have the child see. It is important, however, that one does not rely on technology alone, as the common sense taught to children during daily interaction will be much more beneficial in the end.

Cryptography began as a tool for the government to send classified or sensitive information to other people or to decode messages that had been intercepted. In order to protect the vast amounts of personal information placed on the Internet everyday, the government was forced to allow the public access to these tools. The Internet has changed the needs and uses of this technology and it is now in the hands of the private sector and available for use by the public in the form of Pretty Good Privacy (PGP) and Public Key Infrastructure (PKI) (Mickna, 2001).

There have been many political discussions regarding the development, use, and sale of encryption technology. This is an exceptionally strong tool to protect ones privacy, which is becoming increasingly more vital as we become more technologically dependent. Encryption, in essence, completely masks one's communication and can only be read by the person who has the proper key to decode the message. Law enforcement's main concern is not being able to decrypt necessary information sent by criminals, other governments, or some other party in whom they have a legitimate interest. For this reason, exporting strong encryption technology from the US has been prohibited. This changed in 1999 and the Clinton administration allowed the export of this technology to all but seven nations who have been accused of terrorism. Other issues that exist with this technology would include the various federal intelligence and law enforcement agencies lobbying for access to all the keys. In the New Jersey computer crime report (Celentano et al., 2000), the authors highlight the state of our computer security in the following analogy, "[A]s a computer system security device, strong encryption, by itself, is like putting steel security doors on a grass hut" (p.61). Hackers exploit weaknesses in a software program or a computer system of which there are a multitude. Encryption is useful for protecting an entire database of information, as that is what the criminals will work to find. The likelihood of them trying to intercept a single transmission is low, as it is too much work. When asked why he robs banks the infamous bank robber Willie Horton once said, "it was because that is where the money is." Common sense goes a long way in both traditional crime prevention and in our quest to prevent computer crime.

Firewalls have the ability to protect a computer system against almost anything that can destroy it. Further, the firewall can be configured by an individual or the system administrator to allow certain information to flow in or out of the computer system. In essence, this prevents a computer from being attacked by a hacker as firewalls monitor who and what is trying to gain access to a protected network or individual computer. Firewalls provide a basic line of defense between a network or a computer and the Internet. Firewalls, like everything within the technological category, are ever changing and highly user or organizationally specific. Other risks include viruses and malicious codes and the best defense against those are anti-virus programs that are updated on a regular basis. The best prevention can be found when these two things are used together and updated regularly. This may not be true for every user and is certainly not true for large organizations, which are much more complex and require multilevel prevention strategies of which many books have been written (see Parker, 1998; Janal, 1998; Nichols et al, 2000).

The final, and probably most important, aspect for technological measures to prevent criminal activity is choosing secure passwords. In nearly every text that is written about prevention this is the most common topic discussed. A common adage is "security is only as strong as the weakest link." Thus, having strong passwords is the simplest and easiest way to protect one's information and is the most commonly neglected aspect of security on the individual level.

6.
OTHER

Other strategies can run the gamut from books, tip lines, interactive videos, task forces of all kinds or other institutional actions aimed at preventing computer crime. This section therefore attempts to highlight some of the implemented strategies that do not fall into the previously discussed categories.

6.1 TIP LINES

Tip lines can be used for a variety of purposes. In general, people call in and try to provide law enforcement officials with "tips" in order to apprehend a perpetrator. Each state has a tip line or a hot line for various criminal activities. In the US, federal tip lines exist in addition to those that are state or locally sponsored.

Many hotlines specialize in a set of crimes or issues and often have the goal of a being a clearinghouse of sorts for that particular type of behavior. In other words, they will collect tips and give it to appropriate law enforcement agencies thereby removing the users' concern of "who do I report it to." In addition, they often try to analyze the information they receive and try to provide some kind of educational functions to the professionals in the field as well as educate the public to reduce the risk of victimization.

Two US hotlines working on the issue of child exploitation in its various forms (i.e. child pornography, child sexual molestation, child sex tourism, child prostitution, and enticement of children for sexual acts) are the National Center for Missing and Exploited Children (NCMEC) and the US Customs Department. The National Center for Missing and Exploited Children has both a phone line and a cyber tip line that handles these types of complaints. Since 1998, the cyber tip line has received over 68,000 tips and expects to receive increasingly more as the online population continues to grow (National Center, 2002).

The Customs CyberSmuggling Center (3C's) has a hotline for international child pornography investigations. On the 3C information page (US Customs, n.d.), it is clear that this is not the only area on which they are focused. They are attempting to combat the various crimes that are "conducted or facilitated by the Internet" which include international money laundering and offshore cyber-banking, drug trafficking, intellectual property rights violations, illegal arms trafficking, and stolen antiquities/art. The Customs Department focuses primarily on the law enforcement portion and does not have an obvious educational aspect.

The Internet Fraud Complaint Center (IFCC), created as a partnership between the FBI and the National White Collar Crime Center (NW3C) for law enforcement, is meant to be a place where consumers and/or businesses can file a complaint about fraud. Other partners include the US Postal Service and the Internal Revenue Service.

From the data collected it attempts to identify fraud patterns and provide statistical data on these trends.

The IFCC recently won the excellence in ".gov" award, which is presented to government agencies that demonstrate "innovative electronic government initiatives." The selection criteria are the extent of the project's impact, its ability to save resources and increase productivity, the project's ability to simplify and/or unify processes and its repeatability for other government agencies. Dennis M. Lormel, a Section Chief, Financial Crimes Section, Criminal Investigative Division of the FBI was quoted as saying, "we anticipate the number of complaints to rise from 1,000 a day . . . we know more Internet crime is out there, it's just a matter of victims knowing where to go to report it and then actually reporting it" (US DOJ, 2002). The IFCC website also offers a place to submit suspected terrorist activity. In the same press release, the IFCC was praised for collecting over 100,000 tips about terrorist activity without problem. This is in fact one of the easiest and least complex websites where one can go to report fraudulent activity.

The Internet Watch Foundation (IWF), an independent UK-based organization, launched in 1996, focuses on combating illegal content on the Internet, especially child pornography. This particular group has been funded by subscriptions from UK industries as well as through funds from the European Union under the *Safer Internet Action Plan.* The IWF seeks to implement proposals drawn up in co-operation with the governments, police forces, and Internet providers. These proposals are implemented by using the "R3-Safety Net," the three R's being, rating, reporting, and responsibility. In essence, if users take responsibility for the content they place on the Internet, the Internet Content Rating Association (ICRA) rates it and inappropriate content is reported to the proper place then the Internet will be a safer venue for all users. As already stated the focus of this foundation is on child pornography, however, it also takes other types of illegal content into consideration. This particular association also provides policies for traceability for illegal content and how Usenet groups should be conducted.

Although not a tip line in the strictest sense of the word the Recherche et Etude sur la Criminalité Informatique Française RECIF (translated - Research and Study of Computer Related Crime) association aims at the exchanging of ideas and experiences to combat computer related crime between its members as well as between other organizations. RECIF tries to reach this goal through the collection of information, creation of documents their dissemination among members. This organization also provides information on computer viruses to the public.

6.2 Task Forces and Investigation Bodies

Task forces are law enforcement creations that are charged with focusing on one particular crime and have a multidisciplinary and multi-level approach to solving the problem. Some task forces consist of many different departments and others are created using only one department. For example, a typical state task force in the US would be created by utilizing local, state, and federal personnel and resources. Federal task forces tend to either come together with the resources of

various federal departments or within the department itself. There are, however, no specific rules regarding the creation of task forces. These are an important part of our crime-fighting arsenal, however, their role is not usually one of prevention as their job usually occurs after the crime has been committed and work most effectively within the investigation stage. This is particularly true within the United States.

The Innocent Images National Initiative (IINI) was started in 1995 when it became clear to the FBI that adults were using technology to send illicit photographs of minors and to make contact with children for the purpose of exploitation. A central office receives text and online images gathered from ongoing investigations all over the nation and abroad. This office serves to organize and collect all the information about the various investigations that are occurring and incorporates it into their case management system. They have a particular focus on people who indicate a desire to travel across state lines to make contact with children as well as those who would enjoy some type of financial gain from the online exploitation of children. They also focus on major producers or distributors of child pornography in addition to the people who upload child pornography onto the Internet or various online services.

The initiative has remained possible through its commitment to using creative investigative techniques and current technology to apprehend perpetrators. Over the lifetime of this particular initiative, they have significantly increased the number of cases opened, investigated, and prosecuted. For example in 1996, they opened only 113 cases compared 1,559 in 2001. This first year of operation saw 68 convictions or pretrial diversions while the year 2001 saw 540. The IINI continues to receive federal funding and maintains contacts with several independent and commercial online service providers, all of which add to the success of this project (Federal Bureau of Investigations, 2002). The Cyber-smuggling center as discussed earlier also focuses on child pornography. In addition, it trains and assists state, local, and foreign law enforcement on various aspects of this crime. It averages one child pornography arrest every two days (Celentano et al., 2000).

The Office of Juvenile Justice and Delinquency Prevention, also in the US, created the Internet Crimes against Children (ICAC) program, which develops training, and technical assistance programs to respond more effectively to the threat of online sexual predators. This program encourages the creation of regional task forces, which it has succeeded in doing in over half of the states (Cyber Criminals, n.d.). In addition, ICAC funds could be used to start safety education and prevention programs for children, parents, and educators.

The FBI's National Computer Crime Squad has national jurisdiction and investigates violations of the Computer Fraud and Abuse Act. Some of the crimes they investigate include, but are not limited to, industrial espionage, computer intrusion, and privacy violations. This particular squad coordinates its efforts with its foreign counterparts who have an interest in a particular case.

Some states in the US have computer crime squads who are concerned with computer crime in general in addition to a specialized task force related to children. One example of a general task force is the High Technology Crime and Investigations Support Unit (HTC/ISU) in New Jersey. This unit consists of two civilian and nine sworn police officers and spends most of its time investigating or assisting with investigations on a wide array of computer related crime. This unit

also provides training to other law enforcement agencies as well as other civilian institutions such as educational or business organizations (Celentano et al., 2000). Another state that has several task forces is California. This particular state has both types of task forces (crimes against children as well as general computer crime). In addition, they also have "High-Technology Investigation Teams."

The National Infrastructure Protection Center (NIPC) engages in intelligence collection work from the various industries as well as foreign and domestic governments. The NIPC, housed within the FBI, seeks to build a connection between the public and private sectors in order to protect the nation's critical infrastructures (oil, gas, telecommunications, electrical power, transportation, emergency services, and water). The NIPC has three main functions: computer investigations and operations, analysis and warning as well as training, outreach and strategy.

The NIPC is attempting to follow an example set by the US banking industry, which created a private computer network that shares information anonymously regarding various threats. The InfraGard is the NIPC's version of this information-sharing network and is comprised of the public and private sectors as well as academic communities. The InfraGard chapters are created at a local level with local, state, and federal participants; this allows the team to create personalized approaches to local problems. The basic goal is to create a network of information sharing about, but not limited to threats, vulnerabilities, disruptions, and trainings. By creating an InfraGard chapter, local members have access to a secure website that contains significant amounts of information regarding the protection of the various infrastructures (Information Warfare, 2002; National Infrastructure Protection Center, n.d.). The creation of NIPC demonstrates the growing dependency on technology and is changing how America protects itself. The government is attempting to collaborate with the private sector in a way that has never been done before in regards to security issues and there will be many problems to resolve regarding privacy and what is expected from each party. This collaboration is particularly important as the private sector controls nearly 80% of the nation's infrastructure.

Computer Emergency Response Team and Coordination Center (CERT®/CC) located at Carnegie Mellon is probably the most well known and established group. This particular organization provides an information sharing and analysis center as well as collects and responds to computer security issues. CERT teams exist for both federal and state bodies and seek to maintain secure systems through research and response to security issues. They perform both a preventative and an analytical approach to the problem. They collect and compile data about past security issues as well as write research reports designed to help professionals protect their systems and become more knowledgeable about potential security threats.

Europe is not without its own set of task forces and investigative bodies. The German government, in 1991, created the Bundesamt für Sicherheit in der Informationstechnik (BSI). The goal of this governmental organization is to develop criteria, investigate, and provide certification services to the information technology sector. This is done in the hopes that it will facilitate the development of better security (BSI, 1990). Although the BSI is a governmental organization, it cooperates with privately run companies. One example of this is the taskforce for 'Sicheres Internet' (secure internet). Furthermore, BSI has drawn up recommendations for Denial of Service-attacks (DoS) attacks.

In 2001, the CERT-Bund was created, which is the German computer emergency response team. This particular CERT-Bund is also a member of FIRST (Forum of Incident Response and Security Teams), which was founded in 1990 and has more than 100 members today. Apart from the CERT organizations in the various EU Member States, other members are privately run companies. In addition to the North American and European CERT's other members include Asian, South American, and Australian CERT's.

6.3 Institutional Actions

Institutional action could be any set of activities designed to prevent the commission of a computer crime created by a given body. Large numbers of institutions are concerned with computer crime such as individuals who come together for a purpose like the Anti-defamation league, small businesses, multi-national corporations, and everything in between. Other institutions include governmental bodies that are charged with protecting society from criminal activity. All of these have their own idea about what could be done to prevent computer crime. Some are more notable or creative than others and some are found repeatedly in the literature.

In his book *Fighting Computer Crime* (1998), Parker presents the basics of what should be done to protect one's information. Within a company, it is important to have segregation of duties, which in essence means that one person should not have exclusive access to the information. This allows for cross checking among employees and limits one's ability to commit fraud. It is not foolproof but it is a good system to ensure one person does not have all the power. This is also a good policy to protect oneself if an employee is fired; the company will not be at a complete loss without their skill set and will be able to protect themselves appropriately. Another suggestion given by Parker (1998) is to ensure the entire staff understands and agrees with the security measures that are implemented. Ensuring the staff understands and supports these measures will in turn increase the likelihood that they will take the extra few minutes in the morning to update their virus protection, as an example. The institutional policy and attitude towards security can make a substantial difference in the employees' behavior

Some companies engage in what are termed "tiger team attacks" or in some kind of ethical hacking behavior. This has received mixed reviews; some groups contend it is good way to discover security problems. Others say it should only be used in the most honest manner and a system administrator should always know they are under attack if the company has engaged in these actions. It is important that if we, as a global society, choose to support hacking to reinforce defenses that we do not lose the ethical portion. Unfortunately, many children may not know what ethical hacking is and think they are improving their skill set when in fact they are breaking the law. Hacking has played and continues to play a crucial role in the development of technology but it must be taught and treated with respect if future hackers do not want to be the group now called "crackers," which denotes a group of people who do not subscribe to the original hacker "ethical" code.

In a creative effort to combat online fraud, the US Securities and Exchange Commission (SEC) created what they call "Cyberforce." This particular unit is composed over 200 professionals including accountants, lawyers, and investigators who have been trained to find online fraud. This group of professionals is overseen by the Office of Internet Enforcement, which identifies areas to monitor and outline investigative procedures for prosecution. According to the SEC website about the Office of Internet Enforcement (US Securities, 2002) it maintains contact with many international bodies as well.

The most creative aspect of this particular institution is its implementation of "surf days" wherein people surf all day looking for online frauds. The first International Internet Surf Day was March 28, 2000, and was initiated by the International Organization of Securities Commission. Over twenty international bodies participated in this effort to combat online fraud. This effort continues today and is also used by other agencies such as the Food and Drug Administration who utilized a surf day to help Veterinarians search for animal food that was being sold on the Internet and did not meet regulatory standards (Food and Drug Administration, 2000).

The Federal Trade Commission created one of the most publicized and creative ways to get consumers' attention. They have several tip or hot lines that are mostly focused on consumer issues such as a help line for fraud tips and another line for Identity theft. According to the Computer Crime Report (2000) the FTC stated that one of the tools they used in the battle against fraudulent websites was to create their own website that looks like a fraudulent offer. If the person viewing the website responds to the ad, they see a notice that says the following:

If you answered an ad like this, you could get scammed. We're the Federal Trade Commission. Here are some things you need to watch out for if you are looking for a home based business opportunity on the Internet.

This campaign is designed to get the consumer's attention and will direct them to the appropriate resources. In addition, the FTC publishes reports regarding the top ten online scams as well as what it has been done to combat online auction fraud (Federal Trade Commission[FTC] October, 2000; February, 2000).

Within the European Union, a number of initiatives have also been created. For example, the European Working Party on Information Technology Crime (EWPITC) was formed in 1990 under the authority of Interpol. This group has met three times a year since its inception. In January of 2001, the Secretariat hosted the 30th meeting of the working party. This group consists of members from Austria, Belgium, Denmark, Finland, France, Germany, Italy, Netherlands, Norway, Portugal, Sweden, Switzerland, Spain, and the United Kingdom. The working party has completed many projects in the last twelve years. It has created many handbooks which are continually updated and offers several training courses.

The above-mentioned organizations form a small selection of the number of organizations working in this field within the European Union and the United States. These examples highlight the fact that these associations can be government as well as privately run. In most organizations, governmental and privately run entities attempt to cooperate. Because of the diversity within the various organizations throughout the EU and the US, it is nearly impossible to create a complete overview. Not only would this list be extremely large, but new co-operation's are initiated every day.

7.
CONCLUSIONS

What has become clear after reviewing the various available strategies is that the main problem continues to be an ill-informed public. Both the United States and the European Union have made great efforts in this front. More states and individual countries than not have computer crime laws and the larger governmental bodies have not shied away from creating federal statutes and/or initiatives to help battle this problem. Regretfully, it may all be in vain unless the individual users are informed about safe computing practices and take precautionary measures before they are victimized. In order to drive a car, one must pass a test, in order to use the library one must get a library card and read the policies. Regulating is not likely to be the answer as issues of privacy and e-commerce are very real but we must take a step back and attempt to educate users about the dangers they face in an effective way. Keeping in mind that those who log on for the first time will not search out the large number of websites with safety information, thus, it must be disseminated in another format.

CHAPTER 5

PRIVACY VERSUS COMPUTER RELATED CRIMES PREVENTION STRATEGIES

1.

THE DEFINITIONS OF PRIVACY

Privacy is a human right recognized worldwide, however, no universally accepted definition exists. Definitions of privacy vary widely according to interpretation, context, and environment. In many countries, the concept has been fused with data protection, which interprets privacy in terms of personal information. Outside this rather strict context, privacy protection is frequently seen as a way of drawing the line at how far society can intrude into a person's affairs (Singh, 2000). According to Privacilla Organization, privacy is best defined as "a condition people maintain by controlling who receives information about them, and the terms on which others receive it." Following this, Privacilla Organization sees privacy as "a personal, subjective condition, depending on a person's level of tolerance for information sharing. Two factors are in place when a person has privacy: the ability to control personal information or the existence of choice to release information; and the perception that this control is consistent with the person's value" (Privacilla Organization, May 2001).

The concept of privacy can be divided into different dimensions. In their study about privacy and human rights, the Electronic Information Privacy Center (EPIC) and Privacy International (PI) describe these dimensions as follows (Banisar, 2000):

- **Information privacy** involves the regulation of the collection, distribution and processing of personal data such as credit information, medical and government records. It is also generally referred to as "*data protection.*" According to DJ Freeman (2001) personal data can be defined as data which relates to a living individual who can be identified from the data directly or when the data is used in conjunction with other information, held, or likely to come into the possession of the data handler (the data controller or data processor).
- **Bodily privacy** concerns the protection of a person's physical privacy. This is particularly relevant in the area of procedures such as genetic tests or drug testing.
- **Privacy of communications** covers the confidentiality and privacy of all types of personal communications such as mail, telephones, and e-mail.
- **Territorial privacy** concerns the protection of a person's domestic and other environments such as the workplace or public space. This relates to searches, video surveillance, and ID checks.

Privacy on the Internet is generally focused on *information privacy* or *data-protection.* However, privacy of communications is also of importance when referring to privacy on the Internet, particularly if it concerns communication by e-mail or other forms of telecommunications.

Considering the definition of privacy varies significantly according to circumstances and interpretation, national governments have produced various ideologies as to what encompasses the consumer's privacy. Consequently, there are different policies with regard to privacy protection across the world. This makes the regulation of privacy even more difficult. What is believed to be an infringement of privacy in one region does not necessarily transfer to other regions of the world. Thus, those regions may be less regulated regarding privacy issues. Criminals who

operate in different jurisdictions around the world often abuse this fact. Moreover, non-congruent consumer privacy policies hinder the growth of worldwide e-commerce. As a result, there is a strong need for internationally harmonized privacy regulations, applicable to different situations and regions (Singh, 2000).

Internet users concerns regarding privacy vary unpredictably according to specific demographic segments and according to individuals within these segments (DeLotto, April 16, 2001). In addition, research indicates that privacy concerns vary according to different factors such as age, race, national origin, and gender.

The Gartner group therefore recommends that policy makers consider the specific privacy concerns within different communities and develop a "single, uniform, and easily understandable consumer privacy policy." In order to assess the efficacy of such a policy, it should be tested across various groups to make sure it is interpreted according to the policy makers' intentions.

2.

PRIVACY RELATED ISSUES

Privacy is a fundamental human right, with a history that goes back several centuries. The protection of privacy is recognized in all of the important international and regional instruments on human rights, and is included in nearly every national constitution worldwide, either explicitly or implicitly. As a response to the rapid evolution of information technology, most recently written constitutions not only focus on the respect for private life, but also focus on specific rights regarding the use and dissemination of an individual's personal information. International agreements that protect privacy rights, such as the International Covenant on Civil and Political Rights adopted by the United Nations (UN) or the European Convention on Human Rights (ECHR), have been implemented into local law in many countries. Moreover, many countries around the world are ratifying comprehensive data protection laws to protect individual privacy (European Information, 2000; see also European Commission, March 6, 2002; Banisar, 2000; Freeman, 2001.).

Despite the legislation in this area, privacy is being increasingly challenged. The information economy has generated a substantial amount of data. Individual users of the Internet can engage in different types of online activities such as using credit and financial services, shopping, and ordering various types of products. Thus, the growth of the Internet and electronic commerce has dramatically increased the amount of personal information that is collected about individuals. Correspondingly, this has increased the potential to invade a person's privacy.

Personal data can be gathered from the Internet by several means, such as registration pages, user surveys, online contests, and application forms to name a few. While surfing the Internet, individual users often unwittingly leave a trail of personal details. Computers routinely collect much of this information for a variety of reasons and purposes. According to Goemans (2002) the particularly open and decentralized structure of the Internet creates many of the opportunities to collect, save, and profile large amounts of personal data.

The loss of privacy through the growing use of the Internet is not limited to adults but must now be extended to children as they too are going on line in larger numbers. When using the Internet, a significant amount of personal data is collected from children, often without parental knowledge. More worrisome is the posting of personal identifying information by and about children in interactive areas such as public chat rooms. Non-reliable sources could easily find and abuse this information (FTC, June 1998).

New technologies (such as data warehousing or data mining) create several opportunities to collect personal information online. Companies often use this data to create a 'user's profile' and to offer personalized services. This can certainly be advantageous because companies only approach customers for products or services that would correspond to their supposed needs and interests. On the other hand, however, this can also lead to receiving all types of commercial advertisements in their mailbox, with or without their consent. The unexpected commercial phone calls during dinner to promote a certain kind of product are the 'real' world version of this type of profiling. Normally, companies can only use personal data for

telemarketing purposes if the user has given his or her consent (for example by clicking on an online box). Unfortunately, in most cases, users are not even aware they have provided this consent.

In addition to the availability of new technologies, the speed at which they evolve is also a threat to ones privacy. Often these technologies are developing faster than legislation, leaving significant gaps in privacy protection. Another concern is that these new technologies are being exported to developing countries that lack adequate protections, which facilitates privacy invasion within these countries.

Besides the growth of the information economy, other macro trends are threatening privacy. According to EPIC and PI (Banisar, 2000), three macro trends can be identified. Most importantly, the increasing globalization removes geographical limitations to the transfer of data worldwide. The global application of the Internet makes it very easy to transfer information across borders. Furthermore, technological systems are increasingly convergent with each other, enhancing the mutual exchange and processing of different forms of data. Another contributing trend to the increasing threat to privacy is the fact that modern multi-media systems combine different forms of transmission and expression of data and images. Thus, the information gathered in one form can be easily translated into other forms.

In the context of computer related crime, privacy is violated in a variety of ways. New technologies can be used to gather and disclose personal data without the individual's consent. In addition, criminals can take over a person's ‘virtual identity” to commit criminal offences using another person's name. Finally, personal data that is collected online can be sold or distributed to third parties without the individual's consent. Invasion of ones privacy is a fundamental aspect of many of the crimes that are perpetrated using current technologies.

When discussing the prevention of computer related crime, privacy is a crucial issue. The main challenge in this field is to find the proper balance between preventive measures and the right to one’s privacy. In the name of the fight against "cyber-crime," countries may implement decisions and laws that could lead to a breach of an individual's rights to privacy on the Internet. Within this context, privacy is threatened even further by the demands of intelligence and law enforcement agencies that are requesting an increase in surveillance powers. Following this, there is a strong need for improved regulation, oversight, and stricter enforcement of current laws, to ensure compliance with the privacy legislation. According to Dumortier and Goemans (2000), this could explain the move towards the adoption of comprehensive national data protection laws, enacted in several countries since 1974.

However, there seems to be a consensus that legislation alone will not solve online consumer privacy problems, as this might be an obstacle for the further development of e-business. It is agreed that the enacting of this legislation alone to prevent privacy invasion, might be an obstacle to the further growth of e-business. For example, as stated in an article of the Information Technology Association of Canada (2000), some legislation meant to protect privacy might also criminalize the exchange of information, as well as some types of research and testing activities that are required to develop tools to detect security weaknesses and to protect against virus-attacks. Legislation should therefore be combined with self-regulative measures and be adapted to changing situations and technologies.

It is commonly accepted that co-operation is needed between government and industry as well as other parties expressing an interest in privacy protection. This ensures that all viewpoints are taken into account. Besides, enforcement of the legislation is mandatory. Policy makers commonly agree on the necessity of an implementation organism to control and monitor privacy policies. Currently, there is an ongoing debate about whether privacy should be protected through legislation or through self-regulation.

In addition to the legal importance, privacy protection is also mandatory for further development of e-business. The main factor underlying the growth of e-commerce is the amount of confidence consumers have in the protection of their personal data, which is sent worldwide. Surveys have indicated the increasing concern of consumers about the privacy of their personal information used within the electronic marketplace (FTC, June 1998). Adequate privacy protection can therefore be seen as a sort of "quality-label" for businesses engaging in Internet services (M. Walrave personal communication, May 6, 2002). Ultimately, enterprises will profit from defining and implementing good privacy policies, as this will contribute to consumers' confidence and wish to engage in electronic transactions.

The consequence of these threats to privacy would be that consumers are increasingly concerned about the confidentiality of their online data. Consumers feel they have lost control over their own information and often have the perception that they do not know who is using their information and for what reason. In the view of FTC Chairman T.J. Muris at a conference in Cleveland Ohio (2001), consumers are especially worried about some of the possible consequences that can result if their personal information is misused. Some of those could be defined as the following:

- **Risks to physical security** - Fear of the misuse of information about children, home addresses, or telephone numbers by stalkers or other criminals.
- **Risk of economic injury** - Fear of identity theft and/or the misuse of credit card numbers or similar items.
- **Concerns for practices that are unwanted intrusions into daily lives** - Unwanted phone calls, spam, or unsolicited e-mails.

Currently it can be said that there are three points of view concerning privacy issues. First, the less developed nations express little interest in the problem of online invasion of privacy, simply because most consumers do not have access to the Internet. Because of these countries vulnerability to poverty and crime, security is a greater issue than privacy. Second, the European approach to privacy, which is similar to Japan, Hong Kong, and China. These countries have enacted extremely strict privacy laws (Singh, July 2000). Finally, the United States has adopted a more liberal policy towards privacy.

3.

MODELS OF PRIVACY PROTECTION

Because the potential for privacy invasion has increased, society has attempted to control this type of violation through several means. Commonly there are three different approaches to ensure privacy protection: legislation, self-regulation, and technological mechanisms. Most countries use each of these approaches simultaneously, either complementarily or contradictorily, depending on their application. Ideally, they should be well integrated with each other.

As already indicated, *legislation* is an important way to safeguard privacy. Beginning in the early seventies, national governments have increasingly adopted privacy laws to respond to the larger numbers of privacy invasions. In general, privacy legislation can be divided into two categories: either comprehensive or in sectors (Hallawell, 2001 May 4; Banisar, 2000; Freeman, 2001; M. Walrave, personal communication, May 6, 2002).

Comprehensive laws refer to the protection of privacy by a general legislation and the establishment of an oversight body to ensure compliance. The EU, as well as by most other countries enacting data protection laws have adopted this model. This type of legislation primarily covers data that can be related to a particular individual. However, it also addresses the protection of corporate data but to a much lesser extent. It is important to note, that the protection of corporate privacy could be seen as contributing or even being mandatory, to the privacy of consumers' data. According to DJ Freeman (2001), legislation concerning data protection does not create a right of privacy, as such, but it aims to achieve a balance between freedom of expression and the individual's right to privacy.

A variation of the comprehensive legislation model can be described as the "*co-regulatory*" model (Banisar, 2000). Under this regime, the industry develops rules for the protection of privacy and enforces compliance with these rules through the oversight of a privacy agency. This last model was adopted in Canada.

Instead of these general protection rules, some countries, such as the United States, have enacted specific *sectoral laws*. Enforcement of these laws is not achieved through an oversight body, but rather through a range of mechanisms. Specific sectoral laws are sometimes used complementarily to comprehensive legislation by providing more details regarding the protection for certain categories of information, such as telecommunications, medical, or government records.

Although privacy legislation is increasing worldwide, its efficacy depends on the implementation of the laws in practice. Control, guidance, and sanctioning are therefore mandatory. To be effective, legislation needs to be adaptable to the changing situations and technological developments.

According to surveys conducted by EPIC and PI (Banisar, 2000), countries adopt comprehensive privacy and data protection laws for several reasons. First, they may adopt them to remedy privacy violations that have occurred in the past (e.g. Central Europe, South America, and South Africa). Some laws are designed to promote electronic commerce by ensuring consumer confidence in the privacy of their personal data, which is sent worldwide. Finally, some ensure compatibility with

international standards developed by international institutions such as the United Nations, the Council of Europe, and the Organization for Economic Co-operation and Development (OECD).

Many countries in Central and Eastern Europe are also adopting new laws to be consistent with Pan-European laws, because they hope to join the EU in the near future. Considering the strict data protection regime of the EU, other countries outside the EU, especially the US, see themselves as obliged to adapt their legislation to ensure that trade will not be effected by the requirements of the EU Directives.

In addition to legislation, an important aspect to protect privacy is ***self-regulation***. This refers to various forms of self-regulative measures taken by businesses and enterprises to protect individual privacy, such as internal and external codes of conduct, practical guidelines, and self-policy. Traditionally this has been the policy adopted within the US.

Self-regulation can only be effective if the defined guidelines or rules are implemented in their entirety. In practice, this is not always the case. In the absence of enforcement bodies, most enterprises define privacy policies but do not always integrate them in their daily business practice. To be competitive, enterprises often publicize their privacy policy without having first educated their internal resources. Privacy policies should therefore only be communicated externally after they have been implemented internally (M. Walrave personal communication, May 6 2002). According to the Gartner group (Hallawell, March 2001), Web privacy policies are designed more to protect the enterprise from legal liability than to grant higher levels of privacy protection to the consumer.

A third way to approach privacy protection is through technological means, which relates to the so-called ***Privacy-Enhancing Technologies*** (PET). Individual users of the Internet can enhance their privacy in a variety of ways. With the recent development of commercially available technology-based systems, users can rely on a range of programs and systems that provide varying degrees of privacy and security of communications. Some of those techniques useful for users are the following (see also London Internet Exchange [LINX], 2001; Hallawell, 2001, May 4; Singh, Cowles and Rendall, 2001; European Commission, 2000 November):

- Encryption systems, such as 'Pretty Good Privacy' (PGP), 'Secure MIME' (S/MIME)
- Encryption between a web server and a user's web browser
- Anonymisation software
- E-mail filters and anonymous re-mailers that strip off the identity of the sender of the mail
- Chained systems
- Freedom Network
- Cyber Smart advice provided by some websites to help minors safely use the Internet.[9]
- 'Platform for Privacy Preferences' (P3P, Microsoft)
- 'Watchfire WebCPO'

[9] For an example see: http://www.iwf.org.uk/safe/children.htm

Companies use privacy enhancing technologies to protect themselves against privacy invasion, either from external or internal sources. In its working document of November 2000, the European Commission Data Protection Working Party stresses the importance of "privacy compliant, privacy friendly, and privacy enhancing technologies." However, within this context, it also recommends consultation on whether or not new technologies are compliant with existing data protection legislation. In this document the working party suggest that it may be useful if industry and the public put in place a system of certification marks.

4.

INTERNATIONAL INITIATIVES CONCERNING PRIVACY

The growing concern for privacy has led to the creation of several international policy instruments. The main principles covered in these instruments, are all based on the consensus that a balance needs to be found between the increasing flow of information worldwide and an individual's privacy. In other words, between the fundamental but competing rights of "respect for private life" (privacy) and "the right to seek, receive and impart information" (freedom of information), respectively Articles 8 and 10 of the European Human Rights Convention (Douwe, 1998).

The Council of Europe, the OECD, and the United Nations (UN) adopted the most important international instruments.

THE COUNCIL OF EUROPE

In 1950, the Council of Europe adopted the *'European Convention on Human Rights'* (ECHR).[10] Article 8 of the Convention states that each person has the right to the protection of their private life, family life, home, and communication. According to Goemans (2002), two aspects of this are important regarding privacy on the Internet: the confidentiality of private communications and the protection of personal data. Article 8 of the ECHR represents the most important legislative provision in Europe on privacy protection.

The Council of Europe has also adopted a comprehensive approach towards data protection. Some important instruments of the Council of Europe are the following:

- The '*Convention No. 108 for the Protection of Individuals with regard to the Automatic Processing of Personal Data'* was adopted in 1981. This convention has binding force and requires Member States to implement the defined principles of data protection into national law. However, it does not oblige contracting parties to establish institutional mechanisms for the independent investigations of complaints. There is no requirement for additional mechanisms such as an oversight body (Dumortier & Goemans, 2000).
- *Recommendation R (99) 5,* provides principles for the protection of individuals with regard to the collection and processing of personal data on information highways.

THE OECD

On September 23, 1980, the OECD adopted the *Guidelines Governing the Protection of Privacy and Transborder Flow of Personal Data*. The Ministers attending the 1998 OECD Conference on Electronic Commerce created the guidelines, which have no binding force, and are only stated 'to [be] take[n] into account' in national

[10] http://europa.eu.int/comm/internal_market/en/dataprot/law/ fechr.htm#8

legislation. Eight principles are stated within these guidelines, all of which concern the collection, use, security, and disclosure of personal information (Gosh, 2001):

- Collection Limitation Principle
- Data Quality Principle
- Purpose Specification Principle
- Use limitation Principle
- Security Safeguards Principle
- Openness Principle
- Individual Participation Principle
- Accountability Principle

THE UNITED NATIONS

Article XII of the Universal Declaration of Human Rights (1948);

Article 17 of the *International Covenant on Civil and Political Rights*, adopted on December 16, 1966;

UN Guidelines concerning *Computerized Personal Data Files*, adopted on December 14, 1980. These guidelines contain minimum guarantees for data protection that should be provided in national legislation and outline provisions to ensure enforcement.

Taken together, all of the above-mentioned instruments provide international minimum standards for data protection, which should be incorporated into local law. To ensure compliance with these instruments many different national laws have been created.

5.

PRIVACY REGULATIONS WITHIN THE EU

5.1 GENERAL DIRECTIVE ON DATA PROTECTION

At the European level, consumer privacy is well guarded through the current data protection regime. The main framework within the European Union Member States for data protection is provided by the EU General Directive on Data Protection,[11] which passed through the European Parliament and Council on October 24, 1995, after years of negotiation. It came into effect in 1998. European Union Member States were required to implement the directive into national law by October 24, 1998, but Article 32 allowed for derogations. Enforcement is achieved through the establishment of an oversight body.

The main purpose of the directive [12] is to ensure minimum standards of data protection so personal information can be transferred between EU Member States. The directive aims to harmonize national data protection regimes, to find a balance between individual privacy rights and the free flow of data within the EU and to foster economical and social growth.

The Data Protection Directive provides rights to the individuals about whom information is gathered, also known as "data subjects." The directive applies to any processing of personal data falling within this scope, irrespective of the technical means used, such as the collection of data, storage, and disclosure. Article 4 outlines, more specifically, the application of the Directive. The following is an excerpt from the EU website regarding this particular objective:[13]

Each Data Controller (the person who determines the purpose for which and the manner in which any personal data is to be processed) has to comply with the provisions of the Member State where he or she is established, even if the personal data relate to data subjects established in other Member States, except where the Controller is established in another Member State as well. In this case, the law of the country of that establishment is applicable to its processing. When the data subject is not established in the Community, he or she has to comply with the law of the Member State(s) where the processing equipment (e.g. computing center) is located. Controllers established out-side of the Community are required to appoint a representative in the Community.

---

[11] Full Article available on http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31995L0046&model=guichett.

Status on the implementation of the EU Directive 95/46/EC : http://europa.eu.int/comm/internal_market/en/dataprot/law/impl.htm

[12] Information about the directive is gathered from different sources: Hallawell, 2001 May 3; European Commission, 2000 November 21; Freeman, 2001; Privacilla Organization; Dumortier and Goemans, 2000; M. Walrave, Personal communication, May 2002.

[13] http://europa.eu.int/comm/internal_market/en/dataprot/backinfo /info.htm

European data protection legislation has to be applied to data collected using automated or other equipment located in the territory of the EU or the European Economic Area (EEA), i.e the EU Member States plus Norway, Iceland and Liechtenstein, as stated in Article 4, 1.c.

Article 28 outlines the enforcement of the directive, through the establishment of the 'Data Protection Commission,' which consists of different national data commissioners. All EU Member States must have an independent oversight agency to control privacy protection and treat complaints. If data protection laws are not respected, these agencies have a legal power to impose sanctions. In addition, the national data protection commissioners have the responsibility to prevent privacy abuse, educate the public and to safeguard privacy protection within data transfers to third countries.

According to the EU legislation, data processing is permitted as long as it is transparent. Individuals have wider privacy rights, which are clearly outlined in the basic principles of the directive:

- Individuals must be informed about the processing of their personal data, which data is collected and for which purpose (*transparency*). Websites must inform data-subjects by publicizing their privacy policy.
- The data collected should be accurate, and if necessary, be updated.
- Data subjects must have easy *access* to the information collected about them and must have the right to correct it if the data appears to be inaccurate. In certain circumstances, a person should have also the right to object to the processing of his or her data. In this case, the data commissioner decides if processing is allowed.
- The information collected about a person can only be used for the specific *purpose* for which it was originally collected. It is prohibited to further process personal data for a non-compatible use. The data collected should also be retained no longer than necessary for the purpose for which they have been collected.
- Data controllers must ensure *fair and lawful processing* of personal data, as well as *data-protection*. They have to take technical and organizational security measures that reflect the risks presented by the processing of data.
- Companies that want to use personal data for *direct marketing*, or want to transfer the data to third parties for this reason, can only do so if the data subject is informed about this and has been given the opportunity to object.
- *Sensitive information* (for instance information relating to racial and ethnic background, political ideas, health, or sexual preferences) can only be collected if the data subject has given his/her explicit consent and if the collection occurs under specific safeguards.

The most controversial principle outlined within the general directive is the prohibition of personal data transfers without the consent of the data subject, to countries outside the EU where privacy protection laws are considered inadequate (article 26). Although the directive foresees several exceptions to this article, this requirement puts great pressure on countries outside Europe to pass privacy laws if they wish to engage in information transfers. For example, enterprises located in countries outside the EU with inadequate privacy legislation, can only use or store personal data generated in the EU, if this happens in compliance with the principles outlined under the directive. Such companies are required to obtain the explicit permission of the individuals involved and to gain approval from the national data

protection commission of the concerned countries. To obtain the approval companies have to ensure that the data will be adequately protected during the transfer (Hallawell, May 3, 2001).

The Commission, assisted by a committee of Member State officials and a Working Party (the national data protection authorities) considers the "adequacy" of data protection measures for transfers outside Europe on a case-by-case basis. In the worst case, it can be decided to block a certain type of data transfer to a non-EU country. This blocking should then apply across the EU as a whole or not at all. Several other methods exist to ensure data protection during data transfers that do not disrupt international data flow (European Commission, 1998).

It is not impossible to transfer European information to destinations that are seen as providing inadequate data protection. The directive provides several exceptions, for example, if companies, themselves, can ensure data safeguards by providing appropriate contractual clauses or if individuals have given their approval to transfer their data outside the EU.

Another exception is if the transfer is necessary to close a contract in the interest of the data subject. The Commission has adopted a decision on this particular matter on December 27, 2001 (2002/16/EC). This decision defines *'standard contractual clauses'* for transfers of data to *processors*[14] or subcontractors established in third countries that do not offer an adequate level of data protection. This decision complements the previous decision approved by the Commission on June 15, 2001 (2001/497/EC), which applies to the transfer of data to *controllers* rather than processors. The use of such standard contractual clauses will be voluntary.

Until now, the Commission has recognized Switzerland, Hungary, Canada, and the US Department of Commerce's Safe Harbor Privacy Principles as providing adequate protection.[15]

Most European countries have now implemented the directive into national legislation. However, the way this has been done differs from country to country. In spite of these differences, common trends in the implementation can be identified (Freeman, 2001):

- There is a requirement for registration or notification with a central authority.
- Data must only be used for certain purposes.
- It is usually necessary to obtain the consent of the data subject before disclosing data.
- Individuals have access rights to their personal data.

The major challenge of the EU directive remains, however, to translate the outlined principles and the resulting national laws into practice. The 'Article 29 Working Party' has written several guidelines or recommendations about the application of the directive. However, national regulators can still view the implementation of the EU legislation differently. For example, Belgium, France, Denmark, and Germany have extended the "sensitive" category, which requires explicit consent by the data

[14] A controller determines the purposes and means of data processing, while the processor processes data on behalf of the controller (http://europa.eu.int/comm/internal_market/en/dataprot/modelcontracts/95-46faq.htm)

[15] http://europa.eu.int/comm/internal_market/en/dataprot/modelcontracts/02-102.htm

subject, to include financial information, national identifiers and the building of consumer "profiles" (Hallawell, May 3, 2001).

Although the European data regime presents strict rules, several exceptions can be exploited. In certain situations, EU Member States are required to establish derogations from their national data protection laws, in order to strike a balance between the right to privacy and the right to freedom of expression as well as freedom of the press and the media. In addition, national law might provide for other exceptions particularly if they are necessary on the grounds of national security, defense, crime detection, enforcement of criminal law or for the protection of data subjects or the rights and freedom of others.[16]

According to Chapman (2002, February), the institutions have to find a better balance between protecting the rights of individuals and protecting the rights of legitimate commercial interests. In his view, there should also be more guidance and less prescription. This year, the workings of the directive are being evaluated by Commissioner Frits Bolkestein's internal market directorate-general.

Based on the general directive, the EU has enacted some other legal provisions. The specific directive on *Privacy in Telecommunications*, adopted on December 15 1997 (Directive 97/66/EC),[17] was created particularly to protect privacy during the processing of data in publicly available telecommunications services. Among other provisions, the specific directive requires providers of telecommunications services to take the necessary security measures and respect the confidentiality of communications. The directive also states that traffic and billing data must be erased or made anonymous upon termination of the call. In this case, traffic data refers to the various types of data that is systematically logged during Internet connection. The directive of 12 July, 2002 (58/CE) represents the updated version of the specific directive from 1997, aimed protecting privacy in 'electronic' communications services.[18] Other EU regulations also deal with privacy protection on the Internet, but most of them do not specify extensive rules for data protection and leave regulation of this to the general directive.

5.2 The Safe Harbor Agreement

As previously explained, the general directive restricts data transfers to third countries outside Europe that do not have the same level of data protection as the EU. This puts great pressure on countries outside Europe. As a response to this directive, the European Commission and the US Department of Commerce

[16] http://europa.eu.int/comm/internal_market/en/dataprot/backinfo/info.htm

[17] http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31997L0066&model=guichett

[18] http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexplus!prod!CELEXnumdoc&lg=en&numdoc=52000PC0385

negotiated the "Safe Harbor Agreement."[19] This aims to offer protection for US companies who want to process European data in the US. Companies who joined Safe Harbor agreed on a voluntary "self-certification" program, by ensuring compliance to the main principles of the general directive. They also agreed to be overseen by some type of US authority, like the FTC, another national oversight agency or an EU national data protection authority. This oversight authority would check the companies' data protection level.

On July 26, 2000, the EU Commission recognized the Safe Harbor international principles and the program came into effect on November 1, 2000. From that time, the US Department of Commerce opened the online self-certification process for US organizations that wish to join Safe Harbor. Since December 1, 2001, 129 US based organizations have signed up with the program. All participating companies are listed on the publicly available website of the US Department of Commerce.[20] Although the number of US organizations joining Safe Harbor is lower than expected, it is foreseen that this number will grow in the future.

However, in its working paper of February 13, 2002, the EC Commission Staff reported that several organizations that joined Safe Harbor, do not express the expected degree of transparency concerning their privacy policies. In this same document, the Commission staff mentions that adequate enforcement is a key element in the Safe Harbor framework. The EU Commission and the US Department of Commerce are currently working together to improve these issues.

A problem mentioned with Safe Harbor is that some sectors were left out of the deal. In an interview with European Voice (Chapman, 2002), senior data-privacy official Stefano Rodotà said that "financial services were excluded because they are not controlled by the Federal Trade Commission." The US media industry was also excluded from Safe Harbor. The 'Article 29 committee' of national data protection commissioners (the Working Party), is examining other model contracts that offer an alternative to joining Safe Harbor.

[19] Information derived from the EC Commission Staff Working Paper, February 13th 2002; Hallawell, May 3, 2001; EU Website: http://europa.eu.int/comm/internal_market/en/dataprot/news/datatransf.htm

[20] http://www.export.gov/safeharbor

6.

PRIVACY REGULATIONS IN THE US

6.1 GENERAL POLICY AND ACTORS

In contrast to the European comprehensive approach to privacy protection, the United States has adopted several sectoral laws regulating individual privacy.[21] Different federal laws cover specific categories of personal information, such as financial records, credit reports, video rentals, cable television, telephone records, educational records, and motor vehicle registrations. There is no explicit right to privacy in the US Constitution.

The *'Fourth Amendment'* of the US Constitutions serves as a legal framework for law enforcement in the information society and tries to find a balance between privacy and public safety. Under this amendment, the government must demonstrate 'probable cause' before obtaining a warrant for a search, arrest, or other significant intrusion on a person's privacy. A search without a warrant is only possible if it does not violate a person's "reasonable expectation of privacy" or in the case of an established exception. For example, this type of search is allowed if it is to prevent physical harm or if an authorized person has given his consent to perform the search on private information (US DOJ, 2001).

The collection of data by businesses has traditionally been protected as commercial free speech (relating to the *'First Amendment'* jurisprudence on commercial free speech). According to the US liberal theory, it is the market rather than the law that should shape information privacy through self-regulation. In practice, this means that the information collected on an individual belongs to the "collector" rather than to the individual from whom it is collected. According to the Gartner group (Singh, 2000) the democratic lawmakers have, until now, been the most vocal advocates for consumer privacy legislation, while the Republicans have sided with the industry.

Another striking difference when compared to European privacy regulation is that no independent oversight agency exists within the US. The Office of Management and Budget (OMB) plays a limited role in setting policy for federal agencies under the Privacy Act (see previous section). Within the OMB, a special office was created in early 1999 to coordinate federal attitudes regarding privacy. In addition, a Chief Counselor of Privacy was appointed who has only limited advisory capacity.

An important body regarding privacy in the US is the FTC. However, they only have oversight and enforcement powers for the laws protecting children's online privacy, consumer credit information, and fair-trading practices. They have no general authority to enforce privacy rights (Banisar, 2000). Despite this lack of authority, the FTC has adopted several recommendations concerning consumer's privacy online. Over the years, the FTC has expressed an approach in favor of self-regulation. This has been with the belief that the safeguarding of privacy will not only contribute to greater protection of consumers, but also increase consumer confidence and finally their participation in the online marketplace. In 1998, the

[21] Information gathered from Di Gregory, 2000; Gosh, 2001; Privacilla Organization; Banisar, 2000

FTC wrote its "*Fair Information Practices,*" which represents a common view on how privacy protection should be achieved (FTC, June 1998). The general principles are as follows:

- **Notice/Awareness**: Data controllers must inform individuals about their disclosure practices before collecting personal information (what information is collected, for which purposes, how it will be used). One way to accomplish this is to publish privacy policies online.
- **Choice/Consent**: Individuals must be given choice with respect to the use and dissemination of their personal information. The consumer must be given the chance to opt-out, which requires affirmative steps to prevent the collection and/or use of this information. In comparison, opt-in regimes require affirmative steps by the individual to allow the collection and/or use of his or her information. This is particularly important if companies want to use the collected information for purposes other than originally stated, either internally (for direct marketing reasons) or externally (transfer of information to third parties). This can be done for example, by clicking a box screen.
- **Access/Participation**: Consumers must be able to view the data collected about them and to contest its accuracy and completeness.
- **Integrity/Security**: Data controllers must take reasonable steps to ensure data protection and integrity.
- **Enforcement/Redress**: The FTC recommends the adoption of a mechanism to enforce compliance with fair information practices; for example, through external audit of enterprises, by making compliance a condition of membership in an industry association or through certification programs. At a minimum, there should be institutional mechanisms to treat consumer complaints and find remedies for violations of privacy.

The FTC conducted a survey in 1998 about industry association fair information practice guidelines, to assess their compliance with these principles. The results showed that industry association guidelines generally encourage members to provide notice of their information practices and some choice with respect to this, but they fail to provide for access and security or enforcement mechanisms. The FTC also investigated the practices of 1,400 US commercial websites relating to privacy. The survey revealed that almost 85% of the examined sites collect personal information from consumers. Only 14% provide any notice with respect to their information practices and even fewer, approximately 2%, provide notice by means of a comprehensive privacy policy (FTC, June 1998).

6.2 US Legislation

Despite the absence of a comprehensive law, there are several sectoral laws to protect privacy. The '*Privacy Act*' of 1974 protects records held by US government agencies and requires agencies to apply basic fair information practices. The surveillance of wire (cable), oral and electronic communications for criminal investigations is regulated by the '*Omnibus Safe Streets and Crime Control Act*' of 1968 and the '*Electronic Communications Privacy Act*' (ECPA) of 1986. According to

these federal wiretap laws, surveillance of wire, oral and electronic communications is only allowed if it is based on a court order.

The ECPA, passed by the Congress in 1986, aimed to include new communications technologies into the wiretap laws. This law is specifically targeted at e-mail and Internet Service Providers. It provides the legal framework in which the government can gain access to stored information, such as e-mail, account records, or subscriber information, from electronic communication service providers. Based on the seriousness of the privacy interests involved, ECPA offers varying degrees of privacy protection for different types of information. For example, the content of an e-mail does not require the same level of protection as a user's account information. Despite these legal requirements, investigators try to use new technologies and surveillance techniques under the authority of the ECPA law (US DOJ, January 2001). One of the technologies they attempt to use is "Carnivore," which has the ability to scan e-mails for key words and then alerts the authority to monitor that account for suspicious activity.

Surveillance for national security purposes is governed by the *Foreign Intelligence Surveillance Act.* This particular act, however, has lower legal requirements than its criminal investigation counterpart. The federal wiretap laws were amended by a controversial bill in 1994, named the *Communications Assistance to Law Enforcement Act*. This required telephone companies to redesign their equipment to facilitate electronic surveillance. Suffice it to say, the use of electronic surveillance in the US has more than tripled in the last ten years.

An important legal provision is the *Children' s Online Privacy Protection Act* (COPPA). This law was passed by Congress in 1998 and came into effect in April 2000. Based on this law, businesses can only obtain information from children for commercial purposes, such as e-mail addresses, after the parents have given their approval.

The *Freedom of Information Act* (1966) allows for broad access to federal government records by any requestor, except for those records held by the courts or the White House. This was amended in 1996 by the *Electronic Freedom of Information Act*, which specifically provides access to electronic records. There are also laws in each state that provide access to government records.

New privacy regulations for the financial services and healthcare industries also affect enterprises on a larger scale. For example, in July 2000 American financial institutions were required to comply with the *Gramm-Leach-Bliley Act*, adopted in 1999, which foresees increased inspection of the institutions to ensure they are compliant with the financial privacy regulations. Furthermore, in order to be able to process European information and to comply with European legislation, US businesses feel obliged to make considerable changes in their daily practices of information collection and usage. As previously discussed, the Safe Harbor deal has been an important advancement in this matter.

Although there is reluctance to develop a comprehensive federal law protecting privacy, it is generally recognized in the US that some type of action is required. It is commonly agreed that a general framework for privacy regulation is needed, together with an oversight body and enforcement mechanisms to ensure compliance. On March 13, 2002, the 'Senate Republican High Tech Task Force' released its policy goals for the rest of this congressional session. Among other

goals, it stressed the importance of consumer privacy on the Internet and e-commerce (Privacy Law Adviser, March 20, 2000).

Spam, which is the sending of unsolicited advertising e-mails to customers, without their consent, has prompted industry groups and anti-spam organizations to express the need for a federal standard instead of the multiple state laws. Unfortunately, they disagree on how far such a federal law should go (Hallawell, March 2000). Several consumer groups such as the 'Online Privacy Alliance' and the 'Electronic Privacy Information Center' (EPIC) are also gaining attention and have requested immediate actions to protect consumer privacy on the Internet.

7.

TRADE-OFF BETWEEN CRC PREVENTIVE STRATEGIES AND PRIVACY

7.1 INTRODUCTION

Respect for privacy is of growing concern in the prevention of computer related crime. The main challenge in this domain is to find a proper balance between the fight against computer related crimes and an individual's right to privacy. With the increasing flow of computer related crimes and terrorist attacks, a worldwide climate has been shaped to enhance the monitoring of data and take the necessary measures to prevent that type of activity. Of course, September 11, 2001 has contributed dramatically to this growing tendency. However, as previously mentioned, prevention policies can have serious consequences for personal privacy rights. Privacy is also under threat by the demands of intelligence and law enforcement agencies for the increase of surveillance powers.

Privacy policies do not necessarily have to hamper strategies to prevent computer related crime; they can also be a part of solution (M. Walrave personal communication, May 6, 2002). In the long term, privacy protection could even be an associate of prevention policies, by decreasing the possibility of invasion to privacy and misuse of personal information. These types of protective policies would also contribute to further the growth of e-business. A company, whose practices are based on a good privacy policy, that is well communicated both internally and externally, will more than likely increase the consumer's confidence in their online transactions. If users have the perception that their online personal data can be abused, they will respond critically and may hide their identity by giving false information. Consequently, companies would then base their marketing strategies on false information. Businesses should therefore be conscious of the fact that effective privacy policies represent a quality aspect and that it is in their best interest to safeguard individual privacy.

7.2 RELATION BETWEEN CRC PREVENTION STRATEGIES AND PRIVACY

LEGISLATION

SURVEILLANCE AND INTERCEPTIONS OF COMMUNICATIONS

The increased concern for computer related crime has led to a call for surveillance of communications and methods for preserving electronic evidence. Nearly every country in the world has established some form of surveillance of communications, including telephone, fax, telex, and electronic surveillance. In most countries, these interceptions are initiated and authorized by law enforcement or intelligence agencies, such as the police or legal bodies who have a power to demand information.

Law enforcement agencies (LEA) frequently work together with telecommunications companies to investigate or prosecute a crime. In this context, LEA demand access to user information about traffic data, telephone calls, e-mail messages, and other forms of communications. A number of countries are demanding that ISPs install "black boxes" on their systems that can monitor the traffic of their users. These boxes are systems based on "packet sniffers" typically used by computer network operators for security and maintenance purposes (Banisar, 2000).

SURVEILLANCE AND INTERCEPTION OF COMMUNICATIONS IN THE EU

According to European law,[22] monitoring of data is allowed as long as it is transparent. The involved persons must be informed regarding the reason for the monitoring, how their data is collected, for whom and how long. Interception of e-mail is illegal, unless authorized by law in specific cases for limited purposes, in accordance with the European Convention of Human Rights (ECHR) and the European Data Protection Directives. Sniffing refers to use of software for electronic surveillance and interception wherein the traffic data is monitored and all the data packets on a network system are read. Large scale sniffing is only allowed if in accordance with Article 8 of the ECHR (right to privacy).

At present, interceptions of communications by law enforcement agencies require an authorization by a judicial order or in the case of two EU Member States, a warrant personally authorized by a senior Minister. This approval for interception is decided case by case and must comply with Community laws. For example, the use of interception must be limited to investigations of serious crimes, and interception has to be necessary and proportionate. Similarly, interceptors must ensure that the individual is informed about the interception as soon as it appears that informing him would no longer hamper the investigation (European Commission, 2000). Within European legislation, disclosure of personal information is therefore weighted against the balance between individual privacy and the prevention of computer crimes. For severe offences like child pornography, privacy is generally inferior to the tracing of the criminals.

The European Commission has created several initiatives on this matter. On August 25, 2000, the EC put forward a proposal to update the specific directive from 1997, to better protect privacy in 'electronic' communications services.[23] The European Parliament accepted a compromise on this on May 30, 2002 (see section on data retention). On January 26, 2001, the European Commission adopted a communication on “Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-Related Crime” (2000). April 23, 2002, marked the adoption of a new proposal to combat cyber-crime. This proposal provides for a Council framework decision on "attacks against

[22] Information gathered from the following sources: European Commission, 2001 November 6; www.statewatch.org/news/2001/may/03Cenfopol.htm; www.statewatch.org/news/2001/apr/07swdata.htm; EC Working Party, 2000 November; http://www.epic.org/privacy/intl/data_retention.html

[23] http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexplus!prod!CELEXnumdoc&lg=en&numdoc=52000PC0385

information systems" (European Commission, 2002, April 19). It aims to protect users and to improve the security of information infrastructures, while considering other issues such as network security, law enforcement powers, privacy, user rights, the development of new technologies, and economic priorities. With the adoption of the EU Convention on Mutual Assistance in Criminal Matters (Council of European Union, May 29, 2000), an approach has been agreed upon to facilitate co-operation on legal interception between the EU Member States.

According to the European Commission Communication 890 (2000), new technical interception requirements on telecommunication operators and Internet service providers should be coordinated internationally to prevent distortions of the European Single Market, to minimize the costs for industry and to respect privacy and data protection requirements.

The European Information and Communications Technology Industry Association (EICTA) has suggested several recommendations on this matter (EICTA, 2000). According to EICTA, surveillance and interception of telecommunications have to be conducted under lawful conditions. The provisions and requirements for interception have to be well formulated and allow for review at court. Any misuse with respect to espionage or unauthorized infringement of privacy has to be prevented.

Moreover, the involved person should have the right to information about the interception of his data. The whole interception process must be controlled and supervised by the court and a proper balance needs to be found between the interests of law enforcement and privacy. Furthermore, EICTA stresses the importance of harmonization between the different national legislations and safeguards, which in practice may differ much from one another. This would facilitate international co-operation.

The Article 29 Working Party (November 5, 2001) highlights its concern for procedural law measures to collect personal data on individuals suspected of having committed computer related crimes. According to the same Working Party, these measures could end up being very wide in scope, to the extent that they could be applied to all types of crime and not just computer related crimes.

Surveillance of communications should therefore only be allowed if there is a legal basis, a social need and if other less invasive measures are absent. Law enforcement agencies should only be able to process the connection data that are necessary for their specific request.

SURVEILLANCE AND INTERCEPTION OF COMMUNICATIONS IN THE US

The debate about the interception of telecommunications has been ongoing in the US for several years. Privacy in regards to this matter is protected by several laws. As previously stated, most important are the Fourth Amendment, the Electronic Communications Privacy Act, and the Wiretap Statute. Under the Fourth Amendment, the government must demonstrate probable cause before obtaining a warrant for a search, arrest or other significant intrusion on privacy. Legally, interception of communications is only allowed if authorized by a court order.

Real-time electronic surveillance is covered by two federal statutes. First by the wiretap statute, that initially passed as *Title III of the Omnibus Crime Control and Safe Streets Act* in 1968. This allows the government to disclose the contents of wire and electronic communications. The second legal statute for electronic surveillance is the 'Pen Registers and Trap and Trace Devices chapter of Title 18' (also known as the "the Pen/Trap statute"). This concerns the collection of addressing information relating to wire and electronic communications. For example, regarding e-mail, the addressing and routing information includes the e-mail address of the sender and recipient, as well as information about when and where the message was sent.

However, over the years the US government has been promoting greater use of electronic surveillance. Police and intelligence services are demanding the usage of surveillance techniques such as “Carnivore” and “Echelon.” These techniques however, are used within the domain of state security, which is a separate subject that falls beyond the scope of this study and cannot be treated in this context.

The US has also been working through international groups such as the OECD, G-8, and the Council of Europe to promote increased surveillance. Since 1993, the FBI has organized at its research facility in Quantico, Virginia, the "International Law Enforcement Telecommunications Seminar" (ILETS). Present at these meetings have been representatives from Canada, Hong Kong, Australia and the EU. Based on these meetings, several "international technical standards for surveillance" have been adopted, like ENFOPOL 98, created by the EU Police Co-operation Working Group in which interception standards were set that apply to new communication technologies (including the Internet and satellite communications). Several proposals have been made to update the ENFOPOL 98 document, to better define the scope of the interception standards (Banisar, 2000).

DATA RETENTION

The logging of traffic data or "data retention" is a leading item in the fight against computer related crime. At issue is the length of time during which Internet service providers or telecommunications services have to keep traffic data in their systems. Indeed, to investigate or prosecute a crime, law enforcement authorities frequently use traffic data, which is stored by service providers, telecommunication operators, or access providers for billing purposes.

Traffic data refers to all the types of data that is systematically logged during an Internet connection, such as login credentials, IP address, location (Beirens, 2002). An expert statement of the European Working Party on Information Technology Crime - EWPITC - and Interpol, describes in more details the importance of traffic data for law enforcement agencies. Generally, traffic data is used by police forces to "trace back and locate geographically and chronologically the end user device that was used to transmit the initial information" (Beirens, 2002). The purpose of data logging is clearly not to make profiles of individual telecommunications users.

According to Beirens (2002), the availability of traffic data is particularly crucial for LEA as new technologies provide the possibility to remotely control and operate different types of computers and telecommunication systems from anywhere in the world. These operations can have serious consequences in the real world, for instance, breaking into computer systems, sabotage of telephone systems, blackmail, harassment, and defamation. Such offences can easily be perpetrated

without being physically present and in the absence of any witnesses and without leaving physical traces.

Another good reason for keeping and using traffic data is that the personal information given online by the Internet user is generally not reliable enough for criminal investigation because most subscribers use nicknames or false identities. The only reliable information for LEA to identify the person responsible for criminal offences is therefore telecommunications traffic data.

According to the expert statement from the EWPITC, the following data is "vital" to investigate or prosecute a computer related crime: the identifying elements of the source and destination of the communication and the date and time of the connection (Beirens, 2002). In criminal offences against computer systems, as well as in computer-facilitated crime, electronic data is the essential element to identify the perpetrator and to prove the criminal act.

However, at present no legislation exists that requires the retention of traffic data specifically for law enforcement purposes. Under both existing European directives on data protection, personal data may only be held for specific purposes and for the appropriate amount of time to meet those purposes. After a given period, the data has to be destroyed. Traffic data must be erased or made anonymous immediately after the telecommunications service is provided, unless it is necessary for billing purposes.

For flat-rate or free-of-charge access to telecommunications services, the service providers are in principle not allowed to preserve traffic data. Under the EU directives, Member States "may" adopt legislation to restrict the scope of the obligation to erase traffic data when this is necessary for the prevention, investigation, detection, and prosecution of criminal offences or unauthorized use of the telecommunications network. Such measures have to be appropriate, necessary, and proportionate as required by European and international law, especially for measures that would involve the routine retention of data on a large part of the population. Lately, the price charged for communications has become less dependent on distance and destination, and service providers are moving towards flat rate billing. Consequently, there will no longer be any need to store traffic data for billing purposes. This will reduce the potential material for criminal investigations.

Law enforcement authorities are therefore demanding the adoption of “data retention” [24] requirements. This would force communications service providers to routinely capture and store users' communications and traffic data for at least a minimum period, this data could then be available for law enforcement purposes. In most cases, a long period of data retention is necessary to cover the preparation phase, as crimes are not always immediately discovered. Besides, even if the crime is discovered, the victim may still need some time to decide if he or she will file a complaint (Beirens, 2002).

[24] Information gathered from the following sources: European Commission, 2001, November 6; www.statewatch.org/news/2001/may/03Cenfopol.htm; www.statewatch.org/news/2001/apr/07swdata.htm; European Commission, 2000 November; http://www.epic.org/privacy/intl/data_retention.html

Although data-retention can be an efficient way to combat computer related crime, it must be balanced against personal privacy. Privacy advocates fear that data-retention will give police forces great power to keep records on phone calls, faxes and e-mails, which could then lead to large-scale storage of personal electronic data for long periods of time (Reuters, 2002). If data is systematically monitored to prevent abuse, this could lead to a breach of privacy for all concerned persons, not only for persons who intend to commit a crime, but also for all persons whose data is involved. In this view, privacy advocates fear serious damage to user's confidence in the privacy of their information sent online.

Law enforcement agencies are aware that the logging of traffic data has to be realistic and should not hamper economic growth. Against that background, they are requesting that only the type of data that is mandatory to investigate and prosecute a crime be stored. A compromise between all parties involved needs therefore to be found.

According to the European Commission, any solution on the issue of data retention should be well founded, proportionate and meet the interests of all parties involved. All stakeholders must be involved in the process of policy-making.

The European Parliament has generally taken a forward position in the debate of data-retention. It favors a strong protection of personal data, except for the combating of child pornography on the Internet. In this latter case, the Parliament has expressed an opinion favoring a general obligation to preserve traffic data for a period of three months.

The National Data Protection supervisory authorities took a position in favor of strong data protection. In its Recommendation n°3/99 adopted on September 7, 1999, the Article 29 Data Protection Working Party strongly recommends that traffic data should not, in principle, be kept only for law enforcement purposes (1999). National laws should not oblige telecommunications operators, services, and providers to keep traffic data any longer than necessary for billing purposes.

In the debate about data-retention, ISPs and telecommunications providers mostly fear that the logging of traffic data for a longer period will imply additional costs to them. In fact, they need to have the appropriate equipment to maintain traffic data and provide the necessary security protection, as required by the European Data Protection legislation. These costs need to be well estimated and divided between all parties involved. In addition, the industry also fears that individual users would negatively perceive too much monitoring of data. In their view, this could hamper further growth of e-business.

Recently, the debate about data-retention has entered a crucial stage within the EU. The fight is now centered on the proposal for a reviewed directive on “the processing of personal data and the protection of privacy in the electronic telecommunications sector.” This would update the 1997 directive on data protection, to cover new means of telecommunications such as the Internet and e-mail. In December 2001, the Council of the EU (composed of the 15 Member States) agreed on a position that would allow for data retention and its surveillance by law enforcement agencies. The proposed law calls for the companies to keep traffic data for a period beyond the one or two-month period that is normally necessary for billing purposes.

Several Member States are demanding the preservation of traffic data to investigate serious crimes like child pornography and provocation to racial hatred. Belgium, France, Germany, Netherlands, Spain and the UK want to update the 1997 directive and delete the requirement that traffic data must be erased or made anonymous unless for billing purposes. The reason for that is to give LEA more access to electronic data. The Netherlands, Belgium, and France have already taken steps to require the retention of data.

Initially, the Parliament was strongly opposed to the reshaping of the draft data protection law. In regards to this matter, it has released a report from the Committee on Citizens' Freedoms and Rights that is strongly in favor of the existing Directives and against data retention. On May 30, 2002, the two biggest parties in the European Parliament (the Socialist Party and the center-right European Peoples' Party) agreed on a compromise (Meller, 2002; Reuters, 2002). In this compromise, it is stated that online and telephone surveillance of citizens by law enforcement should be appropriate, proportionate, and limited in length. It must also conform to the European Convention on Human Rights. Under the approved bill, companies in the EU will have to immediately erase electronic data after the period needed for billing purposes, which is usually one or two months. National governments can force operators to store data for a longer period, if necessary for security reasons. This has to be written down in national legislation. In addition to the provisions about data-retention, the approved law also calls for an opt-in approach for unsolicited e-mails or spam. Online marketing companies and other Internet operators are only allowed to send commercial e-mails if the customer has given their approval. The bill also prohibits the placing of invisible data-tracking devices such as "cookies" on a computer until after the user has been properly informed about its use and purpose. The EU governments will officially adopt this new law within a few months and it will be implemented by the end of 2003.

In the US, there is no general law that regulates how long network service providers must store information. According to the seriousness of the privacy interests involved, different levels of protection exist for several information categories. For account records, there is also no general rule that states how long ISPs must preserve the information on their systems. Some providers retain records for months, others for hours, and others not at all. In practice, this means that electronic data may be destroyed or lost before law enforcement agencies can obtain the required legal approval to ask for disclosure of the information. To minimize this risk, the Electronic Communications Privacy Act permits the government to order providers to "freeze" stored records and communications, while waiting for the required legal court order (US DOJ, January 2001). This act also allows law enforcement agencies to order a provider to preserve records that have already been created, but they cannot ask providers to preserve records that have not yet been made. If agents want the providers to store information in the future, this request falls under the electronic surveillance statutes.

To effectively combat computer related crime, legislation concerning data retention should be harmonized. If different countries implement different legislations, this may hamper the ability to cooperate internationally in the investigation or prosecution a crime. This could also be a problem for international companies in that they will have to log their traffic data for a different length of time for each country in which they operate.

INTERNATIONAL CO-OPERATION

Because of the global character of computer crimes, law enforcement authorities are often seeking access to electronic data stored in foreign countries. For data that is not publicly available, investigators face a dilemma when tracing data in foreign states. If they do not copy data quickly, offenders of computer related crime could erase it. Furthermore, if investigators copy the data without first asking the permission of the foreign state in which it is located, they are confronted with serious issues relating to the state sovereignty and the privacy rights of the persons involved.

International instruments try to deal with this issue in a variety of ways. One example can be found in the principles adopted by the G8 in 1999 (UN Economic and Social Council, 2001). One principle that was agreed upon states that data could be freely accessed if publicly available; for example, on an open website, or after a statutory authority has given his approval to access and disclose the data. For data not publicly available, the principles adopted by the G8, involve a request for *mutual legal assistance* between the requesting state and the state in which the data are located. The latter would then be asked to take immediate steps to maintain the data. The transfer of the data to the requesting state would then be accomplished using more conventional proceedings and safeguards for mutual legal assistance. Unfortunately, this procedure is well known by offenders. They exploit it by routing their communications through a large number of different countries between the source and the destination, or by routing them through countries that lack the laws or the infrastructure to conduct traces of their communications.

Often administrative procedures to disclose electronic data from other countries are too slow. Law enforcement agencies are frequently confronted with legal and operational constraints to obtain a quick exchange of information; for example in the preparation of cross border evidence and victim identification. For these reasons, it is mandatory that fast and efficient co-operation between law enforcement agencies in trans-national cases exists.

The establishment of a network of contacts could be one way to achieve fast international co-operation. The G8 has established a 24 hours a day/7 days a week information network with points of contact from various law enforcement agencies. This network is already operational and aims to receive and respond to urgent requests for co-operation in cases involving electronic evidence (European Commission, 2000). The Council of Europe and the US have already taken several other initiatives for such a network.

OTHER LEGISLATION

In its communication on 'Creating a Safer Information Society', the European Commission also mentions other legislation that can interfere with privacy (European Commission, 2000):

- A*nonymous access and use of the Internet:* This contains a duality for governments and international organizations that is difficult to evaluate. The Article 29 Data Protection Working Party has written a Recommendation on this subject (1997). On the one hand, the possibility to remain anonymous on the Internet is essential to preserve fundamental rights to privacy and freedom of

expression in cyberspace. On the other hand, this anonymity runs against policies to fight computer related crime such as distribution of illegal and harmful content, financial fraud or copyright infringements. The possibility to engage in online activities without revealing one's identity could seriously decrease the possibilities for law enforcement agencies to investigate or prosecute a crime. According to the Working Party, a balance needs to be found between these two policy objectives, as it has been done in the real world. Principles concerning anonymity in offline forms of communication (such as television, newspapers, radio, etc) should be extended to the online world.

- *Procedural law powers and jurisdiction:* After the necessary legal requirements are fulfilled, law enforcement authorities should be able to search and seize data stored in computers. This should be done fast enough so that criminals do not have the opportunity to erase the criminal evidence. When this procedure involves data stored in different countries, serious issues arise concerning state sovereignty, human rights, and privacy protection.
- *Evidential validity of computer data:* Once electronic data has been accessed, law enforcement agencies need to be able to use it in criminal investigations and prosecutions.

CONCLUSION

In the prevention of computer related crime, law enforcement needs to find a proper balance with the respect for individual privacy. Extensive data monitoring will be negatively perceived by Internet users. As Kevin Di Gregory (2000) writes, public confidence in government will erode if privacy is not respected. A lack of consumer's confidence in online privacy will also block further growth of e-business. On the other hand, law enforcement has to be efficient as well. If law enforcement is too timid, cyberspace will become a safe haven for criminals and terrorists to communicate and conduct crime, without any fear of authorized government surveillance.

It is also important for law enforcement agencies to retain the possibility to identify a person who has committed a computer related crime, obviously after the necessary approval has been obtained (court order or statutory authority). It is generally agreed that legislation can only be efficient if it is combined with enforcement, control and sanctioning in case of non-compliance. If there is no link to the 'real identity' behind a perpetrator, effective sanctioning will be difficult (L. Beirens, personal communication, June 5, 2002).

Di Gregory (2000) recognizes three challenges in this context:

- Technical challenges that hamper law enforcement's capacity to locate and prosecute criminals that operate on the Internet;
- Keeping legal provisions to combat cyber-crime up to date with the changing technology;
- Lack of resources within law enforcement.

It is also important that legislation to prevent computer related crime is harmonized worldwide. Harmonization would certainly facilitate international co-operation and avoid the migration of criminal offences to 'safe havens'. Efforts should be made to agree on common definitions, incriminations and sanctions (European Commission, 2000). It is important that certain types of behavior are criminalized in the same

way in different countries. Unfortunately, this is not always the case. What is defined as privacy invasion in one country can be seen differently in another country. As privacy protection varies accordingly, it can be expected that this will make it even more difficult to define a proper balance between the prevention of computer related crime and privacy issues.

Taskforces or forums that consist of all parties involved (government, business, users, etc…) can certainly help to analyze the trade-off between legislation and personal privacy.

SELF-REGULATION

Different self-regulative initiatives have been created by the industry as a response to computer related crime, such as internal guidelines, codes of conduct. To be effective, these measures should be well communicated both internally and externally. Resources should be assigned to control compliance to internal regulations and necessary actions need to be taken in case of non-compliance. Management should define priorities and make resources available to control self-regulation. The 'most critical data' for the company has to be defined, enabling one to take the necessary security measures for protections against criminal attacks (L. Beirens, personal communication, June 5, 2002).

Although self-regulation and compliance are a way for industry to prevent computer related crimes, it may contain a threat to privacy. As a response to the terrorist attack of September 11, 2001, companies have called for an increase of surveillance on their employees' e-mail and Internet usage. Monitoring in the workplace is only allowed however, if employees have been informed about it beforehand (or at least are made aware of the possibility that surveillance exists).

Belgium has recently adopted, a new Collective Labor Agreement to regulate surveillance by employers on their employees (Van Eecke, 2002). This agreement states that employers have the right to reasonably control their employees' computer behavior. For example, the employer can forbid his employees to install new software on their computers for private usage, but he cannot forbid them to use the Internet in general. Moreover, employers have the right to control the Internet behavior of their employees, but only if the latter have been informed. The surveillance can only be performed to control four elements: inappropriate behavior, behavior that can bring serious damage to the company's interests, behavior that can bring serious damage to network systems, and finally conduct that is not allowed according to the internal policy of that particular enterprise. In addition, the surveillance has to be targeted to all employees in general, not to one specific individual. To ensure that this aspect is respected the controlling program has to work with anonymous lists and data. As soon as the employer has discovered something unusual, the person involved can be identified in order to take the necessary actions. With this new agreement, an important effort has been made to regulate surveillance in the workplace.

As previously described, companies that offer online services have to inform users about their privacy policy. In general, this is done in the form of a box-screen that appears when entering a website. In order to be effective, these privacy policies have to be well communicated internally and externally. Company employees need to be aware of the existing privacy policy and that control has to be established to ensure compliance. Once privacy is respected inside the company, it can be

publicized (M. Walrave personal communication, May 6, 2002). Unfortunately, companies often express privacy policies to be competitive rather than to protect their users' privacy.

The industry must be aware that they have their own interest in combating attacks against their network systems. If personal data is protected more, consumer's confidence will increase which will be translated into more online transactions. Business should therefore realize that they play a key-role in protecting their users and that, eventually, they will derive their own benefit from these actions.

INFORMATION/INSTRUCTION

In the prevention of computer related crime, informative and instructive measures are very important. Making users of the Internet aware of its potential risks will certainly contribute to a safer environment online. Individual users should be informed about the existence of computer related crimes and how to prevent abuse of their online personal information. This knowledge will also increase a person's privacy on the Internet. If people know what the potential privacy risks are, they will certainly pay more attention to it when they engage in online activities. Moreover, users should be made aware of their own responsibility. For instance, as it is unusual in the 'real' world to pass the number of a personal credit card to an unknown person, users should treat passwords and confidential personal data on the Internet in the same way.

Education plays an important role in this type of prevention. Children should learn about 'computer ethics' in grade school. Children have to be aware that the same rules apply for both the real world and the Internet; for example, when they use the Internet, they have to treat other persons' information in confidential manner and to respect another person's work as opposed to copying it. Obviously before educating children, teachers should be well informed about the limitations and advantages of the Internet as well as what type of actions are unacceptable (L. Beirens, personal communication, June 5, 2002).

At the European level, legislation concerning computer related crime and invasion of privacy should be well publicized. Actions that are viewed as criminal offences must be communicated to the public. In addition, information about what should be done when a crime is detected or when one becomes the victim of a crime should also be publicized. The public should know who to contact and where to address complaints. Of course, the same can be said for the US Educational campaigns or programs, which are another way to achieve public awareness.

Although the instructive and informative measures, as regards to computer related crime, are too new to assess their impact, it can be said that these measures will contribute to higher privacy protection. Besides awareness, Internet users should be informed about the availability of programs and software to increase personal privacy online. Different types of technological tools can be used to protect privacy, such as encryption and anonymisation software, such as 'Platform for Privacy Preferences.'

Besides the users, the industry should also be informed and made aware of privacy issues. The enterprises must be aware that it is their responsibility to protect the privacy of their customers' information. They should know which measures to take to avoid privacy invasion and how to inform their users in the proper way.

TECHNOLOGICAL MEASURES

Different types of technological solutions are available to protect the users or the businesses systems against criminal offences. With the rapid evolution of information technology, these technological measures often change faster than legislation. Although software and programs offer differing levels of protection, they must be in balance with a person's privacy. Often these technical measures offer a way to prevent, investigate, or prosecute a crime, but careful attention should be paid to infringements on an individuals' privacy and right to free speech.

Technologies can easily maximize the "traceability" of Internet users through various ways, such as systematically logging relevant traffic data, or through the generalization of authentication certificates and digital signatures. If Internet abusers and criminals have the feeling that they can be identified and prosecuted, the amount of computer related crimes would most probably decrease. It is widely recognized that an important incentive to commit computer related crimes is the possibility for perpetrators to easily remain anonymous. However, it is important to note that the impact of such measures would also increase the visibility of what people do. Unless an independent authority carefully regulates and controls these measures, the privacy of honest citizens is endangered.

Another approach to prevention is to obstruct the spreading of illegal material on the Internet. Internet filters and ISP rating systems are two means of accomplishing this. The problem with the existing products is that such devices are not selective and efficient enough to block only and all illegal content. The impact on privacy of filtering and rating systems, if they were sufficiently reliable, would not be a significant problem as no one should have access to illegal content in the first place.

The use of search tools like "sniffers" or "crawlers" to scan Internet contents and find suspicious or illegal material is also technologically feasible. Such proceedings imply "analyzing" all the material that travels on the Internet. Here again, lack of strong legislative regulation and control endangers one's privacy.

OTHER MEASURES

Other strategies exist to prevent computer related crime, varying from the creation of hotlines and task forces to all types of institutional actions.

Different initiatives have been taken within Europe as well as in the US, to create *hotlines* for incident reporting. However, even here a balance needs to be found concerning privacy needs. When treating complaints, it is important that individual privacy is respected and that personal information is treated confidentially. Third parties should not receive personal data without the users consent. If respect for privacy is not a priority, this can be an obstacle for Internet users to address their complaints to hotlines. To make matters worse, many companies are not willing to report cases of computer abuse. This is often with the intent of avoiding bad publicity and exposure to future attacks (European Commission, 2000).

As commonly agreed upon, taskforces and/or 'think-thanks' are needed to analyze the balance between CRC preventive strategies and individual privacy. All stakeholders with an interest in this subject must be involved, to ensure all viewpoints are being taken into consideration.

7.3 Conclusion

In the prevention of computer related crime, different kinds of measures can be taken that may sometimes conflict with fundamental human rights, such as the right to privacy. Measures like the monitoring or the disclosure of electronic data, can have serious consequences for the privacy of the persons involved. As stated by the 'Cyber-Rights & Cyber-Liberties' organization in the UK (Akdeniz, 2000), "sometimes it may be necessary to infringe the rights of honest Internet users in order to secure the prosecution and conviction of guilty parties." To evaluate the balance between CRC preventive measures and the right to privacy, this organization proposes a test to apply to any measures that are taken:

They have to provide clear benefit for society, with an impact on the rights of honest people that is as small as possible and that is widely accepted as tolerable in the light of the secured benefits.

The measures proposed should discriminate effectively between criminals and honest citizens. If possible, they should not expose all honest Internet users to such risks as government access to encryption keys.

Of all measures available, the proposed measures should be the most effective in terms of cost/benefits analysis.

They should be based on clearly defined policy objectives that are easy to understand and to be supported by the citizens.

The proposed measures should be enforceable, transparent, and accountable.

CHAPTER 6

THE DEVELOPMENT OF THE E-ECONOMY VERSUS COMPUTER RELATED CRIMES PREVENTION STRATEGIES

1.
E-ECONOMY OVERVIEW

1.1 DEFINITIONS

In order to analyze the issue of the development of the e-economy versus computer related crimes prevention strategies, it is necessary to first define the scope of the e-economy and the related concepts.

- **E-economy**: For the purpose of this study, e-economy refers to the economic life of all those actors involved in doing business through the Internet. It is, thus, not limited to the companies that provide services related to the Internet (the ISPs) or to the companies that only do business online (e.g. the "dot.coms"). Rather, it concerns all the companies and consumers that participate in transactions completed on the Internet. As such, an increasing number of traditional companies either participate in the e-economy as a dot.com or as a "brick-and-click" company (see definition below).
- **E-business**: E-business is the activity of doing business online using websites. People often use the terms e-business or e-commerce synonymously, however e-business is a concept that encompasses e-commerce. An e-business site may be more comprehensive and offer more than just the selling of products and services. For example, it may feature a general search facility or the ability to track shipments or it may simply provide information about a company or its products, while e-commerce only concerns itself with the order-processing component of the site.
- **E-commerce**: E-commerce is the activity of selling and buying goods or services online.
- **Business-to-Business (B2B)**: B2B refers to the selling of goods or services to other companies either through a commercial website or by connecting the extranets of different companies together.
- **Business-to-Consumers (B2C)**: B2C refers to the selling of goods or services to private persons through commercial websites. The retailers that set up these websites are often called *e-tailers*.
- **E-Marketplaces**: An e-marketplace is an "electronic mall" where buyers find products from numerous suppliers. Those e-marketplaces can be either B2B or B2C. A well-known example of a B2C e-marketplace is e-Bay where thousands of consumers participate in auctions as either buyers or sellers, everyday.
- **ISP**: ISP or "Internet Service Provider," is the general term used for those companies that provide access to the Internet as well as the storage space necessary to set up web pages and the services to help build and maintain those sites.
- **Dot.coms**: Dot.coms is the term used for those companies specifically created to do e-commerce. They became famous in the late nineties, as they were a driving force behind the high-tech boom. However, many of them went bankrupt when the stock markets collapsed in 2000.
- **Bricks-and-Clicks**: Bricks-and-clicks refer to those companies that do business online as an extension of their principal business activity. The Internet, in this case, is used as a new channel to reach new or existing customers.

1.2 Market size and growth

This section does not have the ambition to provide extensive statistics. Rather it seeks to provide an idea of the importance of this market and its potential. According to researchers at IDC, the number of Internet users has grown to 500 million people, a 27% increase. In terms of sales, B2C trade rose 56% to 112 billion USD while the B2B trade rose 73% to 496 billion USD (Hof & Hamm, 2002). Today, e-commerce represents only 2% of all trade; however, this share is bound to grow with time.

Another study, done by CEI Computer Economics, estimates that the projected size of the B2B market should reach 5,294 billion USD by 2006 (CEI, 2002). This expected growth demonstrates that the general economic slowdown and the stock market crisis of 2000 did not signify the end of the e-economy. It did, however, change the way business is done online.

The current trend is that most dot.com companies, with their large budgets and luring revenue promises, have left the e-market place for financially more healthy bricks-and-clicks companies. These companies do not see the Internet as a market in of itself, but rather as a new distribution channel and as a new technology that will enable them to lower their processing costs.

The growths of B2B and B2C are not perfectly correlated. Some of the main factors related to the growth of B2B and B2C are therefore looked at in more detail.

B2B Drivers and Inhibitors

The three main drivers behind B2B growth can be identified as:

- The lower operational costs
- The possibility to access new markets in other geographical areas; a company does not need to have a physical presence in the country in which it wants to sell its products. In addition, the company can offer proper support for its products through information available on websites and forums.
- The possibility to offer better customer service by taking advantage of data gathering techniques, which allows the business to customize its services to the needs of the client.

B2C Drivers and Inhibitors

B2C growth factors are virtually the same as those provided for B2B with a few additional aspects that affect the number of Internet users willing to do transactions online. The number of potential customers in turn influences the number of retailers that would be willing to invest in a commercial website.

Several factors have a direct impact on the number of users willing to buy online. First, several surveys have shown that the decline of Internet connection prices has had a direct impact on the number of Internet users. The democratization of the fast connection technologies, like ADSL and modem cable, have also had an impact by considerably reducing the time necessary to download a new web page, improving greatly the general experience of the people using Internet. Second, is

the issue of the security; according to the study on Internet use in the US conducted by the Center for Communication Policy, 94.5% of Internet users have at least some worry that credit card information could be used without their permission (Saia, 2002). According to research firm Jupiter, this fear translates into the 60 percent of consumers who prefer not to do transactions online (Bennett, 2001). The final variable, which influences the number of people willing to make purchases online, is privacy concerns. According to another survey of large US firms, the second worst impediment to the Internet growing into a market place are fears about privacy (Institute for the Protection and Security of Citizen [IPSC], 2001).

2.

COMPUTER RELATED CRIMES RELATED TO E-BUSINESS

To analyze the impact of the computer related crime *prevention strategies* on the development of the e-economy, it is necessary to first analyze the impact of the specific computer related crimes. If this is not done, prevention strategies could be seen as a pure cost while they should actually be seen as an investment to reduce the overall financial loss incurred by computer related crimes.

In the same line of thinking, not all crimes have a direct impact on the financial health of a company doing e-business. Crimes like prostitution, child pornography, gambling and trafficking, to name a few, are not expected to have a major direct impact on e-business and will therefore not be covered in this section. Nevertheless, the impact of the prevention strategies for those crimes will be discussed in the next section.

When one tries to gather information on this subject, it is clear that hardly any estimates of yearly security breaches and their financial impact exist. The reason for this seems to be that most companies fear that it would provide bad publicity if those attacks were known to the public, and consequently to their investors, partners and clients. The 2002 CSI/FBI Computer Crime and Security Survey, which is based on responses of 503 companies from different sectors, found that 40% of the respondents did not report the computer intrusions to law enforcement or legal counsel (Power, 2002, p.20), while 90% admitted to have been victim of computer breaches in the last 12 months (Power, 2002, p.4).

The main result of this lack of publicity is that most companies still do not see security as a high priority deserving a larger budget. Currently, most companies doing business on the Internet spend less than 5 percent of their overall IT budget on security (Power, 2002, p.18).

Although the small number of reported cases make it difficult to measure, statistically, the financial loss incurred by these attacks, the cases that came to light show that a single successful attack can cause severe damages, depending on the circumstances.

2.1 TYPES OF CRC THAT CAN IMPACT THE GROWTH OF E-BUSINESS

From the economic literature, it appears that financial fraud, such as identity theft, credit card theft, business fraud, proprietary data theft, and malicious code attacks (e.g. virus, denial of service) are those crimes that cause severe harm to a company.

FINANCIAL FRAUD

CREDIT CARD THEFT

Credit card theft is the most prevalent e-business crime. Furthermore, it is easy to understand why this crime is so common. Database servers are not always properly protected, yet they are often directly linked to the Internet to store the customers' data and transaction information. Therefore, a hacker can break into this type of server and retrieve thousands of credit card numbers for a minimum amount of effort.

Thanks to the Internet discussion forums, card thieves can easily resell credit card numbers, in bulk, to other criminals for an amount that ranges from 0.2 to 0.5 USD per card (Richtel, 2002). These card numbers can then be used to commit fraud. An alternative to reselling the cards is to use the information to extort money from the company that was the victim of the card theft.

E-Business Case: *SawyerDesign.com*

Due to a flaw in its "PDG" shopping cart software, some customer records of SawyerDesign.com were exposed. The card numbers of the victims were used to spend thousands of dollars on gambling sites, or to buy phone cards and expensive software (Power, 2002, p.5).

IDENTITY THEFT AND EXTORTION

Criminals understand that companies value secrecy regarding the ability of hackers to obtain customers personal data from their databases. For this reason, hackers may threaten to publish stolen data on public websites if their victims do not pay a ransom. Some security specialists estimate that there are approximately one thousand cases of extortion every year (Salkever 2000, August 22).

E-BUSINESS CASES:

CDUNIVERSE

This is a typical case of extortion in that, CDUniverse, an Internet music retailer, was asked to pay 100,000 USD to prevent stolen data from being published (Richtel, 2002).

Even though these costs may not seem extraordinary, they often do not account for the full financial loss suffered by the victims. For example, a US bank that was extorted for 10,000 USD reported that its total financial loss was approximately 250,000 USD (Computer Business Review Online, 2002).

BLOOMBERG

Bloomberg was asked for 200,000 USD in "consulting fees" to reveal how the "consultants" had compromised its network. The risk incurred at that time, however, was that the security breach information would be passed on to other hackers. Therefore, Bloomberg had to engage in a long process of negotiations in order to have the time to identify and isolate the weak link in its network of

computers. Considering the complexity of the network, this took several months (Salkever, 2000, August 22). This demonstrates how the 200,000 USD was only part of the total financial loss.

BUSINESS FRAUD

Usually, if the stolen credit card numbers are not used for extortion purposes, then they are used to make payments either to e-tailers or to themselves. Typically, the criminals will use the card numbers to make Internet purchases. Considering most e-tailers only require a card number and expiry date, they have little to no ability to verify that the card has not been stolen. By the time the e-tailers realize that they have been paid with stolen cards, their products have already been delivered.

E-BUSINESS CASES

FLOOZ.COM

Flooz.com, an online seller of currency that could be used as gift certificate, sold 300.000 USD to someone using stolen credit cards. This fraud had more severe consequences than just the financial loss. Indeed, in order to cover potential claims from credit card customers, Flooz.com's card processor withheld daily reimbursements from credit cards sales until it had provisions of about 1 million USD. This resulted in a difficult cash flow situation that probably drove Flooz.com to bankruptcy.

Flooz.com was not the only loser in this case. Many B2C companies considered gift certificates to be a good marketing tool to convince Internet users to buy for the first time on Internet. The final casualties of this fraud were the consumers who had not yet redeemed all their e-currency at the time of Flooz.com's bankruptcy (Tedeschi, 2001).

E-BAY

E-Bay, an online auction mall, has unwittingly facilitated many different types of fraud. In order to pay themselves with stolen credit cards, fraudsters use complex programs to act as sellers and winning bidders of various items (Power, 2002, p.12). Others simply cash in the payments from real customers and never deliver the goods (Lee, 2002). Although these crimes do not have a direct impact in terms of financial losses for e-Bay, the loss of customer confidence presents a threat to the growth of e-Bay's business.

In order to maintain its customer's trust, e-Bay began patrolling the auctions on its sites. Although this action globally enhances the protection of its customers, it had a negative impact on the legal side of its business. By trying to control the activity on its sites, it fell out of the scope of the Communications Decency Act (now deemed unconstitutional) and the Digital Millennium Copyright Act, which protects web business from liability for criminal activities that take place on their site. This resulted in a huge increase in legal costs for e-Bay in order to prepare for the claims that were likely to arise in particular from the software industry for allowing activities that infringe upon copyright policies (Crawford, 2002).

The cases above show that companies rarely mention the total financial losses they have suffered. It is understandable that companies, in general, do not want to bear the consequences for the extra distress caused to investors and partners by disclosing those figures. For this reason, it is interesting to look at the category of "anonymous" disclosures of estimates in the CSI/FBI Survey. It reports 12% of the respondents had detected financial frauds and 5% were willing and able to quantify their losses. The average loss was 4.6 million USD with the maximum loss being 50 million USD (Power, 2002, p.9).

ANALYSIS

Multiple conclusions can be drawn from the cases of observed financial frauds. This activity is not rare, and estimates of their global impact on the financial system range from 1 billion USD to more than 10 billion USD (Richtel, 2002). Small companies are particularly vulnerable since they cannot absorb the cost of an attack in the same manner as a larger company. In addition, attacks may compromise the trust relationship they have with their creditors, which often translates into a squeeze of the cash supply and sometimes into bankruptcy. On top of that, small companies may lack the financial and technical resources to put the right protective measures in place (Information Technology Association of Canada [ITAC], 2000, p.3).

An indirect impact is the accrued financial pressure on e-tailers who want to do business online. Indeed, transaction processed with credit cards cost almost twice as much (2.5 % on average vs. 1.5%). This higher cost was implemented, primarily to cover the risk that a transaction is done with a stolen card (Forsman, 2000).

At the consumer level, the consequence derived from the credit card theft cases, as presented above, is that a larger amount of consumers will not trust online sites with credit card information. Consumer would rather use the Internet to gather product information. Once they have decided to purchase the product, they will go to a real shop for the final transaction (IPSC, 2001). The result of this trend cannot be quantified either, but several impacts can already be identified. First, some sales will probably be lost. Consumers that make up their mind on a product while surfing on a commercial site will buy it if they feel secure enough. However, if they prefer to wait and make the purchase in a shop, there is enough time to change their mind before they pass by a store that sells the desired product. Second, for those websites that sell commodities, the marketing effort they put into their site is likely to be spent for the benefit of the competitors' shop that is nearer to the consumer.

Eventually, this trend poses a problem when trying to estimate the "Return on Investment" of a commercial website. Even if the consumer buys the product from the same shop that advertised it online, no share of the sale will be allocated to the online website even though it is through that channel that the consumer made up their mind. Considering the returns of the website will be underestimated, it will not receive its share of the budget, which would allow it to grow and offer better services to the client. Therefore, this trend is likely to further slow down the growth of B2C trades.

PROPRIETARY DATA THEFT

Proprietary information theft is not something new, and is often called industrial espionage. The Internet has only facilitated the way companies can now do it. Typically, this type of activity results in lost sales or loss of market shares. One can get an idea of the financial damage it can do to a company by looking at the importance of the fines that are usually associated with trade secret theft cases, as they can exceed 10 million USD.

In the 2002 CSI/FBI Survey, 20% were victims of proprietary data theft. Five percent (5%) of the respondents were willing and able to quantify their losses due to the theft of proprietary information. The average loss was 6.6 million USD with the maximum loss being 50 million USD (Power, 2002, p.6).

MALICIOUS CODE ATTACKS (VIRUS, DENIAL OF SERVICE ETC…)

In the CSI/FBI Survey, 85% of the respondents reported that they had been victims of some kind of malicious code attack in the last 12 months. Thirty-seven percent (37%) of the respondents were willing and able to quantify their losses due to this type of activity. The average estimated loss due to such attacks was 283,000 USD (Power, 2002, p.16). The "Melissa" virus alone was estimated to have caused 80 million USD of damages (US DOJ, 2002).

To conclude, all companies that have their network connected to the Internet are likely to suffer from computer related crimes. The damage caused by computer related crimes can take several forms such as, extortion, bad reputation, declining shares, loss of market shares, disturbance of business, etc… The largest threats come from financial frauds and lost business due to theft of proprietary data. These two plagues cost several billions US dollars annually.

An indirect consequence is that the development of business-to-consumer trade suffers from the lack of consumer confidence in the security of commercial websites. This, in some cases, may be a legitimate concern in that many instances of computer breaches happen because of a lack of security. Interestingly, victims of computer breaches are not always those who are responsible for the lack of security (see the Flooz.com e-business case).

This brings to the foreground the important question of responsibility. Who should be held responsible for business fraud perpetrated using stolen credit card numbers? Is the e-tailer responsible for accepting payment using an unreliable authentication method (e.g. the card number plus the expiry date)? Should it be the owners of the commercial website from which the card numbers were stolen? Unfortunately, many owners of such websites are more concerned about putting their site online before a competitor even though not all the necessary security measures have been implemented. Finally, should it be the software provider that released the software without first thoroughly checking the security aspects of it, which is now used by the commercial website? These questions are important because, when the responsibilities are legally binding, they are part of the risk assessments completed before launching a new business and can therefore shape the way a market evolves.

3.

COMPUTER RELATED CRIMES PREVENTION STRATEGIES

3.1 LEGISLATIVE MEASURES

Independent of the need to put in place legislative measures aimed at combating computer related crime, particular effort should be made to harmonize country laws for computer related crimes. Harmonization, in effect, avoids the creation of safe havens where criminals could operate. Considering the Internet is a global and borderless network, countries with little or ineffective legislation are a major attraction for criminals. Furthermore, situations that would procure an economic competitive advantage to a company according to the country in which it is based are avoided.

It is also a common idea that legislation should avoid shifting costs of crime fighting directly to industry players doing business on the Internet (see sections below on *obligation* and *co-operation*). This could have a negative impact, in particular, on the growth of small and medium size enterprises (Global Business Dialogue [GBDe], 2000)

There are also concerns that broad criminal regulations might restrict legitimate research like third party testing and evaluation of software or reverse engineering (World Information Technology and Service Alliance [WITSA], 2000). In the computer security field, these activities are necessary to mitigate risks by gaining an in-depth understanding of the problems and to verify that vendor patches actually work (Levy, 2001). In other words, they are necessary to stay ahead of hackers on the technological ground.

OBLIGATION OF INTERCEPTION OF DATA AND RECORD KEEPING

A law that would oblige Internet Service Providers to maintain historical traffic data records from their servers can be useful for the investigation and prosecution of computer related crime. However, the implementation of the facility to intercept data could imply harsh financial costs for ISPs (European Information and Communication Technology Association [EICTA], 2000) and would ultimately affect the access costs of end users. This would, in turn, negatively impact the growth of Internet usage (WITSA, 2000) and thus the potential growth of business-to-consumer trades.

CO-OPERATION IN AN INTERNATIONAL SETTING

The coordination of national law enforcement procedures is considered an important prevention strategy due to the openness and borderless nature of the Internet. Even if it is a necessary step, the co-operation within the EU and between individual EU countries and the US is far from being sufficient to combat the cyber-

criminality. Credit card frauds, for example, often find their perpetrators in countries in the former Soviet Union, Eastern Europe, and Asia (Richtel, 2002).

THIRD PARTY CONTENT AND ACTIVITY

The question of whether or not companies should be held accountable for the activity on their websites is debatable. It may be considered that once there is the possibility to control the content and the activity on a website, there should be some liability involved. This is the view taken in the United States with the, now unconstitutional, Communications Decency Act and the Digital Millennium Copyright Act (Crawford, 2002). These particular acts protect web business from liability for criminal activities that take place on their site. It is primarily aimed at ISPs but it is also applicable to other service providers, like e-market places, but only under certain conditions.

BUSINESS CASE

E-BAY

E-Bay attempted to monitor its site to prevent criminal activity and protect the interest of its customers. This resulted in an increased liability that had important legal consequences for the running of its day-to-day business. Legal costs soared in order to prepare for the claims that were likely to arise, in particular from the copyright holders like the software industry. The software industry is likely to consider that it is e-Bay's responsibility if illegal copies of software are sold during an auction on e-Bay's website (Crawford, 2002).

It is difficult to strike a balance between consumer protection, the growth of e-economy, and the rights of copyright holders. Until now, the software industry associations have been very active lobbyists. Their point of view is understandable in that the Business Software Alliance (BSA) estimates that, due to piracy, the software industry suffered a loss of profit of about 5.09 billion EURO in 2001 for Western Europe, Eastern Europe, US and Canada together (Business Software Alliance [BSA], 2002, p.5). On the other side, there is an increasing fear that, more laws that are limiting could prevent the growth of the e-economy by putting unreasonable liabilities on Internet Service Providers and by trying to excessively regulate the Internet.

MISLEADING OR ERRONEOUS INFORMATION

The question can be asked whether news providers should be liable for damages caused by false or erroneous information that they provide. Although it may not be possible to constantly check all the content of the web pages they store, e-newspapers should at least put in place some preventive measures that try to detect any unauthorized change of content on their website.

BUSINESS CASE

NEWSPAPERS

Semantic hacks aim at perverting trusted sources, like an article on the website of a newspaper, by manipulating information in ways not immediately obvious to readers (Salkever, 2001, October 10). There is a case, for example, where some false press release caused Lucent Technologies shares to fall 4% in March 2001.

This business case shows why newspapers also must understand their responsibility to secure their information servers and run regular checks for unauthorized changes in content. The consequences of semantic hacks can be diverse and difficult to estimate. A known fact though, is that stock markets are very sensitive to certain types of information.

SOFTWARE SECURITY FAULTS AND PROMPT SECURITY PATCHES

Gartner analysts estimate that, in 2005, 90% of the attacks resulting in material loss for a company will exploit known security flaws for which a software patch is already available. One of the reasons for this is the lengthy testing procedures required in their computing environment (Surmacz, 2002). In addition, software companies leave it to the users to constantly track known and unknown security flaws and to fix them before hackers exploit them (Banisar, 2001). This demonstrates how some software companies that release software with known security flaws put the extra financial burden and additional risks on their customers.

For years, security specialists have been recommending stricter liability for those companies that produce insecure software, as they place business and consumers at risk. Often the comparison is made with the automobile industry where imposing liability and setting minimum-security standards greatly improved automobile safety (Banisar 2001). An increasing number of independent bodies, like the National Academy of Sciences, have also started to support the idea (Rodger, 2002).

While a software producer cannot realistically write software without any flaws, there is a minimum set of standards that should be applied. Most importantly, security should be integrated into all levels of the design and production of software (Levy, 2001). Known security flaws should be patched before the release, as there is no reason to put the extra financial burden and risk on the customers without their consent. Finally, there should be some maximum allowable time lapse imposed between the discovery of a flaw and the release of its patch. When a hacker discovers a security flaw, it only takes days for their exploits to be spread through the underground community of hackers. On the other hand, users may have to wait for several months between the moment a critical issue is raised and the moment the patch is released (Mullen, 2002).

3.2 Information campaigns

It is recognized that the anonymity conferred by the Internet, combined with the lack of perceived consequences for inappropriate behavior, implies that too often users will show a conduct online that will be different from the one adopted in normal life (ITAC, 2000). Because of this fact, several strategies should be undertaken to assist in the battle against cyber-crime. Educational programs on cyber ethics should be taught at every level of the society such as at schools, home, as well as the business and governmental environments. It is hoped that cyber ethics programs will at least help reduce the amount of offences like web defacement (where website contents are modified in an obvious manner), which is the equivalent of vandalism.

Ethics campaigns will not change the fact that there will always be criminals to commit computer assaults. Therefore, efforts must be made by all persons to protect the Internet more effectively. Security awareness campaigns are a first step in that direction. The lack of security awareness is definitely an aspect that appears to be the cause of security weaknesses in large companies. There is often expensive security equipment like firewalls; yet, they cannot make up for the bad utilization of the network by employees who inadvertently open backdoors. Deficient security awareness also explains part of the lack of consumer trust, in that the consumer does not know how to create a secure environment when connected to the Internet and are then reluctant to use it. Finally, increased security awareness should reduce financial losses incurred through security breaches and increase business-to-consumer trade due to enhanced consumer confidence. Considering everyone would benefit from a more secure business environment; governments as well as businesses should participate in this informational campaign effort.

3.3 Self-regulations/ Market regulations:

Some of the prevention strategies presented here should not really be called strategies because they are, in fact, the result of market forces at work. Strategies emerge when government and industry consider it useful to create a framework that facilitates or controls these new trends.

Pressure from Strong Partners

As it often happens in the market, when a strong player sees a financial interest in applying a new technology it tends to force its smaller partners, suppliers, and customers alike, to adopt it as well. For example, in May 2001 Visa required its online merchants to follow its 12 security commandments and ABN Amro requested YellowPages.com to implement an intrusion detection system into their network as a condition to continue doing business (Salkever, 2001, December 4). Although this behavior means the adoption of security standards will take place at an accelerated pace, it also usually leads to higher financial pressure on smaller partners.

PRESSURE FROM SECURITY COMPANIES AND CONSUMERS

Responsible computer security professionals do not disclose security flaws that they discover before the concerned vendor has released a patch for it. Nevertheless, many security professionals feel frustrated by the length of time the vendors take to release patches and want to start using Vendor Notification Alerts (VNA). Vendor notification alerts will disclose, on a website, the list of vendors and products at fault as well as the protection methods. Of course, there should not be enough information for hackers to exploit the flaw (Mullen, 2002). The hope is that if customers could see how long they have to wait for the release of patches they are likely to put pressure on the vendors.

E-BUSINESS INSURANCE

The e-business insurance can cover most computer related crimes such as virus attacks, unauthorized access to a company's system and even cyber-extortion. The e-business insurance market was worth 100 million USD in 2001. It is expected to grow to 1 billion USD by 2007 (Salkever, 2002, April 2). Considering all companies doing business online are exposed to some degree to computer related crimes, it is expected that most of them will feel the need to invest in e-business insurance. This in turn means that Insurance companies are likely to dictate what security practices or products would be acceptable by the simple fact of lowering their insurance premiums for those companies that adopt secure procedures and products. This is also likely to improve security awareness within companies. Finally, it would probably also exert some financial pressure on software producers that do not release secure software by demanding responsibility for flaws in their products.

3.4 TECHNOLOGICAL MEASURES

IDENTIFICATION AND AUTHENTICATION TECHNOLOGY

It has become obvious that online payments with a credit card that only require one to provide a card number and expiry date are not sufficiently secure, and it makes databases that store such information an attractive target. Some technological measures could solve this problem. One example is the use of smart cards. Smart cards are similar to the usual credit card but contain a microprocessor chip and memory to store electronic data. Using a smart card in combination with a PIN number will encrypt the transaction data with the private key of the cardholder. The encrypted data stored on the merchant's database would be of no use to thieves if they do not have the private key codes of the cardholders. Although smart cards have their own security flaws (Markoff, 2002), the scale of fraud using smart cards will never be the same since the fraudster first needs to physically gain possession of the cards before he can steal information like the private key code.

One problem with the use of smart cards is that the readers are not cheap and it is not sure that customers will want to bear the full cost of it. In addition, customers should not be the only ones to bear the cost for the use of smart cards. Indeed, the generalized use of smart cards would increase overall B2C trades by boosting customer confidence in online payments and limiting the cost of fraud to credit card companies and merchants alike.

ENCRYPTION

Some governments may want to create a controlled digital key registry with all the digital keys for encryption software sold in its country. Those keys would enable law-enforcement officials to decode suspect data. This approach is considered completely inefficient since criminals will still be able to use dozens of encryption software programs, not controlled by governments, which are freely available on the Internet (Salkever, 2001, October 2). In general, it is considered that government restriction on the import, export, and domestic use of encryption technology hinders security when doing business on the Internet (GBDe, 2000).

3.5 OTHER MEASURES:

People have been thinking of other types of preventive measures, for instance some suggest adopting a standard email address to report security flaws (Poulsen, 2002). For example, for the site CNN.com, this address could be security@cnn.com. The idea is that while it may only take a few minutes to discover a security breach in a website, it can take weeks to pass the information to the right people within the company, simply because people do not know where to report the information. This type of measure requires little investment and would significantly improve security.

3.6 SUGGESTIONS AND GUIDELINES

Computer related crime prevention strategies are a necessary condition to the continued growth of the e-economy, both in the business-to-business and in the business-to-consumer sectors. These strategies will only be efficient if they are used in a coordinated manner. For example, it is not enough for a company to invest in security technology if its employees do not have any notion of security procedures. Furthermore, security technology will not be adequate if legitimate security research is hindered by new legislative measures. All players in the e-economy have a part to play in implementing computer related crime prevention strategies.

THE ROLE OF THE GOVERNMENT

Legislative measures will have to be carefully balanced to best protect the interest of all the parties concerned and create a favorable environment for the growth of e-business. Legislative measures should extend the concept of responsibility regarding security, or the lack of it, to the domain of the information technology infrastructure (hardware, software, and networks). Keeping in mind that e-insurance will indirectly reinforce the security of the Internet and thus foster the growth of e-business; governments may want to put in place the framework for an extensive adoption of e-insurance by the companies that do e-business. That environment should also favor competition between insurance companies in order to keep the premiums at a fair level for the policyholders.

THE ROLE OF THE INDUSTRY

In a networked environment, security is the responsibility of each player. Short-term considerations have often relegated security issues to the bottom of the agenda. It is now time that companies see security as a necessary cost to conducting business and that they need to be protected against damaging computer assaults and costly lawsuits.

The time is favorable for this type of mental shift; shareholders are becoming increasingly unsatisfied with managements that do not strive for long-term steady growth. Enhanced security at all levels is an investment that can bring just that – better risk management and business growth.

CHAPTER 7

THE FUTURE OF PREVENTION STRATEGIES FOR COMPUTER RELATED CRIME

1.
EU/US PREVENTION PATHWAYS

A rule most people are familiar with is "the whole is greater then the sum of it's of parts." This rule is applicable to the realm of computer crime prevention as well. It is clear that no magic bullet exists and focusing on one aspect of prevention will not solve all the problems. The title "prevention pathways" is used to demonstrate that there are multiple ways that one can look at the prevention of computer related crime. Further, the use of the word "strategy," as pointed out in the e-commerce chapter denotes a plan of attack on behalf of a larger body either working alone or in co-operation with another entity. Casey Dunlevy of CERT®/CC spoke about US prevention strategies and he said that, in essence, no US strategy exists or could be identified. In fact, when one looks at the comparison tables that are in the following pages one will find a patchwork of both private and public organizations. For the most part, this has been enough to meet our needs and there exists, at some level, a bit of order and it is not completely lawless and filled with anarchy. Most users abide by "netiquette" and for those who respect work done by others give credit where credit is due. Obviously, crime is still a concern for both the citizen and the company who utilize the Internet but some groups have "stepped up to the plate" in attempt to make the Internet a safer place.

Given that the Internet is not bursting with lawlessness, we must ask ourselves what is our ultimate goal and then assess whether or not it is attainable given the current circumstances. As Unisys stated the time is ripe for a change in thinking about how we approach the prevention of cyber-crime. Can we protect both the emerging marketplace and an individual's privacy and still combat cyber-crime effectively? This is a difficult proposition, yet if we truly form partnerships between the public and private sectors and begin to encourage consumers to take an active part in protecting the online environment this goal may attainable. David Wall (2000) aptly points out that the Internet has many active players who have helped to regulate this environment and suggests that they will continue to do so. Utilizing his optimism regarding the "order and law" of the Internet the following tables provide concrete examples of those players and perhaps ways in which they can forge partnerships in order to make it a safer environment for all those concerned.

2

LEGISLATIVE MEASURES EU/US

Europe	United States of America
Directive 95/46/EC concerning the protection of individuals with regard to the processing of personal data and the free movement of such data Directive 97/66/EC concerning the processing of personal data and the protection of privacy in the telecommunications sector Recommendation 3/99 on the preservation of traffic data by Internet Service Providers for law enforcement purposes Council decision 2000/375/JHA to combat child pornography on the Internet Directive 99/93/EC on a Community framework for electronic signatures Council Recommendation 95/144/ EC on common information technology security evaluation criteria Proposal for a Council framework decision on attacks against Information Systems COM (2002) 173 Council Recommendation 2001/C 187/02 on contact points for high-tech crime Communication from the European Commission *Network and Information Security: Proposal for a European Policy Approach* (COM/2001/0298) Decision No 276/1999/EC adopting a Multi-annual Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks and COM 2002 152 its Follow-up *Council of Europe* European Convention on Cyber-crime (2001) 14 May 2002 DRAFT of the first Additional Protocol to the Convention on Cyber-crime concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems Recommendation (1989) 9 on computer related crime Recommendation (1995) 13 concerning problems of criminal procedural law connected with information technology	1st Amendment of the Constitution 4th Amendment of the Constitution 5th Amendment of the Constitution Privacy Protection Act 42 U.S.C. § 2000aa Electronic Communications Privacy Act 18 U.S.C. §§ 2701-2711 Gramm-Leach-Bliley Act Child Online Privacy Protection Act 1998 Communications Assistance for Law Enforcement Act (CALEA) 18 U.S.C. §§ 2510-2522) - Prohibits private wiretaps and requires telecom company co-operation with federal government wiretaps. Notice of Certain Electronic Surveillance 18 U.S.C. § 2232 - Makes it illegal to give notice of federal wiretaps Federal Wiretap Act 18 U.S.C. § 1343 Patriot Act of 2001 Computer Fraud and Abuse Act of 1986 plus amendments 18 U.S.C. § 1030 includes Information Infrastructure Protection Act Telecommunication Act of 1996 Credit Card Abuse Act 18 U.S.C. § 1029 Economic Espionage Act 1996 18 U.S.C. § 1831 et seq Digital Millennium and Copyright Act of 1998 No Electronic Theft Act 1997 - allow for federal prosecution of large scale and willful copyright infringements even if the perpetrator does not act for financial gain Child Protection Act of 1984 Child Protection and Sexual Predator Punishment Act 1998 Child Pornography Prevention Act of 1996 Identity Theft and Deterrence Act of 1998

COMMENTS

The previous table provides a basic starting point for legislative action in both the EU and the US. As previously discussed, the legal systems under analysis are quite different. In order to understand the previous table a brief explanation must be provided for those who are unfamiliar with legal-ese. Two European bodies active in this area are the European Union and the Council of Europe. Both of these are composed of the 15 Members States but the Council has many more members and has granted observer status to other countries such as the US, Canada and Japan. The European Union has three methods of trying to harmonize law among countries. The first are *regulations*, which are written at the community level and must be enacted at the state level. Second, directives must also be enacted at the state level; however, they outline legislative goals that need to be met. The state therefore can implement them into their codes in the way they see fit. If a state does not make sufficient effort to enact a directive, individual citizens can seek redress at the European level. Finally, there are *recommendations*, which are simply that, they do not require any action on behalf of the state.

In the US, there are federal and state laws. Some federal laws require states to change their own statutes while others are complimentary to the actual state law. For example, each state has its own computer crime laws through which it can prosecute offenders, but there are also federal laws that may apply. One example is the Computer Fraud and Abuse Act; this is applicable to any computer used to conduct government business. As previously discussed, this could apply to nearly any computer. Considering the interconnectedness of computers, in theory, nearly all federal statutes could be applicable.

The previous table highlights many of the statutes, recommendations, and directives that have been implemented in both the EU and the US. Other important international documents include the *International review of criminal policy-United Nations Manual on the prevention and control of computer related crime* (1999). In fact, this document thoroughly reviews the policies in place and provides suggestions for future strategies. The other important document is the *European Convention on Cyber-crime* (2001). These two documents attempt to outline a common understanding of the problem and possible legislative means to address it.

When one looks at the list of offences covered by the *European Cyber-crime Convention* the list is very similar to crimes prosecuted in the US, therefore legislatively there is some agreement on what is considered a computer related crime. Ideologically, however, difference exists particularly on issues related to free speech and privacy. These differences are likely to cause problems as use and understanding of information technology increases.

Privacy has been discussed at length in the previous section. Unisys put forth several suggestions in relation to legislative issues, primarily harmonization of laws regarding privacy and data retention. Criteria that should be considered include the amount of legal protection an individual should have against searches, seizures, surveillance, and interception of their communication. This area could be especially difficult because Europe is currently increasing its citizen's rights to privacy, while the US government is promoting greater use of surveillance. In light of the tragedy of September 11, 2001, it is not likely that the US government will change its position on this issue.

Free speech is another area where it is clear that there needs to be some level of harmonization or understanding between the EU and the US. Again, however, this may prove to be very difficult, as they lack agreement on the level of a free speech a citizen should have. Considering the fact that this is thought of as a basic right in the US, it would require a significant shift in thinking for the US to limit what is published on the Internet.

One of the main difficulties that will be encountered is the fact that the European Union does not have its own way of creating criminal procedural law. Each individual Member State has its own criminal law and all of the resolutions and recommendations that are passed are enacted differently between the states. This is particularly difficult when trying to harmonize thinking and procedure on a particular topic. Another difficulty encountered in the case of the US is the sheer number of laws that are passed, which creates loopholes and the need to generate more laws.

Finally, laws are largely dependant on public opinion and legislators are cognizant of this. For example, many laws are passed regarding child pornography and, for the most part, the EU and the US agree on the definition of child pornography and what should be prosecuted. Nevertheless, in other areas it appears that laws are passed without a complete understanding of the problem. This is obviously not the fault of any particular group; it is simply the nature of the issue. Therefore, those laws that are passed regarding companies and technological issues, for example, may need to be changed because the truth of the matter is we simply do not know the scope of the problem, as companies do not report when they are victimized.

In sum, legislators or their advisors need to have a complete understanding of the problem and should be in agreement on the *approach* to computer crime. We are in the beginning stages of this process and this concept needs to continue to be at the forefront of our thinking. A common approach will ensure agreement on what crimes need to be punished and how; this will then allow for greater harmonization. Laws need to be created without loopholes and should be flexible enough to account for technological advancement but not threaten the basic human rights of the citizenry. Privacy rights of the citizen should always be taken into consideration and weighed against what needs to be accomplished to establish appropriate exchange of information between those parties with a legitimate interest (e.g. law enforcement agencies). The most important thing about legislation is how laws are used in practice, regardless of the number of laws on the books. One cannot simply pass laws without follow-through or support in place to enact them.

The pathway for this particular area should be littered with signs reminding legislators that laws provide the most deterrence when they are clear and swiftly punished. Neither of these actions appear to be taking center stage in this particular arena. The second sign one must come across is “laws require enforcers.” Who will those enforcers be and where will the resources come from? It is common knowledge that local police forces are under-funded and overworked; can we expect them to accept this role? Is it fair to the citizens of either world? The contention of this author is no. If we want to “police” the Internet, they need to have a separate funding stream that does not jeopardize the safety and security of the physical world.

3.

SELF-REGULATION AND COMPLIANCE EU/US

Europe	United States of America
Each EU Member State has its own Internet Service Provider Association EuroISPA – a pan-European association currently focused on privacy issues Eicar – professionals in the field who create taskforces to handle current issues, most recently worked on the cyber-crime convention	BBB Online Privacy Programs Children's Advertising Review Unit –Advertising standards on the Internet for children Association Computer Machinery Code of Ethics – basic ethic manual for those who work in the technology industry Banking Industry "know your customer" guidelines (International applicability) E-business insurance

COMMENTS

Self-regulation and compliance are the first line of defense against computer crime. Legislation is slow to be enacted and sometimes even slower to be enforced. The previous table gives examples of self-regulative policies that are currently in place. These are the best examples of this type of strategy and can serve as an illustration to others who may be creating this type of policy.

Self-regulation policies should be created in the same manner as legislation – with a comprehensive understanding of the problem, keeping in mind the dynamic nature of computer crime. The importance of these policies cannot be emphasized enough as they can be written in a culturally sensitive way and with a greater understanding of what will work the best for a particular organization or region. This, in theory, should stop many computer crimes before they are committed. Above all, this is likely to be true in the area of computer crimes committed against businesses. If self-regulation also contains compliance aspects sufficient enough to provide deterrence it is even better as the criminal justice system is removed completely.

One such example of self-regulation could be found in the field of psychology. This field has gone through many of the same issues currently facing the technology sector. It is a recent example of an emerging field that has essentially had to define itself. The American Psychological Association provides an ethics manual that one must adhere to in order to have their own practice. Furthermore, this ethics code has been adopted into many state laws or licensing boards. One can be sanctioned and stripped of ones license for violating this code; in general, those who do the monitoring are the patients and other professionals. This type of system could work if consumers become educated and aware of security practices, privacy invasions, and other potentially hazardous practices. Consumers must then be given a method to resolve these issues – for example, by reporting to an independent monitoring board. If this were to occur within the technology sector, it is likely that companies

would take more responsibility, would not survive economically, or would be removed from the association.

Unisys highlights the importance of e-business insurance as a way of increasing security practices. Two things that can make e-commerce and the Internet a safer place are market forces and educated consumers. Unfortunately, neither of these things exists in significant quantities to prevent most of the computer crime currently perpetrated. Instituting or requiring e-insurance is a way to encourage better safety practices. There are of course problems with this solution, in that it goes against the spirit of the Internet as a free place to access and exchange information. In addition, more power is transferred to insurance companies who then perform the monitoring and standard setting.

Many people, particularly Michel Hoffmann of Unisys (presenter at the Pittsburgh conference), suggested the implementation of a chain of liability starting with software companies. This is likened to the transition that took place within the automotive industry. Until those companies were forced, through regulations, to build safer cars they continued to cut corners and make unsafe vehicles. Unfortunately, we are still in the time of producing and racing to the market. One way of forcing software companies to make secure products that have been tested is by hitting them in the pocketbook with threats of lawsuits or severe liability sanctions.

In sum, there are four basic criteria that need to be considered when creating self-regulative and compliance policies. First, there needs to be a comprehensive understanding of the problem. Second, the policies should be written and communicated in a culturally sensitive way in order to get the best response. Third, the consumer needs to be educated and given appropriate tools to help regulate the quality of the Internet. Finally, market forces need to be harnessed to foster basic security practices. If a company is forced to compete with other companies who can offer a more secure and less risky experience to the consumer then security practices would increase in order to attract new customers and keep existing ones.

4.

INFORMATIVE AND INSTRUCTIVE MEASURES EU/US

Europe[25]	United States of America
e-Europe initiative EPCP-Internet Education about Prevention of Child Pornography and the Internet RED – Red Barnet Hotline- Danish hotline against illegal content on the Internet CISA – Consumer Internet Safety Awareness .SAFE – Safety Awareness for E-learning EDUCANET- Education program for a critical approach of the risks linked to the use of the Internet FRIENDLY INTERNET – How to achieve a larger and safer internet by promoting the roles of parents, teachers, and social assistants INFONET- Information on Safer Internet to Italian and Spanish Speakers ONCE – Online Networked Children's Education SIFKaL –Safer Internet for Knowing and Living SUI – Awareness of safer use of the Internet SUSI- Safer use of Services on the Internet	kNOw Fraud™ Cyber Angels EPIC – Report on consumer privacy issues US Department of Education – *Parents Guide to the Internet* Internet Safety Watch CERT –Computer Emergency Response Team SANS Simon Wiesenthal CAIC – Computer Incident Advisory Center NIPC – National Infrastructure Protection Center NSI – National Security Institute Cybersnitch- one stop reporting for computer crime

COMMENTS

Information is power. The more informed a person is, the better their decision-making abilities. Current technology allows people to communicate with others on a global scale and the Internet culture should be encouraged to grow and develop in a respectful way. Respectful, in that people do not see the Internet as a place full of criminal prospects but rather as a tool to educate oneself and expand one's opportunities. In addition, the Internet should be a place each user feels the desire to protect. One does not go into a library and feel threatened; people understand how one should behave in this context, and they generally respect the rules. This also holds true for most other public areas. Obviously not everyone follows the rules and society continues to struggle with those who persist in "rule-breaking"

[25] For a complete description of these programs please visit the website www.saferinternet.org

behavior. Crime will never be completely eradicated for a variety of reasons, thus the best we can do is attempt to minimize the amount and the impact of crime.

Informative and instructive measures in both the EU and the US are quite similar in that both are trying to encourage parents and other people in positions of authority to take an active part in the "online life" of younger generations. This is particularly important given that this is one way in which young people can learn about the Internet without having to be logged on and learning from mistakes. They also utilize a variety of ways to try to reach the public both online and offline. These actions need to continue and be expanded upon by all interested parties. No one party should be in control of the Internet or of educating the users regarding its use. Information and education must remain in the hands of the population at large. The younger generations need to be taught to question the veracity of the information they receive in order to ascertain whether its reporting has been influenced in some way. Information is power and those who control the information are in the most powerful position of all.

The demography of Internet users is currently in flux and the knowledge level of users varies substantially. Informative and instructive measures must consider this aspect. These strategies must have an offline component for beginners and be geared to every age group. At a minimum, these measures should discuss responsible use of the Internet, behavioral ethics, and expectations in chat rooms, when one is gathering, using, or disseminating information, hacking (e.g. ethical hacking, hacking vs. cracking) and finally threats of the Internet and how to protect oneself.

Internet and computer education should be integrated as a basic course for every child. In addition, parents need to be encouraged to learn and participate as well. The landscape of the Internet will be vastly different in five to ten years; children who have grown up utilizing this technology will become a larger segment of the population of Internet users. For this reason, it is crucial to educate the young users and those that are just starting out in an offline environment. Technology is a powerful tool and should be approached with respect, curiosity and a basic understanding of its potential and its limitations. Finally, this information should be easily accessible to all users regardless of age, race, sex, socio-economic status, or knowledge level.

5.
OTHER MEASURES EU/US

Europe	United States of America
Hotlines for Illegal Content ChildFocus Net-Alert – Belgian Civil Hotline on Child Pornography Belgian Citizen Digital Reporting Site FACE-IT – Fight against child exploitation on the Internet INHOPE – Internet Hotline providers in Europe Association RED – Red Barnet Hotline Securenet- Spanish Active Hotline EU Forum on Cyber-crime Website EU Working Party on Data Protection COMCRIME Study and its Follow-up examined a number of legal aspects related to computer crime. Examined ways of improving co-operation between interested parties in the industry and law enforcement. *Study On Legal Issues Relevant To Combating Criminal Activity Perpetrated Through the Electronic Communication*	*Tip Lines/Hotlines* National Center for Missing and Exploited Children Customs Cybersmuggling Center (3C's) Internet Fraud Complaint Center (IFCC) National White Collar Crime Center *Task Forces* Innocent Images National Initiative Internet Crimes against Children (ICAC) FBI's National Computer Crime Squad National Infrastructure Protection Center and InfraGard CERT/CC at Carnegie Mellon Securities and Exchange Commission "Cyberforce" Surf Days (International) Federal Trade Commission – Warning website to educate consumers regarding fraudulent home based business opportunities.

COMMENTS

Other measures in place in the EU and the US include such things as hotlines, taskforces, and institutional actions. The EU and the US are similar when looking at this category. In fact, there are regional working parties that focus on information technology and crime in the EU and the US as well as many other countries. These working parties work on specific issues relevant to their region, and make suggestions and implement practices that will help combat computer crime.

This particular category should be one that fills in the "gaps" the others leave behind. This category should serve as a breeding ground for innovation and should allow for a thorough understanding of computer crime. The fact that this category is currently filled with task forces and working parties demonstrates that we are still learning how best to handle this type of criminal activity.

The largest gaps now exist in the capabilities of law enforcement agencies. These agencies should seek to create police squads who are capable in the field of computer crime and who do not have to compete with the “physical forces” for resources. This requires funding, training, and the latest computer technology. These police squads could then be used to teach other police officers the basics of computer crime. If our law enforcement agencies are ten years behind the criminals as far technology is concerned, the chances of being successful in this battle are very low.

Finally, taskforces should continue to be created from every part of the population. The only way to effectively understand and combat computer crime is to have the participation and support of those people in the fields of technology, businesses, as well as other professionals including academicians, citizens, and the government. A complex problem requires a multifaceted approach consisting of many strategies and players.

6.

BEGINNINGS

To think what has been written is conclusive is to miss the dynamic nature of this field. This has been a work in progress for over one year. In the original interim report, it was written that gambling on the Internet would never be outlawed. Greece actually chose to outlaw all gaming recently, thus we were required to go back and change this sentence. Therefore, the author chose to use the word "beginnings" as opposed to conclusions. This compilation of information provides one with a feast for thought and lends itself to many new lines of research. In light of current events, research on critical infrastructure protection is greatly needed. How can the government effectively collaborate with the private sector when the private sector wants to have very little to do with the government? How can educators encourage the safe use of the Internet at all levels for all people? How can we learn how organized crime groups are utilizing technology – are they learning it themselves or do they employ hackers? How can we stop that recruitment from taking place, if it in fact exists? The questions are limited only by ones imagination. Thus the conclusion of it all is – it is extremely difficult to produce a "definitive" work, as tomorrow it changes. In light of this, we have attempted to provide a dynamic work that can be added to and used as technology progresses. Researchers, professionals or other persons with an interest are encouraged to add and expand on the information presented. One must be continually cognizant of the nature of this field, knowing that what is written today may or may not be applicable tomorrow.

ANNEX I

COMPUTER-FACILITATED CRIME CASES

VIOLATION OF PRIVACY

CASE 1 ALEXA INTERNET

(USA, 2001) As part of a settlement for a series of lawsuits, Alexa Internet, a subsidiary of Amazon.com, will pay up to $1.9 million to users whose personally identifiable information was found in the company's database. The case started with a Federal Trade Commission investigation into Amazon's privacy policies. Alexa Internet's practices of correlating personally identifiable information with anonymous user data were deceptive (Gray, 2001).

CASE 2 TOYSMART

(USA, 2000) Toysmart, one of the biggest American toy companies, offered to sell their customers' records, such as names, addresses, and credit card numbers, as part of its bankruptcy proceedings. The privacy policy published on the website had specifically stated, "personal information voluntarily submitted by visitors to our site, such as name, address, billing information and shopping preferences, is never shared with a third party" (Greenberg, 2000).

CASE 3 DOCUSEARCH.COM

(USA, 2000) The parents of Amy Boyer, a 20-year-old woman slain by an Internet stalker, filed a suit against the company that provided the killer with her personal information. Before the attack, Liam Youens, the cyber-stalker, tried to find out Boyer's birth date from docusearch.com, but when he could not find that information, he requested her social security number. This information cost him $45. Youens later requested another search for $109 to find out where Boyer worked (Noack, 2000).

CASE 4 DOUBLE-CLICK COOKIES

(USA 2001) Double-Click was sued for violating several acts because it accessed cookies on the viewers' hard drives without their consent and authorization. The particular cookies collected information that Web users consider personal and private (email addresses, home and business addresses, telephone numbers) as well other information users would not ordinarily expect advertisers to collect. Double-Click contended the websites it served were "users" of the Internet and that all of the web users information accessed by Double-Click's cookies were "of or intended for" these websites. The court sided with Double-Click considering the affiliated websites gave Double-Click permission to access the information passing between the websites and its users (Galil, 2001).

IDENTITY THEFT

CASE 1 LAMAR CHRISTIAN

(USA, 2000) Lamar Christian, age 32, was sentenced for conspiracy to commit bank fraud. Federal prosecutors say Christian created 331 fake credit accounts and used them to buy computers and jewelry online. The cards were produced using the names of the nation's highest-ranking officers. Christian claimed to have received the names and social security numbers from a website run by Glen Roberts, a privacy advocate. Roberts said he acquired the information from the Congressional Record, which publishes the social security numbers and names of high-ranking officers when they are promoted ("Man Admits," 2000).

CASE 2 THOMAS SEITZ

(USA, 2000) A 23-year-old man from New Jersey, Thomas Seitz, was arrested after he tried to buy a car using a fake driver's license. He acquired a car loan by using the name, address, and Social Security number of an individual with a file on the public website for the Securities and Exchange Commission. After the arrest, he declared that, "anyone with some computer skill could produce high quality fake documents" (Worden, 2000).

CASE 3 VERIZON WIRELESS

(USA, 2001) Stolen data from the Verizonwireless.com website appeared in several chat rooms for over a week. The exact number of published records is unknown but it was estimated that new records were showing up by a rate of two per minute at one point. The data consisted of driver's license numbers and Social Security numbers, which is the type of information Verizon requires for a credit check needed to purchase a cell phone plan (Sullivan, 2001).

HATE CRIMES

CASE 1 NAZI MEMORABILIA

(*LICRA et UEJF vs Yahoo! Inc and Yahoo France*, 2000). A French student group, UEJF, requested a French Court find Yahoo advertisements, of the sale of Nazi memorabilia, to be in violation of the French Penal Code. They contended it "encouraged the propagation of anti- Semitism and constituted an offence against the collective memory of a country profoundly wounded by the atrocities committed by and in the name of Nazi criminal enterprise" (as quoted in Penfold, 2001). Yahoo France was ordered to post warnings that clients must terminate their connection if it resulted in a breach of French Law. The decision against Yahoo! Inc (US) stated it was technologically possible to filter information that is being disseminated to a given country via the Internet therefore Yahoo Inc (US) must:

…take all necessary measures to dissuade and make impossible any access via Yahoo.com to auction service for Nazi merchandise as well as to any other site or

service that may be construed as an apology for Nazism or contesting the reality of Nazi crimes" (Penfold, 2001).

CASE 2 KINGMAN QUON

(USA, 1999) Kingman Quon, a college student, plead guilty to US Federal civil rights charges in February 1999 after sending hateful email messages to Hispanic professors, students and employees across the United States. These racially derogatory messages contained statements such as that he (Quon) would "come down and kill" them and that they were too "stupid" to get a job or be accepted to Universities without affirmative action policies (Combating Extremism in Cyberspace, 2000).

CASE 3 ALEX CURTIS

(USA) Alex Curtis who calls himself the "Lone Wolf" began disseminating racist propaganda when he was a teenager. He vandalized buildings with racial slurs, swastikas, wrote letters to newspapers and parents, and committed "small-time terrorist acts." He was arrested twice and after the second arrest, he changed his modus operandi to the Internet where he could reach more people. He created an email list and his Nationalist Observer website, hosted by *Stormfront,* an Internet service provider. Alex Curtis claims to reach "100's - 1000's of the most radical racists in the world each week" (Anti-defamation League, 2000).

DEFAMATION

CASE 1 DEMON INTERNET LTD

(London, 1997) Demon Internet Ltd, an Internet service provider, offered a Usenet facility enabling authors to publish material to readers worldwide. Authors submitted articles, or postings, to the Usenet news server through their local service provider who then disseminated the postings via the Internet. Such postings could then be placed in a newsgroup dealing with a certain subject. Ultimately, the postings were distributed and stored on the news servers of all the service providers that offered Usenet facilities. Demon Internet Ltd carried a particular newsgroup that stored postings for approximately two weeks. On January 13, 1997, an unknown person made a posting to that newsgroup on an American service provider and it reached Demon Internet Ltd's server in England. The false and defamatory posting was allegedly written by and in reference to the same person, Godfrey. On January 17, Godfrey informed Demon Internet Ltd that the posting was a forgery and asked the company to remove it from its Usenet news server. The posting was not removed and it remained available on the server until its expiration date of January 27 (Akdeniz, 1999).

CASE 2 DAVID TRIMBLE

(London, 1999) Northern Ireland's First Minister David Trimble sued the website Amazon UK, for selling a libelous book which alleges his involvement in sectarian crimes. The book entitled *The committee: political assassination in Northern*

Ireland, by Sean Mcphilemy was not for sale in UK bookshops; it could only be purchased from Amazon's online shop (Sprenger, 1999).

BLACKMAIL

CASE 1 COLORADO PHD CANDIDATE

(USA, 2000) The FBI arrested and charged Nelson Robert Holcomb, PhD candidate at Colorado State University, with extortion in a plot against Audible Inc., a firm selling downloadable spoken-audio content. Using an anonymous Hotmail account, Holcomb claimed he had discovered a free way to download Audible's content and threatened to alert the media about the vulnerability unless Audible met his requests. In exchange for his silence, Holcomb demanded cash equal to the value of the Audible site's content, a new Volvo station wagon, two diamond Rio digital audio players and unlimited free downloads of Audible content. Holcomb was found and later arrested by the FBI because he sent an email to Audible using his university account and not his anonymous Hotmail account (McWilliams, 2000).

CASE 2 RUSSIAN HACKER – MAXUS

(London, 2001) An eighteen-year-old Russian cracker who calls himself Maxus attempted to extort $100,000 from online music seller Cduniverse in exchange for information about a website security hole that enabled him to steal several hundred thousand customer records, including credit card numbers and expiration dates. According to Maxus, Cduniverse initially agreed to the ransom then failed to follow through. Due to their failure to pay, Maxus decided to set up a website entitled Maxus Credit Cards Datapipe containing more than 25,000 stolen credit card numbers. Maxus announced the existence of this site in an Internet relay chat room devoted to stolen credit cards (McWilliams, 2000).

CASE 3 BARCLAYS

(London, 2001) Graham Browne, a former encryption expert for Barclays, allegedly blackmailed his previous employer. This particular bank is the owner of Europe's largest credit card system. Browne is accused of asking £25 million to be paid to 14 named people at Barclays in order not to reveal some security system secrets (Gillard, 2001).

CASE 4 ELLE MCPHERSON

(USA, 1997) Two men were charged with attempting to extort money from the famous model Elle McPherson by threatening to post stolen photos and an "embarrassing secret" on the Internet. William Ryan Holt, age 26, was arraigned in Los Angeles on one count of sending a threatening letter. His alleged accomplice and mastermind of the scheme, 29-year-old Michael Robert Mishler was charged with two counts of burglary, three counts of sending a threatening letter, and three counts of attempted extortion. Holt and Mishler first sent a letter with a threatening message asking for $60,000 in exchange for not publishing, on the Internet, several "compromising" pictures (Errico, 1997).

FRAUD

CASE 1 RISK-FREE INVESTMENT

(USA, 2002) Six people were sentenced in Manhattan, New York for defrauding 172 people in a fake investment scheme that was marketed over the Internet. This investment program offered to "lease" $1 million from a European bank, which would be placed in a "high-yield investment program" that has returns of $5 million or more in a ten-month period. In order to receive the "leased" $1 million and have it invested for them the victims were required to make an up-front payment of $35,000 to the fraudsters. False "proof of funds" letters were printed from one of the defendants' home computer and mailed to the "investors" to further gain their trust. It was later discovered that the entire scheme was fictitious and none of the European banks existed. In a one-year period, two of the defendants received over $16 million in "leased" fees from the victims (US Department of Justice, 2002).

CASE 2 NIGERIAN 419 LETTER

(Charlottesville, 2002) A letter from Nigeria was emailed to a potential victim in Virginia using the September 11 terrorist attacks on the World Trade Center and the Pentagon to extort money. An excerpt from the original letter is as follows:

The foreign late engineer richard moore, an oil merchant/contractor with the fedral government of nigeria, who is based in new jersey with this telephone number:973 776-3900 fax number:973 776-3735, was confirmed to be among the victims of the terrorist attacks on the usa. Before the september 11,2001 terrorist attacks on the united states, he banked with us here at the orient bank plc and had a closing balance of us$10,000,000.00 (ten Million united states dollars) which the bank has put up for claim by The late engr. Richard moore's next of kin....

As with most Nigerian 419 scams it is likely that if someone responded they would be asked to deposit some amount of money in a foreign bank account or provide the fraudster with personal banking information in order to receive the money. There is usually an element of illegality involved, which prohibits the victim from immediately reporting the fraud to the appropriate authorities. The fraud continues until the person has no money left or refuses to give any more money to the perpetrators (419 Coalition, 2002).

CASE 3 PYRAMID SCHEME

(Minnesota, 1998) A website offered copies of a software program that formed the basis of a pyramid-marketing program. The software contains five names and address of people who the victim is to send $20, once the money has been sent the people who receive the money will send the person "access codes" that unlock the program for the person to delete the names and put their name at the top of the list. The promotional material for this site encourage the victims to perpetuate the scheme by copying the software on to a disk and giving them out or sending emails to people giving them the same information (FTC Press Release, 1998).

CASE 4 PAIRGAIN

(*United States v. Hoke*, 1999) Gary Hoke pled guilty to securities fraud in the PairGain case. A person claiming to be Stacey Lawson of Knoxville Tennessee said in a chat room that PairGain, a Californian telecommunications equipment company, was being sold to an Israeli company for $1.35 million. This particular message included a link to a Bloomberg News story covering the sale of this company. When interested investors clicked on the link, they were directed to a website that looked very similar to the legitimate Bloomberg news site. This site included links that would take people to the real Bloomberg site as well as to the false story of the PairGain purchase. Due to time differences on the east and west coast as well an Israeli holiday none of the facts presented could be verified. This hoax caused a buying spree, which resulted in PairGain stocks rising over 31%; once it was disclosed to be a hoax, the stock prices fell causing substantial monetary loss for thousands of people. Hoke had tried to falsify his identity by subscribing to a web page service provider with a false Hotmail account (Painter, 2001).

CASE 5 CREDIT CARD

(USA, 2000) Xpics, a California based company, utilized banner ads and unsolicited emails to entice people to try their network of adult websites which contained images that could be viewed "100% Free" according to the advertisements. Once people visited the site, they were asked to provide their credit card information to verify they were of legal age but were not told that their credit cards would be charged a monthly fee for access. In addition to the false advertisement of free images, Xpics made it nearly impossible for the victims to cancel this service by redirecting the person to different pages or blocking access to the cancellation page. When people attempted to phone or email, the voicemail box was full and the emails went unanswered. Some people who were successful in "canceling" this service continued to receive monthly charges for "upgraded services" from the company (Enos, 2000).

CASE 6 ONLINE AUCTION FRAUD– NON DELIVERY OF GOODS

(Los Angeles, 2001) Using fake identities, a man registered on eBay and offered fraudulent auction listings for a variety of products (golf clubs, beanie babies etc.). The checks received from the highest bidders were cashed and no goods were delivered to the "winners" (Bartlett, 2001).

CASE 8 WORK AT HOME

(USA, 1999) Four people were charged in criminal court for distributing 50 million emails that falsely advertised the chance to work from home if the victim would send them $35 as a start up fee. There was in fact no work at home opportunities available ("Internet Fraud," 2001).

CASE 9 OTHER FRAUD

(USA, 2000) A man was sentenced for his role in a fraudulent scheme to provide immigration assistance and documentation for aliens who were seeking citizenship in the United States. Websites, newspapers, recruiters, and word of mouth were all ways the fraudsters got their message to the victims. Some victims paid more than

$10,000 with a promise that they would receive certain immigration documents. Some documents never came, which was blamed on the government. Other documents that did arrive were counterfeit or false documents ("Internet Fraud," 2001).

CYBER-STALKING

CASE 1 BALLINGALL

(Australia, 2001) Brian Andrew Sutcliffe, age 37 from Melbourne, Australia, was charged with stalking Sara Ballingall who played a role for a Canadian TV series. Sutcliffe allegedly stalked this actress with various types of communication (emails, phone, mail) for 6 years. Sutcliffe asked her to sign a copy of an ABC book about her series and sent her a present of a toy koala in an attempt to have her sign it. The book arrived unsigned; Sutcliffe then contacted her mother, returned the book, and still did not receive a reply. After not receiving any response, he wrote to Ballingall and stated, "…there will be trouble if no action was taken…" (Cant, 2001).

CASE 2 LEXINGTON HERALD

(USA, 2000) After firing a freelance photographer accused of downloading pornography, a vice president at the Lexington Herald Leader newspaper started getting strange phone calls from men who said they had met her in chat rooms and wanted to meet her in person. Then came subscriptions to several magazines (*Playboy, Penthouse, Seventeen, Bride*) without having ordered any of them. At one point she received a phone call about her order to stock a lake full of fish, which she never placed. Colleagues received similar phone calls about chat room encounters. This activity was reported to the police; however, nothing could be done to stop the activity, as no serious threats to anyone's life were made (Radcliff, 2000).

CASE 3 NICKNAME – "SUPERHACKER"

(China 2001) Twenty three year old Ko Kam-fai was jailed for one year on cyber-stalking charges. He hacked into the email accounts of two women using a program he downloaded from the Internet and started to send obscene photographs and messages. Using the nickname "Superhacker," he left pornographic pictures and stories in their email box. In one message, he threatened to rape one of his victims and attached a picture of a woman engaged in sex (Cyberstalker, 2001).

PROSTITUTION

CASE 1 EGYPTIAN STUDENTS

(Egypt, 2001) Two Egyptian University students were sentenced to one year in prison for setting up a website that allegedly offered homosexual contacts for money (International Gay and Lesbian Human Rights Commission, 2001).

CASE 2 RUSSIA – SICILY PROSTITUTION RING

(Italy, 2000) Natalia Deposkaia organized an international prostitution service using emails. After recruiting new customers using Web-based advertising, Deposkaia would send an email with a detailed catalogue of the prostitutes, which matched the characteristics outlined by the customers. Deposkaia and her customers completed entire transaction via email. Once a final agreement between the Deposkaia and the customers was reached, a prostitute was "delivered" directly to the customer's house. In this particular case, the prostitute came from Russia and went to Sicily ("Scoperto giro," 2000).

CASE 3 CHAT ROOM – LURING

(Singapore, 2000) A pimp who preyed on impressionable teenage girls in Internet chat rooms in an attempt to lure them into prostitution had his one-year jail sentence tripled in a Singapore court. Tan Kian Peng, utilized chat rooms to befriend lonely girls and entice them into prostitution. Tan further admitted to living on the earnings of a 14-year-old girl. The court accused Tan of finding men to have sex with the 14 year old as well as convincing an 18-year-old to become a prostitute (Ecpat, 2000).

CHILD EXPLOITATION

CASE 1 CHAT ROOM VICTIM

(London, 2001) Peter Green, 33 years old, received a sentence of 5 years in prison by the Aylesbury Crown Court for sexually abusing a 13-year-old girl he met in an Internet chat room. Green disclosed that he spent weeks gaining trust of the victim in a series of chat room conversations and eventually emailed her. Ultimately, he talked to her on her mobile phone and arranged a face-to-face meeting (Johnson, 2000).

CASE 2 LOLITA FILES

(Russia, 2002) "Lolita" is the name commonly used for thousands of websites running legally on the Internet that feature nude photos of male and female children, ranging in age from as young as three years old to their mid-teens. "Lolita sites" claim their photos are not pornography, because their photos do not have sexual explicit content, but instead are art. The recruitment of the children is done

from poor Eastern European families, thus several girls working for the "Lolita sites" claim to be working voluntarily because they are able to earn enough money for their family. Many times the family receives money for the girls as well. The economic situations of particular countries assist the exploiters in finding new children; for example, a typical government worker in Russia is paid $20 a month while each girl who poses naked receives $200 (Grove & Zerega, 2002).

CASE 3 BARCELONA PORNOGRAPHY NETWORK

(Spain, 1997) Officials discovered a prostitution and pornography network in Barcelona, Spain after a couple had "rented out" their 10-year-old son to buyers for $200. The seized items included thousands of pornographic videos, pictures, Internet images, and diskettes, some of which were later displayed at a news conference in Barcelona. Those arrested in connection to the network included doctors, teachers, a local politician, as well as a former head of a child recreation center. The people connected to this network sexually abused approximately eighty-five children. Pornography distributed by this network has reached several countries including France, Mexico, and the United States. Officials arrested more than 800 suspects. This network had contacts with other foreign networks that exchange and sell pornography (Hughes, Sporcic, Mendelsohn, & Chirgwin, 1999).

CASE 4 ON-DUTY SECURITY GUARD

(Paris, 2000) Police arrested eight people for the exchange of pornographic pictures of children via the Internet. The suspects were between the ages of 15 to 50; the court released the minor aged 15 into his parents' custody "after a warning." The arrest of a security guard who allegedly traded pornographic photos in a chat room while on duty led police to this particular group of offenders (Ecpat, 2000).

CRIMES AGAINST PROPERTY

VIOLATION OF INTELLECTUAL PROPERTY

CASE 1 MORPHEUS

(WWW, 2002) Piracy, what was once the problem of the music industry, has now transitioned into the area of the film and video. A free software program called Morpheus, which was shutdown on March 6, 2002, allowed users to download from other Morpheus users any type of videos (from full-length films to TV series) that were available over the Internet. The selection of downloadable videos depended on who was connected to the Internet and running the software that links the computers at that time. The Internet catalogue increased rapidly with the growing number of Morpheus users and was able to compete with the officially retailed videos for visual and sound quality (Borland, 2002).

CASE 2 INTERNET AUCTIONS AND PIRACY

(USA, 2001) The Software and Information Industry Association (SIIA) filed separate lawsuits against two men, alleging they sold illegal copies of software products to

people who had bid for them on auction websites. Both men are accused of violating the US Copyright Act (Johnston, 2001).

CASE 3 DEEP-LINKING

SNC Havas Numerique v. SA Kelijob, (2000). A French court ruled on a "deep linking" case. An online employment site brought an action against Kelijob, an employment search engine alleging copyright infringement and unfair competition. The defendant had provided links to subordinate pages, bypassing the home page (also known as "deep linking") of the plaintiff's site without authorization. In granting the injunction, the court distinguished between surface linking (to the home page) in which there is an implied right due to the nature of the Internet, and "deep linking" which requires authorization.

CASE 4 PLAYBOY META TAG

(USA, 2002) The Ninth Circuit Court of appeal concluded that the ex-playmate Terri Welles is not guilty for infringement of copyright against her former employer Playboy. Terri Welles created a personal web page and inserted the word Playboy in the meta-tag (areas of text hidden from the viewer but available to browsers and search engines), violating copyright and trademark law. Playboy claimed the use of the meta-tag keyword was illegal because the website content was not related to the famous magazine and the surfers are led astray when they read the results of the search engine. The court affirmed she has a legitimate interest to use such references considering Playboy elected her "Playmate of the year" in 1981, and the description of this event in her biography was undeletable (Staglianò, 2002).

VIOLATION OF PATENT AND TRADEMARK

CASE 1 CHAMPAGNE CEREALES

Société cooperative agricole Champagne Céréales v. G.J (1998). A French court became the first to uphold the rights of an unregistered trademark owner against a domain name registrant. Champagne Céréales had been the plaintiff's company registered name for more than 70 years although it was not trademarked. The defendant, a competitor of the plaintiff, registered and began using the Internet domain names "champagne-cereale.com" and "champagnecereale.com." The court found the domain names created a likelihood of confusion and traded on the plaintiff's goodwill. The case exemplifies the willingness of foreign courts to adjudicate issues involving domain names in the global ".com" domain, and extends the basis for litigation to holders of longstanding common law trademark rights even without a prior registration.

CASE 2 "1 CLICK" TECHNOLOGY

(USA, 1999-2001) In 1999, Amazon.com and its biggest rival Barnesandnoble.com began filing violation of patent lawsuits against one another. Amazon.com first sued its competitor for the infringement of the patented "1-click" technology, which allows users to enter billing and shipping information then place future orders

without having to re-enter same information. The second lawsuit occurred in 2001 when Amazon.com asked for an injunction prohibiting Barnes and Noble from using its "express lane" checkout features because it infringes once again on the single action order method used by Amazon.com (Glasner, 2001).

CASE 3 CANDYLAND

(USA, 1996) Hasbro, the famous toy company, sued the International Entertainment Group for violation of patent in relation to the name "Candyland" which is a registered trademark. "Candyland" is the name of a popular children's board game that the International Entertainment Group gave to a sexually orientated Internet website (Spatt 1996).

CASE 4 SAINT TROPEZ

(France, 1998) The city of Saint Tropez owns the trademark rights to its name. A company registered the domain name "Saint-Tropez.com" which subsequently infringed upon the city's rights. The court ordered the defendant to relinquish the domain name and to pay $120,000 in damages to the plaintiff. In reaching its decision, the court held the facts that the ".com" top level domain although administered in the United States and the "Saint-Tropez.com" account was maintained on a US server were of no consequence, since the infringing activity was accessible in France and the plaintiff was damaged there ("Saint-Tropez", 1998).

TRAFFICKING OF DRUGS

CASE 1 MARIJUANA WEBSITE

(Padova, Italy 2001) The first Italian website which sells marijuana online is based in Amsterdam. The website offers not only advice on how to cultivate marijuana, but it also sells all the equipment necessary for its growth (e.g. lights to create the greenhouse and the seeds). There is a large catalogue of different quality seeds, which can be delivered directly to your house through the mail ("Vendere Semi," 2001).

CASE 2 ONLINE VIAGRA

(Kansas, 1999) Six doctors were identified who were not properly licensed to practice medicine in the state of Kansas and were providing prescriptions and medications without ever seeing the patients. In addition, there were several online pharmacies that were selling medication illegally. One of the companies sold Viagra to a sixteen-year-old boy who was truthful about his age in the online application ("Online Pharmacies," 1999).

TRAFFICKING OF ORGANS

CASE 1 KIDNEY ON EBAY

(Florida, 1999) A man offered "one fully functional human kidney" the bidding hit $5.7 million before eBay could remove the item from their website. The details were that the buyer would be responsible for all costs incurred during the transplant and subsequent hospitalization (Young, 1999).

CASE 2 INTERNATIONAL ORGAN TRAFFICKING

(Rome, 1998) Jim Cohan Farkas was arrested for international trafficking of organs involving several countries such as South Africa, China, Brazil, Mexico, Colombia and Philippine. Italian police located a website created by "Cohan and associates" to contact possible clients. Those in need of a transplant wrote to Cohan describing their situation and in exchange for US $10,000, received the needed organ. The arrangement included a flight to the state where the surgeon worked, admittance to the hospital, and aftercare. The organs available were kidneys, hearts, and pancreases, which mean some came from living donors. The police were convinced this was a prime example of trafficking in human organs and was related with the kidnappings of several children all over the world. The Italian police could not prosecute Cohan, as there was insufficient evidence. He is currently still in business, conducted primarily via the Internet (Finkel, 2001).

TRAFFICKING OF HUMANS

CASE 1 BRAZILIAN EMAILS

(Brazil, 2001) Police received a complaint about a widely circulated email directed towards Brazilian prostitutes in an attempt to get them to move to Spain ("Prostitutes hook up," 2001).

CASE 2 RAPE CAMP

(Cambodia, 1999) An American in Cambodia offered a website "Rape Camp" where he promoted "Asian sex slaves" who were to be used for bondage, discipline and humiliation. The extended service, for those who wished to purchase it, promised interactive transmission with "pay-per-view access" in which requests could be made and then the customer could watch it occur. The owner of the website, stated he used Vietnamese women as opposed to local women so that he would not offend the local residents with his business. In addition to the "Rape Camp," his site offered sex tours to men visiting Cambodia. He faced charges of human trafficking and sexual exploitation, however, it was arranged that he not be prosecuted in Cambodia and he was deported to the US (Hughes, 2000).

CASE 3 GERMAN LAWYERS

(Germany, 1997) Two lawyers were arrested on several charges, such as conspiracy to abuse, conspiracy, murder, and kidnapping. They offered to purchase a Czech girl between the ages of 12-14 for "extreme sex games" and stated that if she died they would dispose of the body for an additional fee. The Internet was utilized for initial contacts using nicknames such as "Sado-Hangman" and "Leather-Witch." (Hughes, Sporcic, Mendelsohn, & Chirgwin, 1999).

GAMBLING

CASE 1 JAY COHEN

United States v. Cohen, (2001) Cohen ran a bookmaking company based in Anitgua; the customers who utilized his services were required to open accounts and then betting could take place over the phone or through the Internet. The business would then provide a confirmation for the received bets. The courts convicted Cohen; he later lost his case on appeal because the court contended he had sufficient knowledge of the laws of New York to know his actions were in violation of the law (also see Goss, 2001).

CASE 2 CREDIT CARDS SUED

(California, 1999) A California resident sued several credit card companies including Visa and MasterCard, after losing $70,000 through Internet casinos. She accused the companies of profiting from illegal gambling activities on the Internet. Visa and MasterCard agreed to forgive the debt, and change some of their requirements for the gambling sites with which they do business (Raysmen & Brown, 2000).

MONEY LAUNDERING

CASE 1 MAZE LTD

Robert established and registered a company "Maze Ltd" in Country A to set up gambling services on the Internet. He did not apply for a regulatory license to operate this company within Country A. A legitimate Internet gaming company already existed with a similar name "Maize Ltd" in another country, which was not connected to *Robert*. *Robert* then opened a bank account for his business in Country B; this was an Internet account and provided extensive flexibility.

Robert then traveled to Country C and advertised his business via the Internet specifically to Country D where Internet gaming was very popular. Robert provided information and gambling services on the Internet to his clients as if he was linked to the legitimate company "Maize Ltd" (hiding the fact that he was actually bound to *Maze Ltd*). The banking information provided to the potential gamblers was that of

yet another account in Country E in which the victims ultimately transferred approximately US $3,500,000.

In his home Country F, using a laptop computer *Robert* attempted to transfer US $1,000,000 from the Internet account to another bank account in Country F where the bank froze his assets and reported the activity to the Financial Investigative Unit. The jurisdiction of the various crimes has not been decided, however Country D opened a criminal case and began investigations, as that is where the majority of the victims resided (Financial Investigation Unit, 1999).

CASE 2 GAME.COM

(Europe, 2001) A possible case of money laundering was reported utilizing a "virtual" casino.

The components of the activity:

Company 1 in Country A (owned by *Danny*) constructed a virtual casino that was housed on a server in the Caribbean. However, Internet gaming prohibitions existed in Country A. In order to access the gambling the customers had to download a relay application from an Internet Service Provider in Country A.

Danny then made an investment in Company 2, also in the Caribbean, which he used to purchase the domain name "game.com"

Ownership of "game.com" was transferred to Company 3 in the Far East.

Large amounts of money appeared at a bureau de change and at a shopping center in Country A, as well as in several companies, including Company 3 in the Far East and other companies in Country B, which neighbors Country A.

A person at the bureau de change was known for gaming violations and had possible connections to other illegal activities.

The company in Country B was being investigated for illegal exploits primarily connected to the gaming industry.

Possible events could be as follows:

The virtual casino and the bureau de change were used to launder the money from the illicit activity of Company 3. This is thought to be the case because the money in the accounts for the "virtual casino" was more than what could be possible for that enterprise and the amount of business that was conducted through the gambling operations. In fact, there were many funds supported by false invoices that were transferred to Company 1, the bureau de change as well as to its manager (Financial Action Task Force-XII [FATF-XII], 2001).

CASE 3 SPORTS TOUT SERVICE

An illegally established sports tout service (STC), which also operated as an Internet service provider, collected and distributed information regarding sporting events to its subscribers. The customers utilized this information when they placed bets on certain sporting events. This business was expanded to include two offshore

gambling companies located in the Caribbean where one could place bets via the Internet or a toll-free number.

The money from the illegal sports tout service was laundered by leasing the services of the STC and the Internet service provider for a certain amount. This method was used in conjunction with laundering the money through various bank accounts. The perpetrators will likely be charged with a variety of organized crime related offences including gambling, money laundering, and tax evasion (FATF-XII, 2001).

ANNEX II

COVER LETTER FOR QUESTIONNAIRES DISTRIBUTED IN THE USA

Shawna Gibson ("Gibson") is a PhD candidate at the University of Trento-Italy. She is currently the Manager of a project that is being funded by the European Commission entitled the "EU/US Co-operation for the Prevention of Computer Related Crime: A Transatlantic Agenda." Gibson is working with several European and American partners including Erasmus University (Netherlands), UNISYS (Belgium), CERT (University of Pittsburgh), Carnegie Mellon and the Mathew B. Ridgeway Center (University of Pittsburgh). The project has multiple aims and one of them is to define and identify the various preventative measures that have been implemented in this field in the both the EU and the United States. Gibson has been charged with collecting the information from the United States. This information will be utilized to write a report on what the EU and United States have in common as far as preventative strategies as well as address those things are different. Gibson's team would eventually like to provide interested parties future direction and things to consider when implementing preventative strategies. Gibson's contact information is provided at the bottom of the questionnaire.

The report will be produced for the European Commission at the end of October 2002. Gibson will acknowledge the professionals who provided their time and expertise on the topic. Gibson will also forward a copy of the document (in .pdf format) to those who participated. IF selected respondents would rather talk with Gibson, instead of typing the information, she is available for telephone interviews.

INSTRUCTIONS

If you have any underlying documents referring to following questions, it would be greatly appreciated if you included either the document or its reference. If necessary please note this within the answers you have provided.

Please complete this questionnaire to the best or your ability within this document if you wish and return to the email address indicated. If you do not know the answer please indicate "DK" next to that question. We thank you in advance for taking the time to complete this questionnaire.

Questions and completed questionnaires can be directed to CONTACT PERSON by email at

1.

QUESTIONNAIRE EU/US CO-OPERATION FOR THE PREVENTION OF COMPUTER RELATED CRIMES

1.1 Definition of computer related crimes

Three types of computer related crimes (CRC's) can be defined:

A. Computer-facilitated crime. Crimes committed with the use of the electronic highway, these types of crime are facilitated by the use of computers they exist in both the physical and the virtual world (e.g. child pornography, credit card-fraud);

B. Computer as target. Crimes related to the circulation of informatics-instruments, these types of crime exist through the use of computers (e.g. viruses, Trojans, hacking);

C. Infringement of intellectual properties.

The crimes that can be viewed as CRC's are the so-called crimes of Confidentiality, Integrity, Availability (C.I.A): These crimes have been outlined in the European Convention on Cyber-crime and have been defined as the following. (A copy of this convention can be found at http://conventions.coe.int/treaty/EN/projets/cybercrime27.htm

Illegal access- access to whole or any part of the computer system

Illegal interception - interception without right made by technical means on non-public transmission

Data interference - damaging, deletion, deterioration, alteration or suppression of computer data without right

System interference- Inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data

Misuse of devices- the production, sale, procurement for use, import, distribution, or otherwise making available a device (including computer program), computer password, access code, or similar data with the intent to commit any of the previous mentioned offences.

Computer related forgery

Computer related fraud

Offences related to child pornography

Offences related to infringements of intellectual property and related rights.

Preventive measures can be divided into five categories:

Legislative measures

Compliance/self-regulation

Information/instruction

Technical measures

Other measures

2.

CONTENT

2.1 Legislative measures

2.1.1 Legislative measures with respect to **computer-facilitated crime**

2.1.1.a **Repressive measures** (e.g. punishable by law)

Is computer related forgery punishable by law?

If yes, what are the severity and type of sanctions?

Is computer related fraud punishable by law?

If yes, what are the severity and type of sanctions?

Are offences related to child pornography punishable by law?

If yes, what are the severity and type of sanctions?

Are there any other offences in which the (mis)use of computers is reason to determine the prosecution or punishment?

If yes, what are the severity and type of sanctions?

2.1.1.b **Preventive measures** (e.g. criminal procedure, demands on internet providers, banks etc.)

Are there any provisions in the criminal procedural law with respect to the investigation of computer-facilitated crimes?

If yes, which?

Are there any provisions in law with respect to demands on Internet service providers to prevent computer-facilitated crimes?

If yes, which?

Are there any provisions in law with respect to other parties (e.g. banks) acting professionally on the Internet to prevent computer-facilitated crimes?

If yes, which?

Are there any provisions in law on consumer protection or product liability concerning electronic trade, electronic banking, use of the Internet etc.?

If yes, which?

Are there other provisions in law with respect to users of computers, Internet, electronic trade etc. to prevent computer-facilitated crimes?

If yes, which?

2.1.2 Legislative measures with respect to **computer as target crimes**

2.1.2.a **Repressive measures** (e.g. punishable by law)

Is illegal accessing of computers, computer networks, websites etc. punishable by law?

If yes, what are the severity and type of sanctions?

Is illegal interception of data punishable by law?

If yes, what are the severity and type of sanctions?

Is data interference punishable by law?

If yes, what are the severity and type of sanctions?

Is system interference punishable by law?

If yes, what are the severity and type of sanctions?

Is the misuse of devices punishable by law?

If yes, what are the severity and type of sanctions?

2.1.2.b **Preventive measures** (e.g. demands on internet providers, banks etc.)

Are there any provisions in the criminal procedural law with respect to the investigation of computer as target crimes?

If yes, which?

Are there any provisions in law with respect to demands on Internet service providers to prevent computer as target crimes?

If yes, which?

Are there any provisions in law with respect to other parties (e.g. banks) acting professionally on the Internet to prevent computer as target crimes?

If yes, which?

Are there any provisions on consumer protection or product liability concerning electronic trade, electronic banking, use of the Internet etc.?

If yes, which?

Are there other provisions in law with respect to users of computers, Internet, electronic trade etc. to prevent computer as target crimes?

If yes, which?

NB: The answers to the following questions concerning this category might be the same as the answers to questions concerning category 2.1.1.b. If so, please mention.

2.1.3 Legislative measures with respect to **infringement of intellectual properties**

2.1.3.a **Repressive measures** (e.g. punishable by law)

Are offences related to infringements of intellectual properties and related rights punishable by law (civil and/or criminal)?

If yes, what are the severity and type of sanctions?

2.1.3.b **Preventive measures** (e.g. demands on internet providers, internet stores etc.)

Are there any provisions in law with respect to demands on Internet providers to prevent infringement of intellectual properties? If yes, which?

Are there any provisions in civil law concerning the protection of intellectual properties and related rights?

If yes, are these provisions applicable to computers, Internet etc.?

If yes, which are these provisions?

Are there any provisions in law with respect to other parties acting professionally on the Internet to prevent infringement of intellectual properties?

If yes, which?

Are there any provisions in law to protect domain names?

If yes, which?

Are there other provisions in law with respect to users of computers, Internet, electronic trade etc. to prevent infringement of intellectual property?

If yes, which?

NB: The answers to the following questions concerning this category might be the same as the answers to questions concerning category 2.1.1.b and 2.1.2.b. If so, please mention.

2.1.4 Technological measures

Have any technological measures been required by law to prevent any of the above-mentioned computer related crimes?

If yes, which?

2.2 Compliance/ self-regulation

2.2.1 Compliance/ self-regulation with respect to **computer-facilitated crime**

2.2.1.a **Repressive measures** (e.g. disciplinary rules)

Are there any codes of conduct, charters etc. containing disciplinary rules for parties subject to computer-facilitated crimes and/or Internet service providers etc.?

If yes, which?

2.2.1.b **Preventive measures** (e.g. demands on internet providers, banks)

Are there any codes of conduct, charters etc. containing preventive rules for parties subject to (possible) computer-facilitated crimes and Internet providers etc.? If yes, which?

Is there an ISPA or a similar association for Internet service providers?

If yes, is participation mandatory?

Is there an opportunity to report computer-facilitated crimes to the competent authorities?

If yes, who does the reporting and to whom?

Is there a CERT (Computer Emergency Response Team) or a similar organization? If yes, is this organization governmental or privately run?

*2.2.*2 Compliance/ self-regulation with respect to **computer as target**

2.2.2.a **Repressive measures** (e.g. disciplinary rules)

Are there any codes of conduct, charters etc. containing disciplinary rules for parties subject to computer as target crimes and Internet providers etc? If yes, which?

2.2.2.b **Preventive measures** (e.g. demands on internet providers, banks)

Are there any codes of conduct, charters etc. containing preventive rules for parties subject to (possible) computer as target crimes and internet providers etc? If yes, which?

Is there an opportunity to report computer as target crimes to the competent authorities?

If yes, who does the reporting and to whom?

2.2.3 Compliance/ self-regulation with respect to **infringement of intellectual property**

2.2.3.a **Repressive measures** (e.g. disciplinary rules)

Are there any codes of conduct, charters etc. containing disciplinary rules for parties subject to infringement of intellectual properties and Internet providers etc?

If yes, which?

2.2.3.b **Preventive measures** (e.g. demands on internet providers, internet stores)

Are there any codes of conduct, charters etc. containing preventive rules for parties subject to (possible) infringement of intellectual property and internet providers etc?

If yes, which

Is there an opportunity to report infringement of intellectual property to the competent authorities?

If yes, who does the reporting and to whom?

2.2.4 **Technological measures**

Have technological measures been implemented to ensure compliance or as a self-regulatory agent?

If yes, which?

2.3 Information/ instruction

2.3.1 Information/ instruction with respect to **computer-facilitated crime**

Is there a hotline, information/ reporting station with respect to computer-facilitated crime?

If yes, which?

Are there computer-facilitated crime awareness activities? If yes, which?

Is there a 'task force' or other organization with an advising/recommending role?

If yes, which?

Are there private organizations aimed at investigating computer-facilitated crime (cybercops)?

If yes, which?

2.3.2 Information/ instruction with respect to **computer as target crimes**

Is there a hotline, information/ reporting station with respect to computer as target crimes?

If yes, which?

Are there computer as target awareness activities?

If yes, which?

Is there a 'task force' or other organization with an advising/recommending role?

If yes, which?

Are there private organizations aimed at investigating computer as target (cybercops*)?*

If yes, which?

NB: The answers to the questions concerning this category might be the same as the answers to questions concerning category 2.3.1. If so, please mention.

2.3.3 Information/ instruction with respect to **infringement of intellectual property**

Is there a hotline, information/ reporting station with respect to infringement of intellectual property ?

If yes, which?

Are there infringement of intellectual property awareness activities?

If yes, which?

Is there a 'task force' or other organization with an advising/recommending role?

If yes, which?

Are there private organizations aimed at investigating infringement of intellectual property (cybercops)?

If yes, which?

NB: The answers to the following questions concerning this category might be the same as the answers to questions concerning category 2.3.1 and 2.3.2. If so, please mention.

2.3.4 **Technological measures**

Have technological measures been suggested to provide information or instruction regarding computer related crimes? If yes, which?

2.4 Other initiatives

Is particular attention given to CRC's in the training of police officers?

If yes, what is done?

Is there any form of co-operation between Internet service providers and other parties subject to (possible) CRC's and legal authorities?

If yes, which?

Are there any existing treaties that facilitate the prevention of computer related crimes between your state and others (not the draft convention mentioned earlier)?

Does an Internet Content Rating Group exist? If so who are the primary participants?

Are there any 'watchdogs' with respect to CRC's (e.g. consumer-organizations, NGO's)?

Are there any other prevention programs?

2.5 Privacy matters

Please answer the following questions as it relates to each of the above categories.

Which role did privacy aspects play in the conception of CRC preventive strategies?

Which aspects of privacy are you aware of that have been taken into account in the creation of CRC preventive strategies?

When implementing CRC preventive strategies, did you encounter privacy issues*?*

If yes, what were the issues and how have you handled them?

2.6 Effectiveness

In your opinion, which of these strategies has been most useful in the prevention of computer related crimes (both computer-facilitated and computer as target) and why?

In your opinion, which of these strategies has made it more difficult to prevent computer related crimes and why?

In your opinion, which of these areas should be the primary focus for the development and implementation of future strategies?

In thanks for your participation, we would be happy to provide you with the final results once the report has been completed. Please include your mailing address if you would like to receive this report.

REFERENCES AND RESOURCES

REFERENCES[26]

419 Coalition News on Nigerian Scam/Nigerian Operations (2002). Retrieved from http://home.rica.net/alphae/419coal/news2002.htm

Aftab, P. (2000). *The parents guide to protecting your children in Cyberspace.* New York, NY: McGraw Hill.

Agreement on trade-related aspects of intellectual property rights (1994). *Annex 1C of the WTO Marrakesh Agreement* [Electronic Version]. Retrieved from http://www.wto.org/english/ tratop_e/trips_e/t_agm0_e.htm

Akdeniz, Y. (1999). Case Analysis: Laurence Godfrey v. Demon Internet Limited. *Journal of Civil Liberties, 4(2)*, 260-267.

Akdeniz, Y. (2000, December 13). Seminar for the media on the convention against transnational organized crime. *Cyber-Rights & Cyber-Liberties.* Retrieved from http://www.cyber-rights.org.

Anderson, K. (1994, May). International intrusions: Motives and patterns. Proceedings of the 1994 Bellcore/Bell South Security Symposium.

Anonymous (1998). *Maximum Security* (2nd ed.). Indianapolis, IA: Sams.

Anti-defamation League (2000). *Alex Curtis: 'Lone wolf' of hate prowls the Internet.* Retrieved from http://www.adl.org/curtis/default.htm

Anti-defamation League (2000). *Combating extremism in Cyberspace: The legal issue affecting Internet hate speech.* Retrieved from http://www.adl.org/ main_combating_hate.asp

Arnaldo, C. (Ed.). (2000). *Child Abuse on the Internet. Ending the Silence.* Paris: UNESCO Publishing/Berghan Books.

Arnold, T. (2000). Internet identity theft: "A tragedy for victims." *Software & Information Industry Association* Retrieved from http://www.siia.net/sharedcontent/divisions /ebus/id_theft.pdf

Arquilla, J. & Ronfedlt, D. (Eds.). (2001). *Networks and netwars: The future of terror, crime and militancy* [Electronic-version]. Santa Monica CA:RAND.

Arquilla, J. & Ronfeldt, D. (2000). *Swarming and the future of conflict*. Santa Monica: RAND. Retrieved from http://www.rand.org/publications /DB/DB311/

Article 29, Data Protection Working Party (1997, December 3). *Recommendation 3/97 on Anonymity on the Internet.* Retrieved from http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/index.htm

[26] All website were visited between January and June 2002.

Article 29, Data Protection Working Party (1999, September 7). *Recommendation 3/99 on preservation of traffic data by Internet Service Providers for law enforcement purposes.* Retrieved from http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wpdocs_99.htm

Article 29, Data Protection Working Party (2000, November 21). *Privacy on the Internet – An integrated approach to online data protection.* (Document no. 5063/00/EN/FINAL/WP37)

Article 29, Data Protection Working Party (2001, November 5). *Opinion 9/2001 on the Commission Communication on: Creating a safer information society by improving the security of information infrastructures and combating computer related crime*. (Document No. 5074/01/EN/finalWP51)

Ashworth, A. (1999). *Principles of Criminal Law* (3rd ed.). Oxford: Oxford University Press.

Association for Computing Machinery (1992, October 16). *ACM code of ethics and professional conduct.* Retrieved from http://www.acm.org /constitution/code.html

Banisar D. (2000, November*). Privacy & human rights 2000: An international survey of privacy laws and developments*. Electronic Privacy Information Center and Privacy International. Retrieved from http://www.privacyinternational.org/survey/index.html.

Banisar, D. (2001, December 18). Save the Net, Sue a Software Maker. *BusinessWeek online*. Retrieved from http://www.businessweek.com /technology/content/jan2002/tc20020129_6083.htm

Bartlett, M. (2001). LA court deal with college hack, online auction fraud. *Newsbytes: The Washington Post Company.* Retrieved from http://www.newsbytes.com/ news/01/168600.html

Beirens, L. (2002, May 21). *Overview of vital traffic data necessary for investigations for which the EWPITC asks the general retention by telecommunications operators and telecommunications access and service providers*. Expert Statement of European Working Party on Information Technology Crime (EWPITC) and Interpol.

Belgian Citizen's Digital Reporting Site Stop (n.d). Retrieved from http://www.ping.be/meldpunt-kinderporno/

Belgian Penal Code Article 380quinquies, § 2

Bennett, M. (2001, October 5). Secure your customers' online payments. *ZDNet (UK).* Retrieved from: http://techupdate.zdnet.com/techupdate /stories/main/0,14179,2815396-1,00.html

Bequai, A. (1997, December). Organized crime: Manipulating cyber-space. *Computer Audit Update,* 25-29.

Bequai, A. (2001, September). Organized crime goes cyber. *Computers and Security*, 475-478

Better Business Bureau (2000, October 4). *Press release: BBB finalizes code of online business practices providing crucial road map for e-commerce.* Retrieved from http://ww.bbbonline.com/about/press/2000/102400.asp

Black, H.C. (1979). *Black's Law Dictionary*. St. Paul, MN: West Publishing Co.

Borland, J. (2002 March 6). Morpheus shutdown puts rival in the spotlight. *Zdnet UK.* Retrieved from http://news.zdnet.co.uk/story/0,,t287-s2106035,00.html

Broder, J (2000). *Risk analysis and the security survey (2nd ed.).* Woburn, MA: Butterworth-Heinemann.

BSI (1990, December 17). Errichtung des BSI. [Establishment of BSI]. Germany: Bundesgesetzblatt, Teil 1, seite 2834. Retrieved from http://www.bsi.de/dasbsi/gesetz.htm

Business Software Alliance (2002, June). Seventh annual BSA global software piracy study. Retrieved from http://www.bsa.org

Cabot, A. & Kelly, J. (1998). Internet, casinos, and money laundering. *Journal of Money Laundering, 2,* 134-147.

California Penal Code §1524.2 (b) (c)

Cant, S. (2001, March 27). Speed up urged on cyber-law. *The Age*. Retrieved from http://www.theage.com.au/news/2001/03/27/FFXTJ95ARKC.html

CEI Computer Economics (2002, June). Internet B2B transactions by continent 2002 to 2006. Retrieved from http://www.computereconomics.com /article.cfm?id=598

Celentano, L., Thompson, M., Edwards, W., Kernan, A. Farmer, J. (2000). Computer crime: A joint report. *State of New Jersey Commission of Investigations & Attorney General.* Retrieved from www.state.nj.us/sci

Chapman, P. (2002, February 14-20). *Data Privacy*. European Voice p. 15-17.

Child Online Privacy Protection Act, 15 U.S.C. (1998)

Child Pornography Prevention Act of 1996

Child Protection Act, 18 U.S.C. § 2251-2255 (1984)

Child Protection and Sexual Predator Punishment Act of 1998

Children's Advertising Review Unit (2001, December). *Self regulatory guidelines for children's advertising.* Retrieved from http://caru.org/carusubpgs/guidepg.asp

Ciminello, D. (2000 April 5). Patenting e-business processes: Time for reform? *The Internet law Journal.* Retrieved from http://www.tilj.com/content/ipheadline04050001.htm

Ciminello, D. (2000 September 12). Deep linking is here to stay...for now. *The Internet law Journal*. Retrieved from http://www.tilj.com/content/ipheadline09080002.htm

Clinton announces moves to curb illegal gun sales (2000, September 23). *CNN.* Retrieved April 2, 2002 from http://www.nisat.org/blackmarket/north_america/

united_states/united_states_of_america/2000.09.23Clinton%20Announces%20Moves%20to%20Stop%20Illegal%20Guns%20Sales.html

Communications Assistance for Law Enforcement Act (CALEA), 18 U.S.C. §§ 2510-2522.

Computer Business Review Online (2002, January 28). Russian hacker breaks into banking database. *Computer Business Review Online*. Retrieved from http://www.computerbusinessreview.com /cbr.nsf/100/FB041291D873B60380256B4E00160F60?Opendocument&Highlight=2,extort

Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (1986).

Cooper, J. & Harrison, D. (2001). The social organization of audio piracy on the Internet media. *Culture & Society*. London: Sage Publications.

Cornish, D. (1993). Crimes as scripts in D. Zahm and P. Cromwell (eds.). *Proceedings of the International Seminar on Environmental Criminology and Crime Analysis*. Coral Gables Fl: University of Miami.

Council of Europe (1981). *Convention for the protection of individuals with regard to the automatic processing of personal data.* Retrieved from http://europa.eu.int/comm/internal_market/en/dataprot/inter/con10881.htm

Council of Europe (1990). *Recommendation No. R (89) 9 on computer related crime*. Strasbourg, France: European Committee on Crime Problems.

Council of Europe (1995). *Recommendation (95) 13 concerning problems of criminal procedural law connected with information technology.* Retrieved from http://cm.coe.int/ta/rec/1995/95r13.htm

Council of Europe (1997). *Recommendation No. R (97) 20 on hate speech*. Retrieved on January 30, 2002 from http://cm.coe.int/ta/rec/1997/97r20.html

Council of Europe (1999, February). *Recommendation R (99) on the protection of privacy on the Internet guidelines for the protection of individuals with regard to the collection and processing of personal data on information highways*. Retrieved from http://www.coe.fr/cm/ta/rec/1999/f99r5.htm

Council of Europe (2000, May 29). *Convention on mutual assistance in criminal matters between the member states of the European Union.* Retrieved from http://www.statewatch.org/news/2001/may/MLAfinal.htm.

Council of Europe (2001, November). *Convention on cyber-crime and explanatory memorandum.* Strasbourg, France: European Committee on Crime Problems. Retrieved from http://conventions.coe.int /Treaty/EN/cadreprincipal.htm

Council of Europe (2002, May 14). *DRAFT of the first Additional Protocol to the Convention on Cyber-crime concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems.* Retrieved from http://www.coe.int/T/E/Legal%5Faffairs /Legal%5Fco%2Doperation/Combating%5Feconomic%5Fcrime/Cybercrime/Racism%5Fon%5Finternet/PC-RX(2002)15E-5.pdf

Crawford, K. (2002, April 23), E-bay's risky bid. *Law.com*. Retrieved from http://www.law.com/jsp/statearchive.jsp?type=Article&oldid=ZZZ6377QYZC

Credit Card Abuse Act, 18 U.S.C. § 1029

Crime and Punishment (2002). *Encyclopaedia Britannica.* Chicago: Encyclopaedia Britannica. Retrieved April 5, 2002 from http://www.britannica.com/eb/article?eu=120709&hook=500345

Cyber Criminals Most Wanted (n.d.). *Computer crime task forces in the U.S.A.* Retrieved from http://www.ccmostwanted.com/policeCCU.htm

Cyberstalker jailed in Hong Kong (2001). *CNN*. Retrieved from http://www.cnn.com/2001/WORLD/asiapcf/east/02/19/Hongkong.cyberstalker/

DeLotto, R. (2001, April 16). *Demographic variation in privacy concerns.* Strategic Planning. Gartner Group (Research Note SPA-12-7860)

DeLotto, R. (2001, April 2). *Is corporate privacy the next 'big thing'?* Select Q&A. Gartner Group. (Research Note. QA-13-039)

DeLotto, R. (2001, February 21). *Is CRM a threat to consumer privacy?* Tactical guidelines. Gartner Group. (Research Note TG-12-6723)

Denning, D. (1999). *Activism, hacktivism and cyberterrorism: The Internet as a tool for influencing foreign policy.* Retrieved from http://www.nautilus.org/info-policy/workshop/papers/denning.html

Di Gregory, K. (2000, July 24). *Statement of K. Di Gregory Deputy Assistant Attorney General US Department of Justice, before the Subcommittee on the Constitution of the House Committee on the Judiciary, on 'Carnivore' and the Fourth Amendment.* Retrieved from http://www.cybercrime.gov /carnivore.htm

Digital Millennium and Copyright Act of 1998

Douwe, K. (1998). *Study on the protection of the rights and interests of legal persons with regard to the processing of personal data relating to such persons*. Brussels, Belgium: European Commission (Study Contract No. ETD/97/B5-9500/78)

Dumortier, J. and Goemans, C. (2000, March 23/24). *Data Privacy and Standardization*. Belgium: ICRI- K.U.Leuven. http://www.law.kuleuven.ac.be/icri.

Dyer, S. & O'Callaghan (1998, January). *Combating illicit light weapons trafficking: developments and opportunities.* London/Washington: British American Security Information Council.

Economic Espionage Act, 18 U.S.C. § 1831 et seq. (1996)

Ecpat International newsletters (2000, September 1). *Ecpat – A cause for celebration.* Retrieved from http://www.ecpat.net/eng/Ecpat_inter/IRC/articles.asp?articleID=75&NewsID=15

Electronic Communications Privacy Act, 18 U.S.C. §§ 2701-2711 (1986).

Electronic Frontier Foundation (2002, May 3). *Unintended consequences: Three years under the DMCA.* Retrieved from www.eff.org

Electronic Privacy Information Center (December, 1999). *Surfer Beware III: Privacy Policies without privacy protection*. Retrieved from http://www.epic.org/reports/surfer-beware3.html

Emma, O. (2000). Cyberstalking: Trends and issues in criminology. *Australian Institute of Criminology*. Retrieved from http://www.aic.gov.au/publications/tandi/ti166.pdf

Enos, L. (2000, July 25). US settles adult web fraud case. *E-Commerce Times.* Retrieved from http://www.ecommercetimes.com/news/articles2000/000725-3.shtml

Errico, M. (1997, July 8). Elle Macpherson victim of an extortion plot. *E!Online.* Retrieved from http://www.eonline.com/News/Items/0,1,1410,00.html

European Commission (1995, April 26). Council recommendation 95/144 on common information technology security evaluation criteria. *Official Journal of the European Communities Series L, 93,* 27.

European Commission (1996). *Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions on Illegal and harmful content on the Internet* [Electronic Version]. Brussels, Belgium: Author

European Commission (1997). *Interim report on initiatives in EU member states with respect to combating illegal and harmful content on the Internet, 7* [Electronic Version]. Brussels, Belgium: Author. Retrieved from http://europa.eu.int/ISPO/legal/en/internet/ wp2en.html

European Commission (1998, January 30). Directive 97/66/EC concerning the processing of personal data and the protection of privacy in the telecommunications sector. *Official Journal of the European Communities Series L, 24,* 1.

European Commission (1998, October 23). *Directive on personal data protection enters into effect.* Belgium: Brussels. Retrieved from http://europa.eu.int/comm/internal_market/en/dataprot/news/925.htm

European Commission (2000). *Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions "Network and Information Security: Proposal for a European Policy Approach."* [Electronic Version]. Brussels, Belgium: Author

European Commission (2000). *Communication from the Commission to the Council, the European Parliament, the Economic and social Committee and the Committee of the Regions, "Creating a safer information society by improving the security of information infrastructures and combating computer related crime* EC, COM 2000, 890 Final.

European Commission (2000). *Council decision 2000/375/JHA to combat child pornography on the Internet*. Brussels, Belgium: Author.

European Commission (2000, January 19). Directive 99/93/EC on a Community framework for electronic signatures*. Official Journal of the European Communities Series L, 13* 12.

European Commission (2001, January 1). Directive 95/46/EC concerning the protection of individuals with regard to the processing of personal data and the free movement of such data*. Official Journal of the European Communities Series L, 8*, 1.

European Commission (2001, November 6). *Discussion paper for expert's meeting on retention of traffic data.* Retrieved from www.statewatch.org/news/2001/may /03Cenfopol.htm

European Commission (2002, April 19). *Proposal for a Council framework decision on attacks against information systems.* Brussels, Belgium: Author. (Document No. COM (2002) 173 final, 2002/0086 (CNS))

European Commission (2002, February 13). *The application of Commission Decision 520/2000/EC of 26 July 2000 pursuant to Directive 95/46 of the EP and of the Council on the adequate protection of personal data provided by the safe harbor privacy principles and related frequently asked questions issued by the US Department of Commerce.* Brussels, Belgium: Author. (Paper No. SEC (2002) 196)

European Commission, (2002, March 6). *Fifth annual report on the situation regarding the protection of individuals with regard to the processing of personal data and privacy in the European Union and in third countries – Covering the year 2000, Part I.* No. WP 54. Brussels, Belgium: Author. Retrieved from http://europa.eu.int/comm/internal_market /en/dataprot/wpdocs/index.htm

European Information and Communications Technology Industry Association (2000). *EICTA comments on the common draft convention on cyber-crime (Draft No.22 REV 2) of the EC on Crime Problems and the committee of experts on crime in cyber-space.* Retrieved from, http://www.eicta.org

Federal Bureau of Investigations (2001, March 18). *Press release: Innocent images operation candyman phase I*. Washington DC: Author. Retrieved from http://www.fbi.gov/pressrel/candyman /candymanhome.htm

Federal Deposit Insurance Corporation (2002, April 29). *FDIC law regulation and related acts.* Retrieved from http://www.fdic.gov/regulations/laws/index.html

Federal Trade Commission (1998, June). *Privacy online: A report to Congress* (p. 71). Washington DC: Author

Federal Trade Commission (2000, February). *Going, going, gone…law enforcements efforts to combat online auction fraud.* Washington DC: Author. Retrieved from http://www.ftc.gov/bcp/reports/int-auction.htm

Federal Trade Commission (2000, October 31). *Law enforcers target 'top ten' online scams.* Washington DC: Author. Retrieved from http://www.ftc.gov/opa/2000/10/topten.htm

Federal Wiretap Act 18 U.S.C. § 1343

Felson, M. (2001). *Crime and everyday life*. Thousand Oaks CA, Pine forges Press

Financial Action Task Force on Money Laundering (2001, February 1). *Report on money laundering typologies 2000-2001*. London, UK: Author.

Finkel, M. (2001, May 21). This little kidney went to market [Electronic Version]. *The New York Times Magazine*. Retrieved February 1, 2001 from http://www.artsci.wustl.edu/ ~anderson/introethics/NYTimes_Organ_buying.htm

Fletcher, G.P. (1998). *Basic Concepts in Criminal Law.* New York: Oxford University Press Inc.

Food and Drug Administration, Center for Veterinary medicine (2000, October 2). *Press release: FDA participating in AAFCO Internet surf day.* Retrieved from http://www.fda.gov/cvm/index/updates/surfdayu.htm

Forsman, T. (2000 September 28), The high cost of doing e-commerce, *BusinessWeek online.* Retrieved from http://www.businessweek.com /smallbiz/content/sep2000/sb20000928_410.htm

Fournier de Saint Maur, A.(1999). Sexual Abuse of Children on Internet: A New Challenge for INTERPOL. *UNESCO.* Retrieved from http://mirror-us.unesco.org/ webworld/child_screen/documents/interpol_e.rtf

Freeman, DJ. (2001, March 1). *Data transfer study, application to the ASP industry*. Retrieved from http://www.djfreeman.com .

FTC Press Release (1998, July 14). *Promoter of online pyramid scheme agrees to settle FTC charges.* Retrieved from: http://www.ftc.gov/opa/1998/9807/meganet.htm

Galil, Y. (2001, June 03) The Cookie Monster Strikes Back. *The Internet Law Journal.* Retrieved from http://www.tilj.com/content/ecomheadline06030102.htm

Gillard, M. (2001, October 19). Secrecy surrounds £26m Barclaycard blackmail case. *Guardian Unlimited.* Retrieved from http://www.guardian.co.uk/Archive/Article/ 0,4273,4280653,00.html

Glasner, J. (2001, February 14). Amazon Loses Patent Suit Round. *Wired News*. Retrieved from http://www.wired.com/news/business/0,1367,41824,00.html

Global Business Dialogue on Electronic Commerce (2000, September 26). Cyber Security and Cyber-crime. Retrieved from http://www.gbde.org/cybersecurity/

Goemans, C. (2002, March 15). Anonimiteit op het Internet. [Anonymity on the Internet]. Belgium: ICRI -*K.U.Leuven*, http://www.law.kuleuven.ac.be/icri

Goodwins, R. and Loney, M. (2002, September 3). Gamers face hail in Greece. *ZDNet UK.* Retrieved from http://news.zdnet.co.uk/story/0,,t269-s2121692,00.html

Gosh, A. (2001, April 22). *Protection of privacy.* Unisys: Australia.

Goss, A. (2001). Jay Cohen's brave new world: The liability of offshore operators of licensed Internet casinos for breach of United States' anti-gambling laws. *The Richmond Journal of Law and Technology, 100.* Retrieved January 24, 2002 from http://www.richmond.edu /jolt/v7i4/ article2.html

Gramm-Leach-Bliley Act, 15 U.S.C (1999)

Gray, D. (2001, May 1) Amazon unit to pay in privacy settlement. *CNN*. Retrieved from http://www.cnn.com/2001/TECH/ industry/05/01/amazon.pays.idg

Green, H. Norm, A. Borrus, A. & Yang, C. (2000, February 14). Privacy: Outrage on the Web. *Business Week*. Retrieved from http://www.businessweek.com/2000/00_07/b3668065.htm

Greenberg, P. (2000, July 13). Toysmart flab triggers privacy bill. *E-Commerce News.* Retrieved from http://www.ecommercetimes.com/perl/story/3766.html

Grove, R. and Zerega, B. (2002, January). The lolita problem. *Red Herring.* Retrieved from http://redherring.com/insider/2002/0118/1249.html

Haines, J. & Johnstone, P. (1999). Global cybercrime: New toys for the money launderers. *Journal of Money Laundering Control, 2,* 317-325.

Hall, K.G. (2001, January 3). The net feeds boom in sex trade and slavery. *SiliconValley.com.* Retrieved from http://www0.mercurycenter.com/svtech/news/indepth/ docs/brazil010301.htm

Hallawell, A. (2001, March 1). *Mr.President, It's time for new privacy protection methods*. Tactical Guidelines, Gartner Group. (Document No. TG-12-8841)

Hallawell, A. (2001, May 3). *Privacy laws abroad: How worried should enterprises be?* Research Note, Gartner Group. (Tutorials TU-13-5533)

Hallawell, A. (2001, May 4). *Beyond the headlines: Privacy issues and the enterprise.* Research Note, Gartner Group: (Document No. COM-13-5873)

Hallawell, A. (2002, February 4). *The regulatory future for spam and Cookies in the EU.* Research Note, Gartner Group, (Tactical Guidelines TG-14-3261)

Hoar, S. (2001). Identity theft: The crime of the new millennium. *United States Department of Justice.* Retrieved from http://www.usdoj.gov/criminal/cybercrime/usamarch2001_3.htm

Hof, R.D. & Hamm, S. (2002, May 13) How e-biz rose, fell, and will rise anew. *BusinessWeek online*. Retrieved from http://www.businessweek.com /magazine/content/02_19/b3782601.htm

Howard, J.D. & Longstaff, T. A., (1998, October). *Sandia Report: A common language for computer security incidents* [Electronic Version]. Albuquerque, NM: Sandia National Laboratories.

Howard, J.D. (1998). A taxonomy of computer and network attacks. In *An analysis of security incidents on the Internet 1989-1995* (chap 6). Retrieved from http://www.cert.org/research/JHThesis/Word6 /chap06.doc

Hughes, D. (2000). 'Welcome to the rape camp' Sexual exploitation and the Internet in Cambodia [Electronic Version]. *Journal of Sexual Aggression.* Retrieved from http://www.uri.edu/artsci/wms/hughes/rapecamp.htm

Hughes, D., Sporcic, L., Mendelsohn, N., Chirgwin, V. (1999). *The Factbook on Global Sexual Exploitation.* Coalition Against Trafficking in Women. Retrieved from http://www.uri.edu/artsci/wms/hughes/spain.htm

Hulme, G.V. (2002, Jan. 28). Businesses keep spending on security. *Information Week.* Retrieved from http://www.informationweek.com/story/IWK20020124S0004

Hunt, S. and Rosch, P. (2001, July 23). *IT trends: enterprise security and privacy*. Giga Information Group. (RPA-072001-00018)

Identity Theft and Deterrence Act of 1998

Individual Reference Service Group (n.d.). *The individual reference service group preamble.* Retrieved from http://irsg.org/html/industry_principles_principles.htm

Information Technology Association of Canada (2000, August 30). Draft Common View Paper, for the International Information Industry Congress Millennium Congress on Sept. 19, 2000, Québec, Canada. Retrieved from http://www.itac.ca

Information Warfare Site (2002). *Critical information protection: Infragard.* Retrieved from http://www.iwar.org.uk/infragard/

Institute for the Protection and Security of Citizen, Cybersecurity Sector (2001). Retrieved from http://www.cordis.lu/euroabstracts /en/april02/ict03.htm

International Gay and Lesbian Human Rights Commission (2001, December 19). *Egypt: One step toward justice, two steps back: More convictions for homosexual conduct in Egypt as teenager freed*. Retrieved from www.iglhrc.org/news/press/pr_011219_2.html

International Narcotics Control Board (2002). *Annual report 2001.* [Electronic Version]. New York: United Nations Publishing.

International review of criminal policy-Untied Nations Manual on the prevention and control of computer related crime (1999). Retrieved December 17, 2001 from http://www.ifs.univie.ac.at/~pr2gq1/rev4344.html

Internet Safety Watch Inc. (2001). *About Internet Safety Watch Inc.* Retrieved from http://www.cyber-hood-watch.org/about_us.htm

Interpol (1995). *Funds derived from criminal activities.* Retrieved from http://www.interpol.int/ public/FinancialCrime/FOPAC/default.asp

Janal, D. (1998). *Risky Business: Protect your business from being stalked, conned, or blackmailed on the Web.* New York, NY: John Wiley & Sons, Inc.

Johnson, P. (2000, November). Net predator jailed for five years *Computer Forensics*. Retrieved from http://www.computer-forensics.com/news/welcome.html

Johnston, M. (2001 January 26). Cracking Down on Software Piracy. *PC World.* Retrieved from http://www.pcworld.com/news/article/0,aid,39382,00.asp

Judah, D. (1997). Defamation in cyberspace. *Computer Law & Security Report, 13*(6), 442-446.

Koster, E. (1999). Zero privacy: personal data on the Internet. *Oppenheimer.* Retrieved from http://www.oppenheimer.com/intprop/ news/zeroprivacy.shtml

Lee, J. (2002, March 7). Once bamboozled, now a bloodhound. *The New York Times*. Retrieved from: www.nytimes.com/2001/03/07 /technology/circuits/07VIGI.html

Levy, E. (2001, October 23). Security in an open electronic society. *BusinessWeek online*. Retrieved from http://www.businessweek.com /technology/content/oct2001/tc20011023_7497.htm

Locke, D. (2000 February). Domain name regulation: Bad news for domain name pirates? *Computer Law and Security Report*, 37-38

London Internet Exchange (2001, May 15). LINX best current practice – user privacy. Retrieved from http://www.linx.org/noncore/bcp/traceability-bcp.html.

Malagò, T. & Mignone, M. (2000). Crimini e Musica online [Crime and music online]. Milano IT: Franco Angeli.

Man admits to stealing military credit accounts (2000, May 17). *Apbnews.com.* Retrieved from http://www.apbnews.com/newscenter/internetcrime/ 2000/05/17/creditcard0517_01.html

Markoff, J. (2002, May 13). Vulnerability is discovered in security for smart cards. *The New York Times*. Retrieved from http://query.nytimes.com /search/abstract?res=FB0C15FA3C5D0C708DDDAC0894DA404482

McDonald, I. (1998). Copyright infringement. Paper presented at the Australian Institute of Criminology Conference – Internet Crime. Melbourne, Australia. Retrieved from http://www.aic.gov.au/ conferences/internet/program.html

McKinley, J. (2002, February 26). State pulls data from Internet in attempt to thwart terrorists [Electronic Version]. *New York Times.* Retrieved from http://www.nytimes.com/2002/03/06/international/asia/06INQU.html?ex=10164 89250&ei=1&en=d6a29f0f17338136

McWilliams, B. (2000, January 9). Failed blackmail attempt leads to credit card theft. *Internetnews.com.* Retrieved from www.internetnews.com/ec-news/article/0,,4_278091,00.html

McWilliams, B. (2000, May 25). PhD student arrested in blackmail attempt. *Internetnews.com.* Retrieved from www.internetnews.com/bus-news/article/0,,3_380531,00.html

Meller, P. (2002, May 30). EU set to weaken Net privacy regime*. The New York Times- The International Herald Tribune Online*. Retrieved from http://www.iht.com/cgi-bin/generic.cgi?template=articleprint.tmplh&ArticleId=59491

Mickna, L. (2001, July 23). Encryption regulation: A first amendment perspective. *Sans Institute.* Retrieved from http://rr.sans.org/encryption/regulation.php

Molander, R. Riddle, A., & Wilson P. (1996). *A new face of war: Strategic information warfare*. Santa Monica: RAND. Retrieved from http://www.rand.org/publications/MR/MR661/ MR661.pdf

Muffet, A. (1993). *Almost Everything You Ever Wanted To Know About Computer Security.* Massachusetts: National Security Institute. Retrieved from http://nsi.org/Library/Compsec/faq.htm

Mullen, M. (2002, May 31). Security hole striptease. *BusinessWeek online*. Retrieved from http://www.businessweek.com/technology /content/may2002/tc20020531_1577.htm

Muris, T. (2001, Oct 4). *Protecting consumers' privacy: 2002 and beyond.* Remarks of Chairman Timothy J.Muris at the Privacy 2001 Conference, Cleveland, Ohio. Washington DC: Federal Trade Commission.

National Center for Missing & Exploited Children (2002, April 19). *National center for missing & exploited children vows to protect children from 'virtual" porn predators*. Retrieved from http://www.missingkids.org/

National Infrastructure Protection Center (n.d.) *About NIPC.* Washington DC: Author. Retrieved from http://www.nipc.gov/about/about2.htm

National Security Institute (n.d.). *Selecting good passwords.* Massachusetts: Author. Retrieved from http://nsi.org/Library/Compsec/goodpass.html

Nichols, R., Bough, W., & Ryan, J., (2000). *Defending your digital assets from hackers, crackers, spies, and thieves.* New York, NY: Mcgraw-Hill.

No Electronic Theft Act, 1997

Noack, D. (2000, April 28). Stalking victim's kin sues info broker. *Apbnews.com.* Retrieved from http://www.apbnews.com/newscenter/ internetcrime/2000/04/28/searchsuit0428_01.html

Notice of Certain Electronic Surveillance, 18 U.S.C. § 2232

Online pharmacies busted (1999, June 10). *Reuters Wired News.* Retrieved from http://www.wired.com/news/print/0,1294,20151,00.html

Oppermann, M. (1999, April). Sex tourism. *Annals of Tourism Research,* 251-266.

Organization for Economic Co-operation and Development (1980). *Recommendations of the council concerning guidelines governing the protection of privacy and transborder flows of personal data.* Paris, France: Retrieved from http://europa.eu.int/comm/internal_market/en/dataprot/inter/priv.htm

Organization for Economic Co-operation and Development (1980). *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security.* Paris: France. Retrieved from http://www.oecd.org/document/42/0,2340,en_2649_33703_15582250_1_1_1_1,0 0.html

Ott, R. (2000, May) Cybersquatting. *Network Security*, .7.

Painter, C. (2001). *Tracing the Internet fraud cases: PairGain and NEI webworld.* US Department of Justice. Retrieved from http://www.usdoj.gov/criminal/cybercrime/usamay2001_3.htm

Parker, D. (1998). *Fighting computer crime: A new framework for protecting information.* New York, NY: John Wiley & Sons, Inc.

Penfold, C. (2001). Nazi, porn, and politics: Asserting control over Internet content. *The Journal of Information, Law and Technology (JILT)* [Electronic Version]. Retrieved from http://elj.warwick.ac.uk/jilt/01-2/penfold.html

Perera, R. (2000, August 17). Swiss bank hit by 'Love Bug' variant. *Computerworld, IDG News Service*.

Poulsen, K. (2002, March 7). Guesswork plagues web hole reporting. *BusinessWeek online*. Retrieved from http://www.businessweek.com /technology/content/mar2002/tc2002036_1544.htm

Power, R. (2000). *Tangled Web: Tales of digital crime from the shadows of cyberspace.* Indianapolis: Que Corporation

Power, R. (2002). *Computer security issues and trends.* San Francisco: Computer Security Institute.

Privacilla Organization (2001, May). *Privacy Fundamentals*. Retrieved from http://www.privacilla.org/fundamentals/ privacydefinition.html

Privacy Protection Act, 42 U.S.C § 2000aa

Privacy rights of (2002). Encyclopædia Britannica. Chicago: Encyclopaedia Britannica. Retrieved April 5, 2002 from http://www.britannica.com/eb/article?eu=62999&tocid=0&query=privacy%2C%20rights%20of

Property (2002). *Encyclopaedia Britannica.* Chicago: Encyclopaedia Britannica. Retrieved April 5, 2002 from http://www.britannica.com/eb/article?eu=63118&tocid=0&query=property

Prostitutes hook up to the net (2001, January 19). *Chicago Tribune.* Retrieved from http://www.nua.ie/surveys/index.cgi?f=VS&art_id=905356362&rel=true

Radcliff, D. (2000, May 31). A case of cyberstalking. *CNN.* Retrieved from www.cnn.com/2000/TECH/computing/05/31/cyberstalking.idg/index.html

Rasch, M. (1996). Criminal law and the Internet. In J. Ruh (Ed). *The Internet and business: A lawyers guide to emerging legal issues*. Fairfax, VA: Computer Law Association. Retrieved from http://www.cla.org/ruhbook/chp11.htm

Raysman, R. & Brown, P. (2000, May 9). Congress may play its hand with Internet gambling law. *New York Law Journal.* Retrieved from http://www.brownraysman.com/publications/techlaw/nylj0500.htm

Renn, O. (1998). Three decades of risk research: accomplishments and new challenges. *Journal of Risk Research 1 (1),* 49-71.

Reuters (2002, May 31), *EU Vote relaxes e-privacy rules.* Retrieved from http://zdnet.com.com/2102-1105-929605.html

Richard, A. (1999). International trafficking in women to the United States: A contemporary manifestation of slavery and organized crime. *Center for the Study of Intelligence*. Washington DC. CIA.

Richtel, M. (2002, May 13). Credit card theft thrives online as global market. *The New York Times*. Retrieved from www.nytimes.com/2001/05/13 /technology/13CARD.html

Risen, J. & Johnston, D. (2002, March 6). Intercepted Al Qaeda emails said to hint at regrouping. *New York Times.* Retrieved from http://www.nytimes.com/2002/03/06/international/asia/06INQU.html?ex=1016489250&ei=1&en6da29f0f17338136

Rodger, W. (2002, January 10). Punish security lapses, NAS urges. *BusinessWeek online*. Retrieved from http://www.businessweek.com /technology/content/jan2002/tc20020110_2851.htm

Rogers, M. (1999, February 12). *Psychology of hackers: Steps toward a new taxonomy.* Retrieved from www.infowar.com

Saia, R. (2002, February 7). Keep e-commerce in mind when boosting security. *ComputerWorld*. Retrieved from http://www.computerworld.com /printthis/2002/0,4814,68101,00.html

Saint-Tropez.com Domain Name Dispute (1998) *Perkinscoie Internet case digest*. Retrieved from http://www.perkinscoie.com/casedigest/icd_results.cfm?keyword1=trademark&keyword2=trademark%20infringement&keyword3=dilution&topic=Trademark%20Infringement%2FDilution

Salkever, A. (2000, August 22). Cyber-Extortion: When data is held hostage. *BusinessWeek online*. Retrieved from http://www.businessweek.com /bwdaily/dnflash/aug2000/nf20000822_308.htm

Salkever, A. (2001, December 4). A new twist in computer security tools. *BusinessWeek online*. Retrieved from http://www.businessweek.com /technology/content/dec2001/tc2001124_8753.htm

Salkever, A. (2001, October 10). Truth could be the web's first casualty *BusinessWeek online*. Retrieved from http://www.businessweek.com /bwdaily/dnflash/oct2001/nf2001110_1399.htm

Salkever, A. (2001, October 2). Uncle Sam should learn to hack. *BusinessWeek online*. Retrieved from http://www.businessweek.com /bwdaily/dnflash/oct2001/nf2001102_7160.htm

Salkever, A. (2002, April 2) E-insurance for the digital age. *BusinessWeek online*. Retrieved from http://www.businessweek.com/bwdaily /dnflash/apr2002/nf2002042_8163.htm

Salkever, A. (2002, June 5). Security blankets: One layer isn't enough. *BusinessWeek online*. Retrieved from http://www.businessweek.com /technology/content/jun2002/tc2002065_8400.htm

Savona, E. (2000). Offshore and Internet: A risky pair. Paper presented at Internet Security – A Contemporary Challenge Conference. Muscat, Sultanate of Oman.

Scoperto giro di prostitutzione via Internet dalla Russia alla Sicilia [Prostitution ring discovered on the Internet from Russia to Sicily] (2000, February 1). *Quotidiano.net.* Retrieved from http://quotidiano.monrif.net/art/2000/02/01/497966

Sieber, U. (1998). Legal aspect of computer related crime in the information society -COMCRIME Study- Version 1.0. Retrieved from http://europa.eu.int/ISPO/legal/en/crime/crime.html

Singh, M. (2000, July 3). *Internet Privacy Issues: Are they real or perceived?* Market Analysis, Gartner Group.

Singh, M., Cowles, R., & Rendall, D. (2001, June 13). *Solving the Internet privacy crisis: Entrusting corporate America or the federal government?* Market Analysis, Gartner Group.

Sinrod, E. J., & Reilly, W.P., (2000). Cyber-crimes: A practical approach to the application of federal computer crime laws [Electronic Version]. *Santa Clara Computer and High Technology Law Journal 16,* (2).

Sixth man jailed in Internet male prostitution ring (1996). *Lubbock Avalanche-Journal* [Online]. Retrieved from www.lubbockonline.com/news/120896/sixthman.htm

Smith-Kubiszyn, M. (2000). Emerging Legal Guidance on "Deep Linking." Retrieved from http://www.gigalaw.com/articles/2000/kubiszyn-2000-05b.html

Smith-Kubiszyn, M. (2000). Web Site Framing: Trademark and Copyright Issues. Retrieved from http://www.gigalaw.com/articles/2000/kubiszyn-2000-04.html

SNC Havas Numerique v. SA Kelijob (2000). *Perkinscoie Internet case digest* Retrieved from http://www.perkinscoie.com/casedigest/icd_results.cfm?keyword1=copyright&topic=Copyright

Snyder, R., Bruck, H., & Sapin, B. (1962). *Foreign policy decision-making: An approach to the study of international politics.* New York: Free Press.

Société cooperative agricole Champagne Céréales v. G.J (1998). *Perkinscoie Internet case digest.* Retrieved from http://www.perkinscoie.com/casedigest/icd_results.cfm?keyword1=trademark&keyword2=trademark%20infringement&keyword3=dilution&topic=Trademark%20Infringement%2FDilution

Sofaer, A.D., Goodman, S. E., Cueller, M. F., Drozdova, E.A., Elliot, D.D., Grove, G.D., Lukasik, S.J., Putman, T. L., Wilson, G.D. (2000). A proposal for an international convention on cyber-crime and terrorism. Retrieved October 26, 2001 from http://www.oas.org/juridico/english/ monograph.htm

Spatt, D. M (1996). The Information superhighway: recent court. *Ocean State Lawyer for the Arts (OSLA)*. Retrieved from http://www.artslaw.org/INTERNET.HTM

Sprenger, P. (1999, July 14) Amazon riles N. Ireland leader. *Wired News.com.* Retrieved from http://www.wired.com/news/business/0,1367,20199,00.html

Staglianò, R. (2002, February 8). Sì, sono stata Playmate e posso scriverlo sul web [Yes, I was a playmate and I can write in on the Web]. *La Repubblica.* Retrieved from http://www.repubblica.it/online/tecnologie_internet/playboy/playboy/playboy.html

Sullivan, B. (2001). Huge identity theft unresolved. *MSNBC.com.* Retrieved from newsgroup message board http://www.landfield.com/isn/mail-archive/2001/Jul/0076.html

Surmacz,J. (2002, May 8). An ounce of prevention. *CIO*. Retrieved from http://www2.cio.com/metrics/2002/metric364.html

Taylor, P (1999). *Hackers.* London: Routledge.

Tedeschi, B. (2001, August 27). Seller of online currency may have been victim of fraud. *The New York Times*. Retrieved from http://www.nytimes.com/2001/08/27/technology/ebusiness/27ECOMMERCE.HTML

Telecommunications Act, Pub. LA. No. 104-104, 110 Stat. 56 (1996).

Terrorism Research Center (2000). *Definitions.* Retrieved from http://www.terrorism.com/index.shtml

The Egmont Training Working Group (1999). *Financial intelligence units in action: 100 cases from the Egmont Group*. London UK: Financial Action Task Force.

The Freedom of Information Act 5 U.S.C. (1966).

The Internet Fraud Complaint Center (2001). *Annual Internet Fraud Report: May 8, 2000-May 8, 2001.* [Electronic Version]. Prepared by the National White Collar Crime Center and the Federal bureau of Investigation. Retrieved from http://www1.ifccfbi.gov/strategy/statistics.asp

Tracey, B. & Mattinson, J. (2000). *The extent and nature of stalking - Findings from the 1998 British crime survey*. London, UK: Home Office Research Department. Retrieved from http://www.homeoffice.gov.uk/rds/pdfs/hors210.pdf

United Nations (1948). *Universal declaration of human rights.* Retrieved from http://www.un.org/Overview/rights.html

United Nations (1966). *International Covenant on Civil and Political Rights*. Retrieved from http://europa.eu.int/comm/internal_market/en/dataprot/inter/16-12-1966.pdf

United Nations (1980). *Guidelines concerning computerized personal data files.* Retrieved from http://europa.eu.int/comm/internal_market/en/dataprot/inter/un.htm

United Nations (1996). *International Convention on the elimination of all forms of racial discrimination.* Retrieved from http://www.hri.org/docs/ICERD66.html

United Nations (2000). *II Protocol to prevent, suppress and punish trafficking in person especially women and children supplementing the United Nations convention against transnational organized crime nations*. Retrieved from http://www.undcp.org/palermo/convmain.html

United Nations (2001). *III Protocol against the illicit manufacturing of and trafficking in firearms, their parts and components and ammunition supplementing the United Nations Convention against transnational organized crime nations*. Retrieved from http://www.undcp.org/ crime_cicp_convention_documents.html

United Nations Assembly (1972). *Single convention on narcotics drugs 1961 as amended by the 1972 protocol*. Retrieved from http://www.incb.org/e/ind_conv.htm

United Nations Economic and Social Council (2001, March 30). *Conclusions of the study on effective measures to prevent and control high-technology and computer related crime.* New York: Author.

United Nations Manual on the prevention and control of computer related crime (1999). *International review of criminal policy 43 and 44.* Retrieved from http://www.uncjin.org/8th.pdf

United States Copyright Office Summary (1998, December). *Digital millennium copyright act of 1998.* Washington DC: Author

United States Customs Services (n.d.) *Customs cybersmuggling center (C3).* Retrieved from http://www.customs.gov/enforcem/cyber.htm#top

United States Department of Education (1997, November). *Parents Guide to the Internet.* Washington DC: Author. Retrieved from http://www.ed.gov/pubs/parents/internet/

United States Department of Justice (2000). *Prosecuting Intellectual Property Crimes* Washington DC: Author. Retrieved from http://www.cybercrime.gov/ipmanual.htm

United States Department of Justice (2000, March). *The electronic frontier: the challenge of unlawful conduct involving the use of the internet* [Electronic Version]. Retrieved June 13, 2001 from http://www.usdoj.gov/criminal/cybercrime/unlawful.htm

United States Department of Justice (2000, October). *New York city law firm paralegal pleads guilty to stealing trial plan.* Retrieved from http://www.usdoj.gov/criminal/cybercrime/farrajPlea.htm

United States Department of Justice (2001). *Internet Fraud*. Retrieved from http://www.usdoj.gov/criminal/fraud/Internet.htm

United States Department of Justice (2001, January). - *Seizing computers and obtaining electronic evidence in criminal investigations.* Washington DC: Computer Crime and Intellectual Property Section.

United States Department of Justice (2002). *Creator of Melissa computer virus sentenced to 20 months in federal prison.* Retrieved from http://www.usdoj.gov /criminal/cybercrime/melissaSent.htm

United States Department of Justice (2002, February 2). *Press Release: Internet Fraud Complaint Center (IFCC) wins the excellence in .gov award*. Retrieved from http://www1.ifccfbi.gov/strategy/wn020602.asp

United States Department of Justice (2002, February 26). *US charges engineer with theft of trade secret at White Plains software company.* Retrieved from http://www.cybercrime.gov/kissaneArrest.htm

United States Department of Justice (2002, January 30). *Press release: Six defendants sentenced in $16 million bogus investment scheme marketed over Internet*. Retrieved from http://www.cybercrime.gov/guastella_martins.htm

United States Department of Justice (n.d.). *Parents guide to Internet safety*. Washington DC: Federal Bureau of Investigations. Retrieved from http://www.fbi.gov/publications /pguide/pguide.htm

United States Securities and Exchange Commission (2002). *About the Office of Internet Enforcement.* Washington DC: Author. Retrieved from http://www.sec.gov/divisions/enforce/internetenforce.htm

United States v. Cohen, 260 F.3d 68 (2d Cir. 2001).

United States v. Hoke, 1999 CR 99-441 C.D. Cal. indictment filed April 30, 1999

Uniting and strengthening America by providing appropriate tools to intercept and obstruct terrorism (USA Patriot Act) Act of 2001.

Van Eecke, P. (2002, May 27). Meer rechtszekerheid bij internetcontrole. [More legal security on control of the Internet]. *De Standaard*. Retrieved from http://www.standaard.be/Archief/Zoeken/ DetailNew.asp?articleID=DST27052002_071&trefwoord=internetcontrole

Vartti, R (2002). German matchmaking web sites-online trafficking in women? Retrieved from http://www.vifu.de/students/vartti/ ElectronicTraffickinginWomen.doc

Vendere semi di marijuana online non e reato [To sell Marijuana is not a crime] (2001). *Il resto del Carlino.it.* Retrieved from http://ilrestodelcarlino.quotidiano.net/art/2001/05/02/2111818

Verton, D. (2000, April 26). DOD Web-watchers find war plans online. *Federal Computer Week.* Retrieved from http://www.fcw.com/fcw/articles/2000/0424/web-jtfcnd-04-26-00.asp

Wall, D.S. (2001). Maintaining order and law on the Internet. In D.S. Wall (Ed). *Crime and the Internet.* London, Routledge

Williams, P. (1999). Trafficking in women and children: A market perspective. In Williams, P. (Ed.), *Illegal immigration and commercial sex. The new slave trade* p.145-170. , London: Frank Cass.

WITSA World Information Technology and Services Alliance (2000, November) Statement on the Council of Europe Draft Convention on Cyber-crime. Retrieved from: http://www.witsa.org

Worden, A. (2000, May 19). Fake Ids flourish on Internet. *Apbnews.com*. Retrieved fromwww.apbnews.com/newscenter/internetcrime/2000/05/ 19/id0519_01.html

World Medical Association (2000). Statement human organ and tissue donation and transplantation. *World Medical Association Policy*.

Young, D. (1999, September 7). *An e-transplant prophecy*. Retrieved January 25, 2002 from http://www.mitec.net/~jryoung/ dgyoung/organs.html

Zanini, M & Edwards, S (2001). The networking of terror in the information age. In J. Arquilla & D. Ronfedlt (Eds.). *Networks and netwars: The future of terror, crime and militancy* [Electronic-version]. Santa Monica CA: RAND. Retrieved from http://www.rand.org/publications/MR/MR1382/

OTHER WORKS NOT CITED IN THE TEXT

Akdeniz, Y. (1999). *Sex on the net: the dilemma of policing in cyberspace.* Reading, UK: Garnet Publishing Limited.

Babbitt, S. (1999). *Internet Cookies and Your Privacy.* Retrieved from Alma College Department of Communications Web site http://cicero.com.alma.edu/communication/303wi99/ students/babbitt/303sbfp.htm

Baker and McKenzie (2001, March). EU developments in IP, IT and telecommunications law*. Computer Law and Security Report* p. 126-131

Bennett, M. (1999, September 14). Online privacy policies: Not (yet) an effective tool for addressing consumer concerns. *Giga Information Group, IdeaByte. (*474631-MB99).

Borland, J. (1998, May 28). German court holds ISP liable for net porn. *TechWeb News.* Retrieved from http://content.techweb.com/ wire/story/TWB19980528S0022

China mine boss touts kidney (2000, December). *BBC News* [Electronic Version]. Retrieved from http://news.bbc.co.uk/hi/english/world/asia-pacific/ newsid_1070000/ 1070684.stm

Clayton, R., Bohm, R., Davies, G. (2001, May 15). *LINX best current practice user privacy, Version 1.0*. International User Privacy Forum. Retrieved from http://www.iupf.org.uk/privacy-bcp.html.

Dmitrieva, I. (2000, May). I know it when I see it: Should Internet providers recognize Copyright violation when they see it? *Santa Clara computer and High Technology Law Journal*. Santa Clara University School of Law: California

Donahey, S. and Hilbert, R. (2000, May). World wrestling federation entertainment, Inc. v. Michael Bosman: A legal body slam for cybersquatters on the web. *Santa Clara Computer and High Technology Law Journal.* Santa Clara University School of Law: California

Field, T. (2001, June). Copyright on the Internet. *Intellectual Property Counselor.* Retrieved from http://www.fplc.edu/TFIELD/COPYNET.HTM

Gall, B. (2000). *An overview of intellectual property protection*. Retrieved from http://www.gigalaw.com/articles/gall-2000-10-p1.html

Ginding, S. (1997). Lost and found in cyberspace: Informational privacy in the age of the Internet [Electronic version]. *San Diego Law Review, 34,* 1153. Retrieved from http://www.info-law.com/lost.html

Grady, J. (2000, December 12). *E-procurement bids up privacy concerns*. Giga Information Group. (Document No. RIB-122000-00108)

Grady, J. (2001, June 29). *Online privacy surveys point toward three types of users.* Giga Information Group. (Document No. RIB-062001-00300)

Hermoso, A. & Cullen, S. (1999). Sexual abuse of children, child pornography and pedophilia on the internet: an international challenge. *UNESCO.* Retrieved from http://mirror-us.unesco.org/webworld/child_screen/ documents/a_hermoso.rtf

Kern, A. & Munro, R. (1996). Cyberpayments: Internet and electronic money laundering: Countdown to the year 2000. *Journal of Financial Crime, 4,* 156-264.

Libertarians say: online sale of human organs could save lives (1999, September 7). *Libertarian Party Press Release* [Electronic Version]. Retrieved from http://www.lp.org/press/ archive.php?function=view&record=63

Murphy, D. (1998). Electronic transfer of funds: Smart cards, Internet banking and wireless communications. *Journal of Financial Crime, 6,* 26-35.

Phua, S. (2000, January 10). *Information security: The e-commerce driver.* Market Analysis, Gartner Group.

Privacilla Organization (2001, July). *Privacy and Business*. Retrieved from http://www.privacilla.org/business.html

Privacilla Organization (2001, July). Privacy and Government. Retrieved from http://www.privacilla.org/government.html

Privacy Law Adviser (2002, March 20), Vol.2. 1117-1144. Silver Spring, MD: Pike & Fischer, Inc.

Privacy Right Clearinghouse " (2001, March). *A review of current privacy issues.* Retrieved from http://www.privacyrights.org/ar/Privacy-IssuesList.htm

Privacy Right Clearinghouse (2000, February 11-12), *Privacy expectations in a high tech world.* Retrieved from http://www.privacyrights.org/ ar/expect.htm.

Privacy Right Clearinghouse (2001 April). *Fact Sheet 7: Workplace Privacy*. Retrieved from http://www.privacyrights.org/fs/fs7-work.htm.

Privacy Right Clearinghouse (2002, January). *Fact Sheet 4: Reducing Junk Mail*. Retrieved from http://www.privacyrights.org/fs/fs4-junk.htm.

Privacy Right Clearinghouse. (2000, August). *Fact Sheet 18: Privacy in Cyberspace.* Retrieved from http://www.privacyrights.org/fs/fs18-cyb.htm .

Privacy Rights Clearinghouse (1997). *Coping with Identity Theft.* Retrieved from http://www.consumer-action.org/Library/English/Privacy/PV-F-01_EN.html

Queen's University, Faculty of Law, (1996) *Freedom of speech and privacy in the information age* from http://qsilver.queensu.ca/law/sopinka.htm

Rasmussen, M. (2001, May 16). *Justifying IT investments: information security*. Giga Information Group (RIB-052000, 00181)

Rosenberg, M. (2000, April 11). *Ad networks privacy concerns have not spilled over to partnering enterprises.* Giga Information Group, IdeaByte (2 RIB-042000-00077)

Rosenberg, M. (2000, March 7). *Privacy – The unexpected guest in data warehousing.* Giga Information Group. IdeaByte, (RIB-032000-00083)

Sex offender banned from the Internet (2002, January 18). *BBC News* [Electronic Version]. Retrieved from http://news.bbc.co.uk/hi/english/uk/england/newsid_1768000/1768970.stm

Sundgren, J. (2001, February 20). *The Security Component of Privacy*. Giga Information Group, IdeaByte. (RIB-022001-00160)

Thibadeau, R. (2000, August 24). *A critique of P3P: Privacy at the Web*. Pittsburgh, PA: School of Computer Science.

UNESCO (1999, January 18-19). *Papers from the expert meeting on sexual abuse of children, child pornography and pedophilia on the Internet: An international challenge*. Retrieved from http://mirror-us.unesco.org/webworld/child_screen/documents.html

Vassilaki, I. (1997, May). Multimedia crime emergence, phenomena and legal questions of "Metacomputer Crime. *Computer Law & Security Report*, p. 158-162. Elsevier Science

Walters, R. (2001, January). Internet law cyberliability: the dangers and how to combat them. *Computer Law and Security Report*, p. 32-35.

Warchus, J. (2000, August). E-defamation: the Atlantic divide grows wider. *Computer Law and Security Report*, p. 261-262.

White, A. (1999). *Freedom of abuse in the face of world wide concern about the sexual abuse of children, pedophilia and pornography on the Internet*. Retrieved from http://mirror-us.unesco.org/webworld/child_screen/ documents/a_white.rtf

Winick, R. (1997). Intellectual property, defamation and the digital alteration of visual images. *VLA Journal of Law and the Arts-Winter*, 143. University of Columbia.

PREVENTATIVE STRATEGIES WEBSITES

EU WEBSITES

Belgian Citizen's Digital Reporting Site Stop – http://www.ping.be/meldpunt-kinderporno/

Bundesamt für Sicherheit in der Informationstechnik (BSI) – www.bsi.de/

Dr. E-commerce – *www.*europa.eu.int/information_society/topics/ebusiness/ecommerce/index_en.htm

Eicar – www.eicar.org

EuroISPA – www.euroispa.org

Europa- Information Society – europa.eu.int/information_society/text_en.htm

European Working Party on Information Technology Crime – http://www.interpol.int/Public/TechnologyCrime/WorkingParties/Default.asp#europa

Forum of Incident Response and Security Teams (FIRST) – www.first.org

INHOPE – www.inhope.org

Internet Watch Foundation (IWF) – www.iwf.org.uk/index.htm

IPR-Helpdesk – www.ipr-helpdesk.org/index.htm

Joint Research Centre – www.jrc.org

QuickLinks – www.qlinks.net

Recherche et Etude sur la Criminalité Informatique Française (RECIF) www.recif.asso.fr/

US WEBSITES

Association for Computer Machinery (ACM) – www.acm.org

Computer Emergency Response Center (CERT®) – www.cert.org

Cyberangels – www.cyberangels.org

The Electronic Privacy Information Center (EPIC) – www.epic.org

FBI National Computer Crime Squad – www.emergency.com/fbi-nccs.htm

Federal Trade Commission – http://www.ftc.gov/

(1-877-FTC-HELP)

High Technology Crime and Investigations Support – www.njsp.org/tech/tech_unit.html

Identity Theft – http://www.consumer.gov/idtheft/index.html

(1-877-ID-THEFT)

Innocent Images National Initiative (IINI) – www.fbi.gov/hq/cid/cac/innocent.htm

Internet Fraud Complaint Center (IFCC) – www1.ifccfbi.gov/index.asp

Internet Safety Watch Inc – www.cyber-hood-watch.org/kids_internet_safety.htm

The National Center for Missing and Exploited Children – www.missingkids.com (1-800-THE-LOST)

National Infrastructure Protection Center – www.nipc.gov

National Security Institute (NSI) – www.nsi.org/

SANS Institute – www.sans.org/newlook/home.php

The Simon Wiesenthal Center – www.wiesenthal.org

US Department of Education – www.ed.gov

ISSN 1824-274X
ISBN 978-88-8443-163-9